Antonio Aparecido de Andrade é Professor do Departamento de Matemática do Instituto de Biociências, Letras e Ciências Exatas (Ibilce) da Universidade Estadual Paulista ``Júlio de Mesquita Filho" (Unesp), São José do Rio Preto - SP. Graduado em Matemática (Licenciatura) pelo Ibilce - Unesp. Mestre em Matemáaica pelo Instituto de Matemática e Computação Científica (Imecc) da Universidade Estadual de Campinas (Unicamp), Campinas - SP. Doutor em Engenharia Elétrica pela Faculdade de Engenharia Elétrica e de Computaçãao (Fecc) da Unicamp. Livre-docente pelo Ibilce - Unesp. Pós-doutorado pelo Departamento de Matemática do Imecc - Unicamp e pelo Departamento de Matemárica e Estatística da Universidade Estadual de San Diego, San Diego - California, EUA. Pesquisador na áarea de álgebra (teoria algébrica dos números), construçõoes de reticulados, teoria da codificação, modulacão e criptografia.

Pesquisador na área de álgebra com enfoque para a teoria algébrica dos números e aplicações.

Uma introdução à matemática discreta

Antonio Andrade

Uma introdução à matemática discreta

Antonio Aparecido de Andrade

Série Álgebra
Volume 7

UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
INSTITUTO DE BIOCIÊNCIAS, LETRAS E CIÊNCIAS EXATAS
CAMPUS DE SÃO JOSÉ DO RIO PRETO - SP
DEPARTAMENTO DE MATEMÁTICA

UMA INTRODUÇÃO À

MATEMÁTICA DISCRETA

© 2022 - Antonio Aparecido de Andrade

Série Álgebra - Volume 7

Primeira Edição.

ISBN 978-65-00-47261-5

Antonio Aparecido de Andrade

São José do Rio Preto - SP
Julho - 2022

Sumário

Capítulo

1

Introdução

O presente texto foi elaborado em cima das disciplinas de álgebras ministradas nos Cursos de Graduação de Matemática (Licenciatura e Bacharelado) e Bacharelado em Ciências da Computação do Instituto de Biociências, Letras e Ciências Exatas (Ibilce) da Universidade Estadual Paulista "Júlio de Mesquita Filho"(Unesp), Campus de São José do Rio Preto - SP.

O presente texto tem como objetivo de fazer uma breve introdução a matemática discreta introduzindo, no Capítulo 2, apresentamos uma breve introdução á teoria dos conjuntos: definição, noção de conjuntos, relações de pertinência e inclusão, operações entre conjuntos, e uma pequena introdução aos conjuntos numéricos.

No Capítulo 3, apresentamos os números naturais com suas principais operações como á adic cão e à multiplicação, relação de desigualdade, sistema de numeração decimal em relação a uma base b e suas respectivas operações: soma, produto e divisão. No Capítulo 4, apresentamos a aritmética dos números inteiros, axioma da boa ordem, princípio de Indução finita, divisibilidade, algoritmo euclidiano, máximo divisor comum e mínimo múltiplo comum.

No Capítulo 5, apresentamos os números primos, Teorema Fundamental da Aritmética, congruências, função de Euler, Pequeno Teorema de Fermat, Teorema de Euler e Teorema de Wilson. No Capítulo 6, apresentamos uma introdução sobre dígitos verificadores, também chamados de dígitos de controle. No Capítulo 7, apresentamos uma introdução a criptografia com enfoque para os sistemas criptográficos de Júlio César e o RSA. No Capítulo 8, apresentamos as relações binárias: definição, exemplos e representações, domínio, contradomínio, relação inversa, imagem direta e inversa de uma relação, composição de relações e propriedades de uma relação definida sobre um conjunto, relações de equivalência (definição e exemplos) e conjunto quociente, relações de ordem (definição e exemplos),

conjuntos totalmente e parcialmente ordenados, elementos especiais em conjuntos parcialmente ordenados. No Capítulo 9, apresentamos as funções (definição e exemplos), funções injetoras, sobrejetoras e bijetoras, conjunto imagem direta e imagem inversa e suas propriedades em relação às operações entre conjuntos, aplicações monótonas, conjuntos equipotentes e conjuntos enumeráveis, exemplificando com alguns exemplos.

No Capítulo 10, apresentamos as operações binárias, também chamadas de operações de composição interna (definição e exemplos), propriedades de uma operação e tábua de uma operação definida sobre um conjunto finito. No Capítulo 11, apresentamos uma introdução a álgebra de Boole. Finalmente, apresentamos a bibliografia utilizada ao longo do texto.

Capítulo

2

Uma introdução a teoria elementar dos conjuntos

A teoria dos conjuntos foi desenvolvida por Georg Ferdinand Ludwing Phillip Cantor (1845 - 1918) por volta de 1872. No início do século XX (1910 - 1913), a teoria de Cantor obteve um auxílio muito importante do matemático, filósofo e sociólogo Bertrand Russel (1872 - 1970). A ideia de conjunto é a mesma de coleção, classe de objetos, agrupamento, etc. Por exemplo, uma coleção de revistas é um conjunto e cada revista é um elemento desse conjunto. A grosso modo, um conjunto é qualquer coleção de objetos, os objetos que compoẽm um conjunto são chamados elementos e, neste caso, os elementos são distos que pertencem ao conjunto. No estudo da teoria dos conjuntos certas noções são consideradas primitivas, isto é, aceitas sem definição. Os conceitos primitivos da teoria dos conjuntos são: conjunto, elemento e relação de pertinência. A notação usada será:

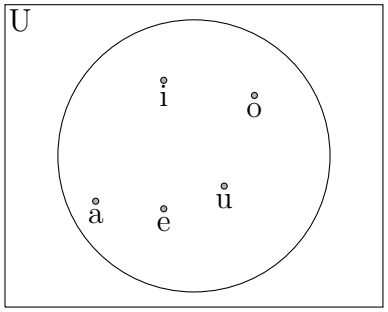
1. para conjuntos são letras maiúsculas: A, B, C, $\cdots$, e
2. para elementos são letras minúsculas: a, b, c, $\cdots$

A relação de pertinência é entre elemento e conjunto, ou seja, se A é um conjunto e x um elemento, diz-se que $x \in A$ se x é um elemento do conjunto A e $x \notin A$ se x não é um elemento do conjunto A. As relações entre conjuntos são dadas por: contido ($\subset$), contido ou igual ($\subseteq$), contém ($\supset$), contém ou igual ($\supseteq$) e igualdade ($=$).

Neste capítulo, apresentamos alguns fatos básicos sobre a teoria dos conjuntos necessários para o entendimento do presente texto.

2.1 Conjuntos

Um conjunto é uma coleção de objetos. Os objetos de um conjunto são chamados de elementos. O matemático inglês John Venn (1834 - 1923) adotou uma maneira de representar conjuntos que muito nos ajuda na visualização das operações entre conjuntos, onde os elementos de um conjunto são representados por pontos interiores a uma região plana, limitada por uma linha fechada simples, isto é, uma linha que não se entrelaça, chamado diagrama de Euler-Venn. Por exemplo, o conjunto das vogais pode ser representado por



onde U representa o conjunto universo.

Basicamente, usamos três maneiras para representar os elementos de um conjunto.

1. Quando o conjunto é dado pela enumeração de seus elementos (mesmo quando possui infinitos elementos). Neste caso, escreve-se os elementos entre chaves e separados por vírgula. Por exemplo, $A = \{a_1, a_2, \ldots\}$.

2. Quando enuncia uma propriedade comum aos seus elementos, ou seja, o conjunto A é dado por $A = \{x : x \text{ possui tal propriedade}\}$.

3. Quando o conjunto é dado pelo diagrama de Euler-Venn.

O conjunto $A = \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$ é um conjunto de quatro elementos, onde cada um dos elementos é um conjunto.

Existem alguns tipos de conjuntos.

1. Conjunto vazio: é o conjunto que não possui elementos e denotado por $\{\}$ ou $\emptyset$. Por exemplo, $A = \{x \in \mathbb{R} : x^2 + 2 = 0\} = \emptyset$.

2. Conjunto unitário: é um conjunto que possui apenas um elemento. Por exemplo, o conjunto $A = \{x \in \mathbb{N} : 2 < x < 4\} = \{3\}$.

3. Conjunto finito: é o conjunto que possui um número finito de elementos. Por exemplo, $A = \{1, 3, 5, 7\}$.

4. Conjunto infinito: é o conjunto que possui um número infinito de elementos. Por exemplo, $A = \mathbb{N}$.

5. O número de elementos de um conjunto é chamado de cardinalidade do conjunto.

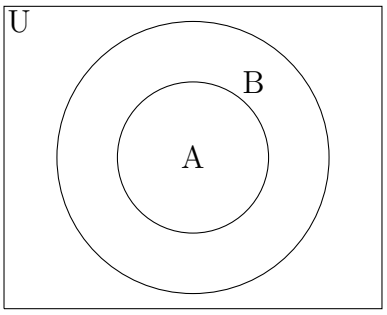
6. Conjunto universo U: é um conjunto ao qual pertencem todos os elementos de estudo.

Sejam A e B dois conjuntos.

1. Subconjunto $A \subseteq B$: se todo elemento x de A for também um elemento de B. Neste caso, A é chamado um subconjunto de B, ou seja,

$$A \subseteq B \Longleftrightarrow (\forall x \in A \Longrightarrow x \in B).$$

Quando $A \subseteq B$, diz-se que A está contido em B ou A é um subconjunto de B ou A é parte de B. O conjunto vazio é um conjunto sem elementos, e assim, $\emptyset$ é um subconjunto de qualquer conjunto A, inclusive dele mesmo, ou seja, $\emptyset \subseteq A$, para qualquer conjunto A. Além disso, o conjunto $\emptyset$ pode ser escrito como $\emptyset = \{x \in U : x \neq x\}$.



2. Conjuntos iguais: são conjuntos que possuem os mesmos elementos, ou seja,

$$A = B \text{ se, e somente se, } A \subseteq B \text{ e } B \subseteq A,$$

isto é, dois conjuntos são iguais quando têm os mesmos elementos.

3. Conjuntos distintos: dois conjuntos são distintos se não são iguais e denotado por $A \neq B$. Neste caso, existe um elemento $x \in A$ tal que $x \notin B$ ou existe um elemento $x \in B$ tal que $x \notin A$. Pode acontecer de $A \neq B$, mas $A \subset B$.

Vale observar que $\emptyset$ é um subconjunto de qualquer conjunto e $A \subseteq A$, para qualquer conjunto A. Um conjunto pode ter outros conjuntos como elementos, por exemplo,

$$A = \{\emptyset, \{a\}, \{b\}, \{a, b\}.$$

Neste caso, $\{a\} \in A$ e $a \notin A$.

O conjunto das partes de um conjunto A é definido por

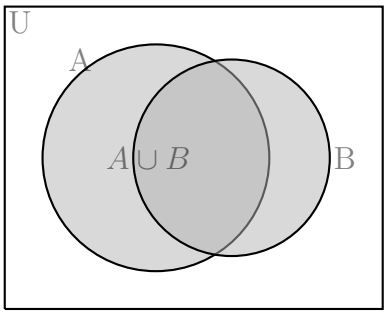
$$\mathcal{P}(A) = \{X : X \subseteq A\},$$

ou seja, $\mathcal{P}(A)$ é o conjunto formado por todos os subconjuntos de A. Neste caso, X é um subconjunto de A e X é um elemento de $\mathcal{P}(A)$, ou seja, $A \subseteq X$ e $X \in \mathcal{P}(A)$. Agora, se A tem n elementos, então $\mathcal{P}(A)$ tem 2^n elementos. Por exemplo,

1. Se $A = \{a, b\}$, com $a \neq b$, então $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.
2. Se $A = \emptyset$, então $\mathcal{P}(A) = \{\emptyset\}$.
3. Se $A = \{\emptyset\}$, então $\mathcal{P}(A) = \{\emptyset, \{\emptyset\}\}$.
4. Se $A = \{0, 1, 2\}$, então $\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}$.

As operações entre conjuntos são: união ($\cup$), interseção ($\cap$), diferença ou subtração ($-$) e complementar (c). Assim, em relação a dois conjuntos A e B temos as seguintes operações.

1. União: $A \cup B = \{x \in U : x \in A \text{ ou } x \in B\}$.



Neste caso, vale as seguintes propriedades:

- $A \cup B = B \cup A$ (comutativa).
- $A \cup (B \cup C) = (A \cup B) \cup C$ (associativa).
- $A \subseteq A \cup B$ e $B \subseteq A \cup B$.
- $A \subseteq B$ se, e somente se, $A \cup B = B$.
- $A = A \cup A$, $A = A \cup \emptyset$ e $U = A \cup U$.

A união de um número finito de conjuntos $A_1, A_2, \ldots, A_n$ é dada por

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n.$$

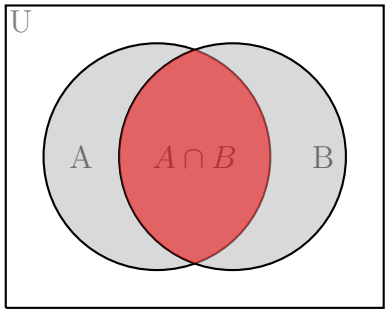
A união de uma família finita de conjuntos $A_1, A_2, \ldots, A_n, \ldots$ é dada por

$$\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup \cdots \cup A_n \cdots .$$

Agora, a união de uma família de conjuntos $(A_i)_{i\in I}$ é dada por

$$\bigcup_{i\in I} A_i = \{a : \exists i \in I,\ a \in A_i\}.$$

2. Interseção: $A \cap B = \{x \in U : x \in A \text{ e } x \in B\}$.



Neste caso, vale as seguintes propriedades:

- $A \cap B = B \cap A$ (comutativa).
- $A \cap (B \cap C) = (A \cap B) \cap C$ (associativa).
- $A \cap B \subseteq A$ e $A \cap B \subseteq B$.
- $A \cap A = A$, $A \cap \emptyset = \emptyset$ e $A \cap U = A$.
- $A \subseteq B$ se, e somente se, $A \cap B = A$.

A interseção de um número finito de conjuntos $A_1, A_2, \ldots, A_n$ é dada por

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n.$$

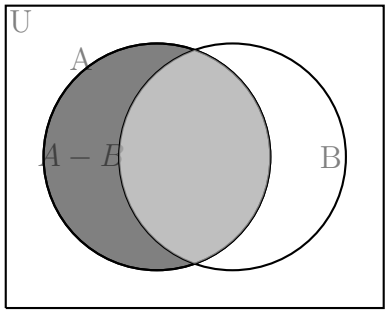
A interseção de uma família de conjuntos $A_1, A_2, \ldots, A_n, \ldots$ é dada por

$$\bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap \cdots \cap A_n \cdots .$$

Agora, a interseção de uma família de conjuntos $(A_i)_{i\in I}$ é dada por

$$\bigcap_{i\in I} A_i = \{a : a \in A_i,\ \forall i \in I\}.$$

3. Subtração: $A - B = \{x \in U : x \in A \text{ e } x \notin B\}$.



Neste caso, vale as seguintes propriedades

- $A = B$ se, e somente se, $A - B = B - A = \emptyset$.
- $A \neq B$ se, e somente se, $A - B \neq B - A$.
- $A - A = \emptyset$, $A - B \subseteq A$, $A - \emptyset = A$ e $A - U = \emptyset$.

4. Complementar de A: $A^c = \{x \in U : x \notin A\}$.

5. Complementar de A em relação a B (neste caso, devemos ter $A \subseteq B$) é definido por $A^c_B = \{x \in U : x \in B \text{ e } x \notin A\} = B - A$. Se $B = U$, então $A^c_U = \{x \in U : x \notin A\}$. Nesse caso, vale as seguintes propriedades:

   - se $A \subseteq B$, se e somente se $B - A = A^c_B$, ou seja, quando A é um subconjunto de B, o conjunto diferença $B - A$ é chamado conjunto complementar de B em relação ao conjunto A.
   - $\emptyset^c_U = U$ e $U^c_U = \emptyset$.
   - $A^c_U \cap A = \emptyset$ e $A^c_U \cup A = U$.
   - $\emptyset^c_A = A$ e $\emptyset^c_\emptyset = \emptyset$.

6. Produto cartesiano: $A \times B = \{(x, y) : x \in A \text{ e } x \in B\}$. Nesse caso,

   - $A \times (B \times C) \neq (A \times B) \times C$ (não é associativa).
   - $A \times B \neq B \times A$ (não é comutativa).
   - $A \times \emptyset = \emptyset \times A = \emptyset$.

O produto cartesiano de n conjuntos $A_1, A_2, \ldots, A_n$, indicado por $A_1 \times A_2 \times \cdots \times A_n$, é o conjunto das n-uplas ordenadas $(a_1, a_2, \ldots, a_n)$, onde $a_i \in A_i$ para $i = 1, 2, \ldots, n$, ou seja,

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_i \in A, \text{ para } i = 1, 2, \ldots, n\}.$$

Agora, se A, B e C são conjuntos, então

1. $A \subseteq A$ (reflexiva).

2. Se $A \subseteq B$ e $B \subseteq A$, então $A = B$ (anti-simétrica).

3. Se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$ (transitiva).

4. Leis de Morgan do matemático inglês Augustus de Morgan (1806 - 1871):

   - $(A \cup B)^c = A^c \cap B^c$ e
   - $(A \cap B)^c = A^c \cup B^c$.

5. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ e $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (distributiva).

2.1.1 Exercícios

1. Determine $A \cap B$, $A \cup B$, $A \times B$, $A - B$, A^c_B e B^c_A.

   (a) $A = \{a, b, c, d, e\}$ e $B = \{a, b, d, f, g, h\}$.

   (b) $A = \{0, 1, 2, 3, 4, 5, 7, 8\}$ e $B = \{2, 4, 6, 8, 10\}$.

   (c) $A = \{x \in \mathbb{N} : \ x \text{ é par}\}$ e $B = \{x \in \mathbb{N} : \ x \text{ é impar}\}$.

2. Determine $A \cap B$, $A \cup B$, $A \times B$, $A - B$, A^c_B e B^c_A.

   (a) $A = \{x \in \mathbb{N} : x^2 + 1 \leq 2\}$ e $B = \{x \in \mathbb{Z} : -1 < x < 2\}$.

   (b) $A = \{x \in \mathbb{Z} : x^3 + 1 \leq 15\}$ e $B = \{x \in \mathbb{N} : 1 < x < 4\}$.

   (c) $A = \{x \in \mathbb{Z} - \{0\} : \frac{30}{x} = n, \text{ onde } n \in \mathbb{N}\}$ e $B = \{x \in \mathbb{R} : x = 3n, \text{ onde } n \in \mathbb{N}\}$.

3. Seja A um conjunto não vazio. Mostre que

   (a) $A = A - \emptyset$.

   (b) $\emptyset - A = \emptyset$.

4. Sejam A e B dois conjuntos. Mostre que:

   (a) $A \cap B \subseteq A$.

   (b) $A \subseteq A \cup B$.

   (c) $A - B \subseteq A$.

5. Sejam $A = \{0, 2, 4, 6, 8, 10\}$, $B = \{0, 1, 2, 3, 4, 5, 6\}$ e $C = \{4, 5, 6, 7, 8, 9, 10\}$. Detemine:

   (a) $A \cap B \cap C$.

   (b) $A \cup B \cup C$.

   (c) $(A - B) \cup (A - C)$.

   (d) $(A \cap B) \cup C$.

6. Determine o conjunto das partes $\mathcal{P}(A)$, onde

(a) $A = \emptyset$.

(b) $A = \{\emptyset\}$.

(c) $A = \{\emptyset, \{\emptyset\}\}$.

(d) $A = \{1, 2, 3, 4, 5\}$.

7. Sejam A e B dois conjuntos.

   (a) Mostre que $A \subseteq B$ se, e somente se, $B^c \subseteq A^c$.

   (b) $A \cap B \subseteq A \cup B$.

   (c) $A - B = A \cap B^c$.

   (d) $(A \cap B) \cap (A \cap B^c) = A$.

8. Seja $A_i = \{1, 2, 3, \ldots, n\}$, para $i = 1, 2, \ldots$. Determine $\cup_{i=1}^{n} A_i$ e $\cap_{i=1}^{n} A_i$.

9. Seja $A_i = \{\ldots, -2, -1, 0, 1, 2, \ldots, i\}$, para $i = 1, 2, \ldots$. Determine $\cup_{i=1}^{n} A_i$ e $\cap_{i=1}^{n} A_i$.

10. Se $(A_i)_{i\in I}$ é uma família de subconjuntos de um conjunto E e se $(B_j)_{j\in J}$ é uma família de subconjuntos de um conjunto F, mostre que $(\bigcup_{i\in I} A_i) \times (\bigcup_{j\in J} B_j) = \bigcup_{(i,j)\in I\times J}(A_i \times B_j)$.

11. Considere a família de intervalos $(A_n)_{n\in\mathbb{N}}$, onde $A_n =]0, \frac{1}{n}[$. Mostre que $\bigcap_{n\in\mathbb{N}} A_n = \emptyset$.

12. Seja $A =]0, 1[$ e considere a família de intervalos $(A_n)_{n\geq 2}$, onde $A_n =]\frac{1}{n}, 1[$.

   (a) Mostre que $\bigcup_{n\geq 2} A_n = A$.

   (b) Mostre que $A_{n_1} \cup \cdots \cup A_{n_r} \neq A$, para quaisquer que sejam $n_1, \cdots, n_r$.

13. Liste todos os elementos dos conjuntos abaixo.

   (a) $A = \{x : \ x \text{ é um número real tal que } x^2 = 1\}$.

   (b) $A = \{x : \ x \text{ é um número inteiro positivo menor que } 12\}$.

   (c) $A = \{x : \ x \text{ é o quadrado de um número inteiro e } x < 100\}$.

   (d) $A = \{x : \ x \text{ é um número inteiro tal que } x^2 = 2\}$.

14. Verifique se os conjuntos abaixo são iguais.

   (a) $A = \{1, 1, 1, 3, 4, 4, 3\}$ e $B\{1, 3, 4\}$.

   (b) $A = \{\{1\}\}$ e $B = \{1, \{1\}\}$.

   (c) $A = \emptyset$ e $B = \{\emptyset\}$.

15. Sejam $A = \{2, 4, 6\}$, $B = \{2, 6\}$, $C = \{4, 6\}$ e $D = \{4, 6, 8\}$. Determine quais desses conjuntos são subconjuntos de outros desses subconjuntos.

16. Verifique se 2 é um elemento dos conjuntos abaixo.

   (a) $A = \{x \in \mathbb{R} : \ x \text{ é um número inteiro maior que } 1\}$.

(b) $A = \{x \in \mathbb{R} : \ x$ é o quadrado de um número inteiro $1\}$.

(c) $A = \{2, \{2\}\}$.

(d) $A = \{\{2\}, \{\{2\}\}\}$.

(e) $A = \{\{2\}, \{2, \{2\}\}\}$.

17. Verifique se $\{2\}$ é um elemento dos conjuntos abaixo.

(a) $A = \{x \in \mathbb{R} : \ x$ é um número inteiro maior que $1\}$.

(b) $A = \{x \in \mathbb{R} : \ x$ é o quadrado de um número inteiro $1\}$.

(c) $A = \{2, \{2\}\}$.

(d) $A = \{\{2\}, \{\{2\}\}\}$.

(e) $A = \{\{2\}, \{2, \{2\}\}\}$.

18. Verifique quais afirmações abaixo são verdadeiras.
(a) $0 \in \emptyset$. (b) $\{0\} \subseteq \emptyset$.
(c) $\{0\} \in \{0\}$. (d) $\{\emptyset\} \subseteq \{\emptyset\}$.
(e) $\emptyset \in \{0\}$. (f) $\emptyset \subseteq \{0\}$.

19. Verifique quais afirmações abaixo são verdadeiras.
(a) $\emptyset \in \emptyset$. (b) $\{\emptyset\} \in \{\emptyset\}$.
(c) $\{\emptyset\} \subseteq \{\emptyset, \{\emptyset\}\}$. (d) $\{\{\emptyset\}\} \subseteq \{\{\emptyset\}, \{\emptyset\}\}$.
(e) $\emptyset \in \{\emptyset, \{\emptyset\}\}$. (f) $\{\{\emptyset\}\} \subseteq \{\emptyset, \{\emptyset\}\}$.

20. Verifique quais afirmações abaixo são verdadeiras.
(a) $a \in \{a\}$. (b) $\{x\} \in \{\{x\}\}$.
(c) $\{x\} \subseteq \{x\}$. (d) $\emptyset \subseteq \{x\}$.
(e) $\{x\} \in \{x\}$. (f) $\emptyset \in \{x\}$.

21. Calcule os seguintes conjuntos abaixo, onde $a \neq b$.

(a) $\mathcal{P}(\{a, b, \{a, b\}\})$.

(b) $\mathcal{P}(\{\emptyset, a, \{a\}, \{\{a\}\}\})$.

(c) $\mathcal{P}(\mathcal{P}(\{a, b\}))$.

(d) $\mathcal{P}(\mathcal{P}(\emptyset))$.

22. Sejam $A = \{1, 2, 3\}$ e $B = \{a, b\}$. Detemine $A \times B$ e $B \times A$.

23. Sejam $A = \{1, 2, 3\}$, $B = \{a, b\}$ e $C = \{x, y, z\}$. Detemine $(A \times B) \times C$, $A \times (B \times C)$, $(B \times A) \times C$ e $A \times (C \times B)$.

24. Sejam $A = \{1, 2, 3\}$, $B = \{a, b\}$ e $C = \{x, y, z\}$. Detemine $A \times B \times C$, $A \times B \times C$, $B \times A \times C$ e $A \times C \times B$.

25. Sejam A um conjunto de m elementos e B de n elementos. Determine o número de elementos de $A \times B$ e $B \times A$.

26. Se $A = \emptyset$ e $B = \{a, b\}$, calcule $A \times B$.

27. Verifique se existe dois conjuntos A e B tal que $A \in B$ e $A \subseteq B$.

28. Determine o conjunto das partes $\mathcal{P}(A)$, onde

    (a) $A = \{\{a\}, b\}$.

    (b) $A = \mathbb{N}$.

    (c) $A = \{x \in \mathbb{Z} : x^2 \leq 10\}$.

29. Seja $A = \{\{a\}, \{a, b\}\}$. Determine $A \times A$.

2.2 Conjuntos numéricos

Os principais conjuntos formados por números são dados por:

1. $\mathbb{N} = \{0, 1, 2, \cdots\}$ é chamado conjunto dos números naturais.

2. $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ é chamado conjunto dos números inteiros.

3. $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z} \text{ e } b \neq 0\}$ é chamado conjunto dos números racionais. Um número racional é representado por uma razão entre dois inteiros, ou seja, é uma dízima periódica.

4. $\mathbb{I}$ é chamado o conjunto dos números irracionais. Um número irracional é um número com infinitas casas decimais e não periódica.

5. $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$ é chamado o conjunto dos números reais.

6. $\mathbb{C} = \{a + bi : a, b \in \mathbb{R} \text{ com } i^2 = -1\}$ é chamado o conjunto dos números complexos.

7. $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1, ij = k = -ji, jk = i = -kj, ki = j = -ik\}$ é chamado o conjunto dos números quatérnios de Hamilton.

Esses conjuntos, com exeção dos números irracionais, possuem as operações de adição (soma) e multiplicação (ou produto) muito bem definidas. Em relação a adição, considerando $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$, segue que

1. $a + b \in A$, para todo $a, b \in A$, chamada propriedade do fechamento.

2. $a + (b + c) = (a + b) + c$, para todo $a, b, c \in A$, chamada propriedade associativa.

3. $a + b = b + a$, para todo $a, b \in A$, chamada propriedade comutativa.

4. $a + 0 = a$, para todo $a \in A$, onde o 0 é chamado elemento neutro.

5. $a + (-a) = 0$, para todo $a \in A$, onde $-a$ é chamado elemento oposto (ou simétrico) de a.

Em relação a multiplicação (produto), considerando $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$, segue que

1. $ab \in A$, para todo $a, b \in A$, chamada propriedade do fechamento.
2. $a(bc) = (ab)c$, para todo $a, b, c \in A$, chamada propriedade associativa.
3. $a1 = a$, para todo $a \in A$, onde o elemento 1 é chamado elemento neutro.
4. Se $ab = 0$, então $a = 0$ ou $b = 0$, com $a, b \in A$, chamada *Lei do Anulamento do Produto*.

Além disso,

1. $ab = ba$, para todo $a, b \in A$, chamada propriedade comutativa, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$.
2. Para todo $a \in A - \{0\}$, existe $a^{-1} \in A - \{0\}$ tal que $aa^{-1} = 1$, onde $A = \mathbb{Q}, \mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$. O elemento a^{-1} é chamado elemento inverso (ou simétrico) de a.

Em relação a adição e a multiplicação, segue que $a(b + c) = ab + ac$ e $(a + b)c = ac + bc$, para todo $a, b, c \in A$, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$, chamada operação distributiva em relação a adição) e a multiplicação. Existe uma operação de ordem, denotada por $\leq$, que satisfaz as seguintes propriedades básicas:

1. $a \leq a$, para todo $a \in A$, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$, chamada propriedade reflexiva.
2. Se $a \leq b$ e $b \leq a$, então $a = b$, com $a, b \in A$, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$, chamada propriedade anti-simétrica.
3. Se $a \leq b$ e $b \leq c$, então $a \leq c$, com $a, b, c \in A$, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$, chamada propriedade transitiva.
4. $a \leq b$ ou $b \leq a$, para todo $a, b \in A$, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$, chamada propriedade da totalidade.
5. Se $a \leq b$, então $a+c \leq b+c$, com $a, b, c \in A$, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$, chamada propriedade da compatibilidade com a adição.
6. Se $0 \leq a$ e $0 \leq b$, então $0 \leq ab$, com $a, b \in A$, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$, chamada propriedade da compatibilidade com a multiplicação.

Em relação a regra dos sinais, segue as seguintes propriedades:

1. Se $a > 0$ e $b > 0$, então $ab > 0$, com $a, b \in A$, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$.
2. $a < 0$ e $b < 0$, então $ab > 0$, com $a, b \in A$, onde $A = \mathbb{Z}, \mathbb{Q}, \mathbb{I}$ ou $\mathbb{R}$.
3. Se $a > 0$ e $b < 0$, então $ab < 0$, com $a, b \in A$, onde $A = \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$.

Finalmente, as seguintes notações são usadas para denotarem os seguintes conjuntos:

1. $A^* = \{a \in A :$ existe $a^{-1} \in A$ tal que $aa^{-1} = 1\}$, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$, chamado conjunto dos elementos inversíveis de A.

2. $A_+ = \{x \in A : x \geq 0\}$ é chamado o conjunto dos elementos positivos de A, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$.

3. $A_+ - \{0\} = \{x \in A : x > 0\}$ é chamado o conjunto dos elementos estritamente positivos de A.

4. $A_- = \{x \in A : x \leq 0\}$ é chamado o conjunto dos elementos negativos de A, onde $A = \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$.

5. $A_- - \{0\} = \{x \in A : x < 0\}$ é chamado o conjunto dos elementos estritamente negativos de A, onde $A = \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$.

2.2.1 Exercícios

1. Mostre que não existe um quadrado perfeito a^2 cujo último dígito é 2, 3, 7 ou 8.

2. Mostre que 44444444444444444443 não é um quadrado perfeito.

3. Mostre que $888\cdots882$ não é um quadrado perfeito.

4. Mostre que não existe um quadrado perfeito cujo os dois últimos dígitos são 85.

5. Mostre que $\sqrt{2}$ é irracional.

6. Mostre que $\sqrt{3}$ é irracional.

7. Mostre que $\sqrt[3]{4}$ é irracional.

8. Mostre que $\sqrt{6}$ é irracional.

9. Mostre que $\frac{1}{3}\sqrt{2} + 5$ é irracional.

10. Mostre que $log_5 2$ e $log_3 5$ são irracionais.

11. Mostre que $\sqrt{101}$ é irracional.

12. Mostre que $\sqrt{p}$ é irracional, onde p é um primo.

13. Determine os cojuntos:

    (a) $A = \{x \in \mathbb{R} : x^2 = -1\}$.

    (b) $A = \{x \in \mathbb{Z} : x - 1 \in \mathbb{Z}\}$.

    (c) $A = \{x \in \mathbb{C} : a^2 + b^2 = 1\}$.

14. Determine os conjuntos:

    (a) $A = \{x \in \mathbb{C} : x^2 + 1 = 0\}$.

(b) $A = \{x \in \mathbb{Z} : x^2 + 2 = 10\}$.

(c) $A = \{x \in \mathbb{R} : x^2 + x + 2 = 0\}$.

15. Mostre que os conjuntos $A = \{2^m 3^n : m, n \in \mathbb{N}\}$ e $\mathbb{Z} \times \mathbb{Z}$ tem a mesma cardinalidade.

16. Mostre que.

(a) Todo conjunto finito está em bijeção com um subconjunto dos naturais.

(b) Os conjuntos $\mathbb{N}$ e $\mathbb{Z}$ tem a mesma cardinalidade.

(c) Os conjuntos $\mathbb{N}$ e $\mathbb{Q}$ tem a mesma cardinalidade.

(d) Os conjuntos $\mathbb{N}$ e $\mathbb{R}$ não tem a mesma cardinalidade.

17. Sejam x e y são números reais positivos. A média aritmética de x e y é definida por $(x + y)/2$. A média geométrica de x e y é definida por $\sqrt{xy}$. A média harmônia de x e y é definida por $2xy/(x + y)$. A média quadrática aritmética de x e y é definida por $\sqrt{(x^2 + y^2)/2}$.

(a) Mostre que $(x + y)/2 > \sqrt{xy}$.

(b) Encontre relações entre essas médias.

2.3 Sequências

Sequências são listas ordenadas de elementos, ou seja, é uma estrutura discreta uasada para representar uma lista ordenada. Sequências são usadas de várias maneiras, por exemplo, na matemática e na computação. A sequência 1, 2 e 4 é uma sequência de três termos.

Definição 2.3.1. *Uma sequência é uma função de um subconjunto limitado inferiormente dos inteiros para um conjunto S, ou seja, é uma função $f : A \to S$, onde $A \subseteq \mathbb{Z}$ é limitado inferiormente, e definida por $f(n) = a_n$, com $ninA$. Os elmentos a_n são chamados termos da sequência. A notação (a_n) é usada para descrever a sequência.*

A soma de duas sequências (a_i) e (b_i) é dada por $(a_i + b_i) = (a_i) + (b_i)$ e produto por escalar é dada por $\alpha(a_i) = (\alpha a_i)$, onde $\alpha \in \mathbb{R}$.

Exemplo 2.3.1. *Se $A = \mathbb{N} - \{0\}$, então $a_n = \frac{1}{n}$, onde $n \in A$. Neste caso, a sequência é dada por $1, \frac{1}{2}, \frac{1}{3}, \ldots$.*

Exemplo 2.3.2. *Uma progressão aritmética $a, a + r, a + 2r, a + 3r, \ldots$ é uma sequência, onde a é o termon inicial e r é a razão. Neste caso, é uma função linear da forma $f(x) = ax + b$.*

Exemplo 2.3.3. *Uma progressão geométrica $a, aq, aq^2, aq^3, \ldots$ é uma sequência, onde a é o termon inicial e q é a razão. Neste caso, é uma função exponencial da forma $f(x) = aq^x$.*

Uma sequência pode ser ser finita (se o número de termos é finita) ou infinita (se o número de termos é infinita).

2.3.1 Somatório

Seja (a_n) uma sequência finita dada por $\{a_1, a_2, \ldots, a_n\}$. A letra grega sigma maiúscula, denotada por Σ, é usada para indicar o somatório. A soma dos n termos dessa sequência é definida por

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n.$$

Se os elementos da sequência são dados por $a_m, a_{m+1}, a_{m+2}, \ldots, a_n$, então sua soma é dada por

$$\sum_{i=m}^{n} a_i = a_m + a_{m+1} + \cdots + a_n.$$

A variável i é chamada de índice da somatória, que também pode ser j, k, etc.

Agora, considerando uma sequência infinita $a_0, a_1, a_2, \ldots$, a sua soma é definida por

$$\sum_{i=0}^{\infty} a_i = a_0 + a_1 + a_2 + \cdots + a_n + \cdots,$$

chamada uma série infinita, que estudadas em análise matemática, onde a soma pode ser finita ou infinita.

Sejam (a_i) e (b_i) duas sequências finitas de n termos, α e β números reais. Neste caso, vale a seguinte propriedade:

$$\sum_{i=1}^{n}(\alpha a_i + \beta b_i) = \alpha \sum_{i=1}^{n} a_i + \beta \sum_{i=1}^{n} b_i.$$

2.3.2 Produtório

Seja (a_n) uma sequência finita dada por $\{a_1, a_2, \ldots, a_n\}$. A letra grega pi maiúscula, denotada por $\prod$, é usada para indicar o produtório. O produto dos n termos dessa sequência é definida por

$$\prod_{i=1}^{n} a_i = a_1 a_2 \cdots a_n.$$

Se os elementos da sequência são dados por $a_m, a_{m+1}, a_{m+2}, \ldots, a_n$, então o seu produto é dado por

$$\prod_{i=m}^{n} a_i = a_m a_{m+1} \cdots a_n.$$

A variável i é chamada de índice do produtório, que também pode ser j, k, etc. Se (a_i) é uma sequência finita de n termos e α um número real, então

$$\prod_{i=1}^{n}(\alpha a_i) = \alpha^n \prod_{i=1}^{n} a_i.$$

2.3.3 Exercícios

1. Determine os termos a_0, a_2 e a_3 das seguintes sequências.

   (a) $a_n = 2.(-3)^n + 5^n$.

   (b) $a_n = (-1)^n + n$.

   (c) $a_n = n + (-2)^n$

2. Determine os termos a_0, a_2, a_4 e a_6 das sequências.

   (a) $a_n = 2^n + 1$.

   (b) $a_n = (n+1)^{n+1}$.

   (c) $a_n = 2^n + (-2)^n$.

3. Calcule:

   (a) A soma $\sum_{n=1}^{100} \frac{1}{n}$.

   (b) A soma $\sum_{n=1}^{5} n^2$.

   (c) A soma $\sum_{i=1}^{n} n$.

   (d) A soma $\sum_{i=1}^{n} (-1)^i$.

4. Calcule:

   (a) O produto $\prod_{n=1}^{100} \frac{1}{n}$.

   (b) O produto $\prod_{n=1}^{5} n^2$.

   (c) O produto $\prod_{i=1}^{n} n$.

   (d) O produto $\prod_{i=1}^{n} (-1)^i$.

5. Sejam a e r números reais com $r \neq 0$. Mostre que:

   (a) $\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$ para $|x| < 1$.

   (b) $\sum_{n=1}^{\infty} nx^{n-1} = \frac{1}{(1-x)^2}$ para $|x| < 1$.

6. Determine os termos a_0, a_2, a_4 e a_6 das sequências.

   (a) $a_n = 2^n + 1$.

(b) $a_n = (n+1)^{n+1}$.

(c) $a_n = 2^n + (-2)^n$.

7. Mostre que:

(a) $\sum_{i=0}^{n} ar^i = \frac{ar^{n+1}-a}{r-1}$ se $r \neq 1$.

(b) $\sum_{i=0}^{n} ar^i = (n+1)a$ se $r = 1$.

8. Calcule:

(a) A soma dupla $\sum_{i=1}^{4}\sum_{j=1}^{3} ij$.

(b) A soma dupla $\sum_{j=1}^{3}\sum_{i=1}^{4} ji$.

(c) A soma $\sum_{i\in\{0,1,4\}} i$.

9. Mostre que:

(a) $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

(b) $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.

(c) $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$.

(d) $\sum_{i=0}^{\infty} x^i = \frac{1}{x}$ se $|x| < 1$.

(e) $\sum_{i=1}^{\infty} ix^{i-1} = \frac{1}{(1-x)^2}$ se $|x| < 1$.

10. Mostre que a soma $\sum_{i=50}^{100} i^2 = \frac{n(n+1)}{2} = 297925$.

11. Mostre que:

(a) $\sum_{n=0}^{\infty} x^n = \frac{x^{n+1}-1}{x-1}$ se $|x| < 1$.

(b) $\sum_{n=1}^{\infty} nx^{n-1} = \frac{1}{(1-x)^2}$ se $|x| < 1$.

12. Calcule às seguintes somas:

(a) $\sum_{i=1}^{2}\sum_{j=1} 3(i+2j)$.

(b) $\sum_{i=1}^{3}\sum_{j+1}^{2}(2i^2+3j)$.

13. Mostre $\sum_{i=1}^{n}(a_i - a_{i-1}) = a_n - a_0$.

14. Determine os valores dos produtos abaixo.

    (a) $\prod_{i=1}^{4} i$.

    (b) $\prod_{i=5}^{6} i^2$.

    (c) $\prod_{i=1}^{4} 2$.

15. Determine:

    (a) A soma dos 1000 primeiros números naturais.

    (b) A soma do números pares menores ou iguais a 1000.

    (c) O produto dos números ímpares menores ou igauis a 10.

Capítulo

3

Números naturais

Neste capítulo, apresentamos a construção lógica dos números naturais, com o objetivo de compreender através do conjunto dos naturais algumas propriedades, operações e relações do conjunto dos inteiros. A formalização que faremos a seguir se deve a Giuseppe Peano ($1858 - 1932$) e data de 1891. Ele usou três conceitos primitivos: o *zero*, o *número natural* e a relação *é sucessor de*, cujas notações são, respectivamente: 0, a e a^+. Para caracterizá-los, formulou os seguintes axiomas.

Os números naturais tiveram suas origens nas palavras utilizadas para a contagem de objetos, começando com o número dois, e assim por diante. O avanço seguinte na abstração foi o uso de numerais para representar os números. Isto permitiu o desenvolvimento de sistemas para o armazenamento de grandes números. Por exemplo, os babilônicos desenvolveram um sistema de atribuição de valor baseado essencialmente nos numerais de 1 a 10. Os egípcios antigos possuíam um sistema de numerais com hieróglifos distintos para 1, 10, e todas as potências de 10 até um milhão. Uma gravação em pedra encontrada em Karnak, datando de cerca de 1500 a.C. e atualmente no Louvre, em Paris, representa 276 como 2 centenas, 7 dezenas e 6 unidades; e uma representação similar para o número 4622.

Um avanço muito posterior na abstração foi o desenvolvimento da ideia do zero como um número com seu próprio numeral. Um dígito zero tem sido utilizado como notação de posição desde cerca de 700 a.C. pelos babilônicos, porém ele nunca foi utilizado como elemento final. Os olmecas e a civilização maia utilizaram o zero como um número separado desde o século I a. C., aparentemente desenvolvido independentemente, porém seu uso não se difundiu na Mesoamérica. O conceito da forma como ele é utilizado atualmente se originou com o matemático indiano Brahmagupta em 628. Contudo, o zero foi utilizado como um número por

todos os computus (calculadoras da idade média) começando com Dionysius Exiguus em 525, porém no geral nenhum numeral romano foi utilizado para escrevê-lo. Ao invés disto, a palavra latina para "nenhum", "nullae", foi empregada.

O primeiro estudo esquemático dos números como abstração (ou seja, como entidades abstratas) é comumente atribuído aos filósofos gregos Pitágoras e Arquimedes. Entretanto, estudos independentes também ocorreram por volta do mesmo período na Índia, China, e Mesoamérica.

No século XIX, uma definição do conjunto teórico dos números naturais foi desenvolvida. Com esta definição, era mais conveniente incluir o zero (correspondente ao conjunto vazio) como um número natural. Esta convenção é seguida pelos teorizadores de conjuntos, logicistas, e cientistas da computação. Outros matemáticos, principalmente os teorizadores dos números, comumente preferem seguir a tradição antiga e excluir o zero dos números naturais.

Neste capítulo, apresentamos os números naturais com suas operações de soma e produto, a relação de ordem de desigualdade e sistema de numeração decimal.

3.1 Números naturais

Nesta seção, veremos a construção lógica dos números naturais, com o objetivo de compreender através do conjunto dos naturais algumas propriedades, operações e relações do conjunto dos inteiros. Uma construção consistente do Conjunto dos Números Naturais foi desenvolvida no século XIX por Giuseppe Peano ($1858 - 1932$). Essa construção, comumente chamada de Axiomas de Peano, formulada em 1891, é uma estrutura simples e elegante, servindo como um bom exemplo, de construção de conjuntos numéricos. Peano usou três conceitos primitivos: o *zero*, o *número natural* e a relação *é sucessor de*, cujas notações são, respectivamente: 0, a e a^+. E, para caracterizá-los, formulou os seguintes axiomas, onde $\mathbb{N}$ é considerado como o conjunto dos números naturais.

P_1 : Zero é um número natural, ou seja, $0 \in \mathbb{N}$.

P_2 : Se a é natural, então a tem um único sucessor que também é natural, ou seja, se $a \in \mathbb{N}$, então $a^+ \in \mathbb{N}$. O elemento a^+ é chamado sucessor de a.

P_3 : O zero não é sucessor de nenhum número natural, ou seja, se $a \in \mathbb{N}$, então $a^+ \neq 0$, para todo $a \in \mathbb{N}$.

P_4 : Dois naturais que têm sucessores iguais são iguais, ou seja, se $a^+ = b^+$, então $a = b$.

P_5 : Seja S um conjunto de números naturais. Se S possui o zero e o sucessor de todo elemento de S, então esse conjunto possui todos os números naturais, ou seja, Se $S \subset \mathbb{N}$ e $0 \in S$, com $a \in S$, então $a^+ \in S$, então $S = \mathbb{N}$.

A Propriedade P_1 garante que o conjunto $\mathbb{N}$ é não vazio. Pela Propriedade P_4, segue que se $a \neq b$, então $a^+ \neq b^+$. A Propriedade P_5 é chamada princípio de indução completa.

Proposição 3.1.1. *Se $a \in \mathbb{N}$, então $a^+ \neq a$.*

Demonstração. Seja $S = \{a \in \mathbb{N} : a^+ \neq a\}$. Por (3), segue que $0 \in S$. Se $a \in S$, então $a^+ \in S$. Por (5), segue que $S = \mathbb{N}$, ou seja, para todo $a \in \mathbb{N}$, segue que $a^+ \neq a$. Pela Propriedade P_5, segue que $S = \mathbb{N}$. □

Proposição 3.1.2. *Se $b \in \mathbb{N}$, onde $b \neq 0$, então existe $a \in \mathbb{N}$ tal que $a^+ = b$.*

Demonstração. Seja $S = \{0\} \cup \{y \in \mathbb{N} : \ y \neq 0 \text{ e } x^+ = y\}$. Assim, $0 \in S$, e portanto, $0^+ \in S$. Agora, se $a \in S$ e $a \neq 0$, então $a^+ = (b^+)^+$. Pela Propriedade P_5, segue que $S = \mathbb{N}$. □

Proposição 3.1.3. *(Primeiro princípio de indução completa) Se para todo número natural n está associado uma afirmação $P(n)$ tal que*

1. *$P(0)$ é verdadeira, e*
2. *Se $P(k)$ é verdadeira, então $P(k^+)$ é verdadeira,*

então $P(n)$ é verdadeira, para todo $n \in \mathbb{N}$.

Demonstração. Seja $S = \{n \in \mathbb{N} : P(n) \text{ é verdadeira}\}$. Pela Propriedade P_5, segue que $S = \mathbb{N}$. □

3.1.1 Operações

Nesta seção, apresentamos as operações de adicão (soma) e de multiplicação (produto) dos números naturais.

Definição 3.1.1. *A adição em $\mathbb{N}$ é definida sob as seguintes condições:*

1. *$a + 0 = a$, para todo $a \in \mathbb{N}$.*
2. *$a + b^+ = (a + b)^+$, para todo $a, b \in \mathbb{N}$.*

Se $a + b = c$, então a e b são chamadas de parcelas e c a soma.

Agora, adotando, $0^+ = 1$, $1^+ = 2$, $\cdots$, segue que

$$\begin{aligned} &1 + 1 = 1^+0^+ = (1 + 0)^+ = 1^+ = 2. \\ &1 + 2 = 1 + 1^+ = (1 + 1)^+ = 2^+ = 3. \\ &\vdots \\ &r + 1 = r + 0^+ = (r + 0)^+ = r^+, \text{ para todo } r \in \mathbb{N}. \end{aligned}$$

Além disso, para todo $a, b \in \mathbb{N}$, obtemos as seguintes propriedades.

1. $0 + a = a$, para todo $a \in \mathbb{N}$. De fato: se $a = 0$, então $0 + 0 = 0$, por definição. Se $a \neq 0$, então existe $b \in \mathbb{N}$ tal que $0 + a = 0 + b^+ = (0 + b)^+ = b^+ = a$.

2. $a + 1 = a^+$, para todo $a \in \mathbb{N}$. De fato, $a + 1 = a + 0^+ = (a + 0)^+ = a^+$.

3. Se $a + b = 0$, então $a = b = 0$. De fato, se $b \neq 0$, então existe $u \in \mathbb{N}$ tal que $b = u^+$. Assim, $a + b = a + u^+ = (a + u)^+ = 0$, o que é um absurdo. Portanto, $b = 0$, e assim, $a = 0$.

Agora, para todo $a, b, c \in \mathbb{N}$, obtemos as seguintes propriedades.

1. $a + (b + c) = (a + b) + c$ (associativa). *Prova:* Por indução sobre c. Para $c = 0$, segue que $a + (b + c) = (a + b) + 0$. Agora. suponhamos que $(a + b) + r = a + (b + r)$. Assim, $(a + b) + r^+ = [(a + b) + r]^+ = [a + (b + r)]^+ = a + (b + r)^+ = a + (b + r^+)$, Assim, $(a + b) + c = a + (b + c)$, para todo $a, b, c \in \mathbb{N}$. o que prova o resultado.

2. $a + b = b + a$ (comutativa). *Prova:* Por indução sobre b. Para $b = 0$, segue que $a + 0 = a = 0 + a$. Agora, supondo que $a + r = r + a$, segue que $a + r^+ = (a + r)^+ = (r + a)^+$. Assim, $a + b = b + a$, para todo $a, b \in \mathbb{N}$, o que prova o resultado.

3. $a + 0 = a$ (0 é o elemento neutro da adição). *Prova:* Segue diretament da Definição 3.1.1.

4. Se $a + b = a + c$ (Lei do cancelamento). *Prova:* Por indução sobre a. Para $a = 0$, segue que $0 + b = 0 + c$, ou seja, $b = c$. Agora, suponhamos que $r + b = r + c$ implica que $b = c$. Assim, se $r^+ + b = r^+ + c$, então $b + r^+ = c + r^+$. Logo, $(b + r)^+ = (c + r)^+$. Por (4), segue que $b = c$, o que prova o resultado.

5. $a + 1 = 1 + a$. *Prova:* Por indução sobre a. Se $a = 0$, então $0 + 1 = 0 + 0^+ = (0 + 0)^+ = 0^+ = 1 = 1 + 0$. Agora, suponhamos que $1 + r = r + 1 = r^+$. Assim, $1 + r^+ = 1 + (r + 1) = (1 + r) + 1 = r^+ + 1$, o que prova o resultado.

Além disso,

1. O elemento 0 é único. De fato: suponhamos que existam dois elementos neutros 0_1 e 0_2. Assim, $a = a + 0_1 = a + 0_2$, para todo $a \in \mathbb{N}$. Pela Lei do Cancelamento, segue que $0_1 = 0_2$. Portanto, 0 é o único elemento neutro da adição.

2. Se $a + b = 1$, então $a = 0$ ou $b = 0$. De fato: se $b \neq 0$, então existe $u \in \mathbb{N}$ tal que $a + b = a + u^+ = (a + u)^+ = 1 = 0^+$. Assim, $a + u = 0$, e portanto, $a = u = 0$.

Definição 3.1.2. *A multiplicação (produto) em* $\mathbb{N}$ *é definida sob as seguintes condições:*

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

2. $a.b^+ = ab + a$, *para todo* $a, b \in \mathbb{N}$.

Se $ab = c$, *então* a *e* b *são os fatores e* c *o produto.*

Assim,

$$1.1 = 1.0^+ = 1.0 + 1 = 0 + 1 = 1$$
$$1.2 = 1.1^+ = 1.1 + 1 = 1 + 0^+ = (1 + 0)^+ = 1^+ = 2$$
$$2.2 = 2.1^+ = 2.1 + 2 = 2 + 2 = 2 + 1^+ = (2 + 1)^+ = 3^+ = 4.$$

Além disso, para todo $a \in \mathbb{N}$, segue que

1. $0.a = 0$. A prova é por indução sobre a. Se $a = 0$, por definição o resultado segue. Agora, suponhamos que $0.r = 0$. Assim, $0.r^+ = 0.r + 0 = 0 + 0 = 0$, o que prova o resultado.

2. $1.a = a$. A prova é por indução sobre a. Se a=0, por definição, segue que $1.0 = 0$. Agora, suponhamos que $1.r = r$. Assim, $1.r^{=}1.r + 1 = r + 1 = r^+$, o que prova o resultado.

Parra todo $a, b, c \in \mathbb{N}$, obtemos as seguintes propriedades.

1. $a(bc) = (ab)c$ (Associativa). A prova é por indução sobre c. Se $c = 0$, então $a(bc) = a(b.0) = 0 = (ab)0$. Agora, suponhamos que $a(br) = (ab)r$. Assim, $a(br^+) = a(br + b) = abr + ab = (ab)r^+$. Portanto, $a(bc) = (ab)c$, para todo $a, b, c \in \mathbb{N}$.

2. $ab = ba$ (Comutativa). A prova é por indução sobre b. Para $b = 0$, segue que $a0 = 0 = 0a$. Agora, suponhamos que $ar = ra$. Assim, $ar^+ = ar+a = ra+a = r^+a$. Portanto, $ab = ba$, para todo $a, b \in \mathbb{N}$.

3. $a.1 = a$ (1 é o elemento neutro). A prova é por indução sobre a. Para $a = 0$, segue que $0 = a.1 = a$. Agoa, suponhamos que $r.1 = r$. Assim, $r^+.1 = 1.r^+ = 1.r + r = r + 1 = r^+$. Portanto, $a.1 = 1.a$, para todo $a \in \mathbb{N}$.

4. Se $ab = 0$, então $a = 0$ ou $b = 0$ (Lei do anulamento do produto). De fato, se $b \neq 0$, então $b = r^+$, onde $r \in \mathbb{N}$. Logo, $0 = ab = ar^+ = ar + a$. Assim, $ar = a = 0$. De forma análoga procedemos com a.

5. Se $ac = bc$, com $c \neq 0$, então $a = b$ (Lei do cancelamento do produto). A prova é por indução sobre c. Se $c = 1$, então, por (3), segue que $ac = bc$ implica que $a = b$. Agora, suponhamos que $ar = br$. Assim, $ar^+ = br^+$, ou seja, $ar + a = br + b$. Como $ar = br$, segue que $ar + a = ar + b$. Assim, $a = b$.

6. Se $ab = 1$, então $a = 1$ ou $b = 1$. De fato, se $b \neq 1$, então $b = r^+$, onde $r \geq 1$ e $r \in \mathbb{N}$. Logo, $1 = ab = ar^+ = ar + a$. Como $ar + a = 1$ implica que $a(r + 1) = 1$. Assim, $a = 1$ e $r = 0$, o que é um absurdo.

7. $(a + b)c = ac + bc$ e $a(b + c) = ab + ac$ (Distributiva). A prova é por indução sobre c. Se $c = 0$, então $(a+b).0 = 0 = a.0+b.0$. Agora, suponhamos que $(a+b)r = ar+br$. Assim, $(a + b)r^+ = (a + b)r + (a + b) = (ar + br) + (a + b) = (ar + a) + (br + b) = ar^+ + br^+$. Portanto, $(a + b)c = ac + bc$, para todo $a, b, c \in \mathbb{N}$. O caso $a(b + c) = ab + ac$, para todo $a, b, c \in \mathbb{N}$, procedemos de modo análogo usando indução sobre a.

3.1.2 Relação de ordem

A relação $\leq$ sobre $\mathbb{N}$ é definida do seguinte modo. Sejam $a, b \in \mathbb{N}$.

1. Se $b = a + u$, com $u \in \mathbb{N}$, então $a \leq b$.
2. Se $b = a + v$, com $v \neq 0$, então $a < b$.

As relações $\geq$ e $>$ são definidas, respectivamente, por:

1. $a \geq b$ se, e somente se, $b \leq a$, e
2. $a > b$ se, e somente se, $b < a$.

Para todo $a, b, c \in \mathbb{N}$, obtemos as seguintes propriedades.

1. $a \leq a$ (reflexiva). *Prova:* Segue do fato que $a = a + 0$.
2. Se $a \leq b$ e $b \leq a$, então $a = b$ (anti-simétrica). *Prova:* Por hipótese, segue que $b = a + u$ e $a = b + v$, com $u, v \in \mathbb{N}$. Assim, $a = a + u + v$, ou seja, $u + v = 0$. Logo, $u = v = 0$, e portanto, $a = b$.
3. Se $a \leq b$ e $b \leq c$, então $a \leq c$ (transitiva). *Prova:* Por hipótese, $b = a + u$ e $c = b + v$, com $u, v \in \mathbb{N}$. Assim, $c = a + (u + v)$, ou seja, $a \leq c$.
4. Se $a \leq b$, então $a + c \leq b + c$. *Prova:* Por hipótese, segue que $b = a + u$, com $u \in \mathbb{N}$. Logo, $b + c = a + c + u$, e portanto, $a + c \leq b + c$.
5. Se $a \leq b$, então $ac \leq bc$. *Prova:* Por hipótese, segue que $b = a + u$, onde $u \in \mathbb{N}$. Assim, $bc = (a + u)c = ac + uc$, e portanto, $ac \leq bc$.

Teorema 3.1.1. *(Lei da Tricotomia) Se $a, b \in \mathbb{N}$, então vale uma e somente uma das relações: $a = b$, $a < b$ ou $a > b$.*

Demonstração. Supondo que $a \neq b$, segue que $a > b$ ou $a < b$, ou seja, $a = b + u$, com $u \neq 0$, ou $b = a + v$, com $v \neq 0$. Se ocorressem as duas possibilidades, segue que $a = a + (u + v)$, e assim, $u + v = 0$ implica que $u = v = 0$, o que é um absurdo. Portanto, $a = b$, $a > b$ ou $a < b$. de modo único. □

Um número n é par se $n = 2k$ e n é impar se $n = 2k + 1$, onde $k \in \mathbb{N}$.

3.1.3 Sistema de numeração decimal

Ao escrevermos um número, precisamos reconhecer em que base de numeração estamos trabalhando. Embora seja usual o tratamento com a base decimal, outras bases podem ser consideradas. Na computação, é usada a base binária, na divisão da hora usamos a base sexagesimal (60 minutos), e na medida da circunferência em 360 graus.

Em um sistema posicional com base b, onde b é um natural maior que 1, todo número natural n pode ser escrito de modo único na forma

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0,$$

onde $0 \leq a_i < n$, para todo i. Esse número é representado por

$$(a_n a_{n-1} \ldots a_1 a_0)_b.$$

Assim, são necessários a algarismos $\{0, 1, 2, \ldots, a-1\}$ para descrevermos os números na base a.

O sistema de numeração decimal, também chamado de sistema de numeração decimal posicional, é um conjunto de regras que são utilizadas para representar os números, sendo escritos na base 10.

A base é a quantidade de símbolos que servem para representar os números. Portanto, na base 10 são utilizados os 10 algarismos: $0, 1, 2, 3, 4, 5, 6, 7, 8$ e 9. A ordem é a posição na qual o algarismo ocupa em um número, sendo analisado da direita para a esquerda. Assim, dado um número natural n, podemos escrevê-lo na base 10 como

$$n = (a_n a_{n-1} \ldots a_1 a_0)_{10} = a_0 10^0 + a_1 10^1 + a_2 10^2 + \cdots + a_n 10^n,$$

onde $a_0, a_1, \ldots, a_n$ são números variando de $0, 1, 2, \ldots, 9$, e a_0 é chamado de unidade, a_1 é chamado de dezena, a_2 é chamado de centena, a_3 é chamado de unidade de milhar, a_4 é chamado de dezena de milhar, a_5 é chamado de centena de milhar, a_6 é chamado de unidade de milhão, a_7 é chamado de dezena de milhão, a_8 é chamado de centena de milhão, a_9 é chamado de unidade de bilhão, e assim, por diante. Por exemplo, o número 1235 é escrito como $1235 = 5.10^0 + 2.10^1 + 3.10^2 + 5.10^3$.

Teorema 3.1.2. *Seja $b > 1$ um inteiro. Se $n \in \mathbb{N}$, então n pode ser escrito de modo único na forma*

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b^1 + a_0 a^0,$$

onde $0 \leq a_i \leq b$, para $i = 0, 1, \ldots, k$ e $a_k \neq 0$.

Demonstração. Se $n = 1$, então $k = 0$ e $a_0 = 1$. Agora, suponha por hipótese de inducção, a validade do teorema para todo $q \in \mathbb{N}$ tal que $0 < q < n$. Pelo algoritmo da divisão, segue que existem únicos $q_1, a_0 \in \mathbb{N}$ tal que $n = bq_1 + a_0$. Como n e b são estritamente positivos com $b > 1$ e $a_0 \geq 0$, segue que $q_1 < n$. Por hipótese de indução, segue que existema$_{k+1}, a_k, \ldots, a_1$

menores que b e $a_{k+1} \neq 0$ tal que $q_1 = a_{k+1}b^k + a_k b^{k-1} + \ldots + a_2 b + a_1$. Portanto, $n = a_{k+1}b^{k+1} + a_k b^k + \ldots + a_1 b + a_0$. A unicidade segue da unicidade do algoritmo da divisão. □

Assim, todo número $n \in \mathbb{N}$ pode ser escrito em uma base b, ou seja,

$$n = a_0 + a_1 b + a_2 b^2 + \cdots + a_n b_r^r,$$

onde $r \geq 0$ e $a_i = 0, 1, 2, \ldots, b-1$, e escrevemos $n = (a_r a_{r-1} \ldots a_1 a_0)_b$. Quando a base é 10 escrevemos simplesmente por $n = a_r a_{r-1} \ldots a_1 a_0$. Observamos ainda que são necessários b números a_i' para escrever qualquer número na base b. Na base 2 usamos os algarismos 0 e 1. Na base 3 usamos os algarismos 0, 1 e 2. Na base 10 usamos os algarismos 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9. Para bases maiores que 10, usamos letras para representar os algarismos maiores ou iguais a 10. Por exemplo, na base 12, usamos os algarismos 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9 e as letras A, B e C, que representam os números decimais 10, 11 e 12, respectivamente. Na base 16, ou seja, base hexadecimal, usamos os algarismos 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9 e as letras A, B, C, D, E e F que representam os números decimais 10, 11, 12, 13, 14 e 15, respectivamente.

Exemplo 3.1.1. *Se* $x = 425$*, então* $425 = 26.16 + 9$ *e* $26 = 1.16 + 10$*. Assim,* $x = 425 = 16.26 + 9 = (1.16 + 10).16 + 9 = 1.16^2 + 10.16 + 9$*, ou seja,* $x = (1(10)9)_{16}$*, para não confundir com* $(1109)_{16} = 1.16^3 + 1.16^2 + 0.16 + 9 = 4361$ *que é diferente de* 425*.*

Se $n < 0$, então $n = -m$, com $m > 0$. Assim, a representação de um número negativo n é dada por $n = -(a_0 + a_1 b + a_2 b^2 + \cdots + a_n b_r^r) = -(a_r a_{r-1} \ldots a_1 a_0)_b$. O número b pode ser escrito com $b = (10)_b$, e em geral, $b^n = (10 \ldots 0)_b$ com n zeros.

Exemplo 3.1.2. *A expansão decimal do número inteiro que tem* $(101011111)_2$ *como sua expansão binária é dada por* $(101011111)_2 = 1.2^0 + 1.2^1 + 1.2^2 + 1.2^3 + 1.2^4 + 0.2^5 + 1.2^6 + 0.2^7 + 1.2^8 = 351$*.*

Exemplo 3.1.3. *O número* 2102 *na base ternária é dada por* $(2102)_3 = 2 + 0.3 + 1.3^2 + 2.3^3 = 65$ *e o número* 1001 *na base binária é dada por* $(10001)_2 = 1 + 0.2 + 0.2^2 + 0.2^3 + 1.2^4 = 17$*. O número* 351 *na base binária é dada por* $(101011111)_2$*.*

Exemplo 3.1.4. *A expansão decimal do número inteiro que tem* $(175627)_{10}$ *como sua expansão na base* 10 *é dada por* $(175627)_{10} = 7.2^0 + 2.10^1 + 6.10^2 + 5.10^3 + 7.10^4 + 1.10^5 = 175627$*.*

Ao escolher 2 como base, temos as expansões binárias dos números inteiros. Na notação binária, cada dígito é 0 ou 1. Em outras palavras, a expansão binária de um número inteiro é uma cadeia de bits. As expansões binárias são usadas por computadores para representar e executar aritméticas com números inteiros.

A prova do Teorema 3.1.2 fornece um processo prático para determinar a representação de um número n em uma base b.

1. Primeiro dividimos n (escrito na base 10 por b) para obter um quociente q_0 e resto a_0, ou seja,

   $$n = bq_0 + a_0, \quad \text{onde} \quad 0 \leq a_0 < b.$$

   Assim, obtemos o primeiro dígito à direta na expansão de n na base b.

2. Em seguida, dividimos q_0 por b para obter um quociente q_1 e resto a_1, ou seja,

$$q_0 = bq_1 + a_1, \quad \text{onde} \quad 0 \leq a_1 < q_1.$$

   Assim, obtemos o segundo dígito à direta na expansão de n na base b.

3. Continuando nesse processo, dividindo sucessivamente os quocientes por b, obtemos os demais dígitos na base b como os restos.

4. O processo termina quando obtemos um quociente igual a 0.

Exemplo 3.1.5. *A expansão do número* 211 *na base* 4 *é dada por:*

1. $211 = 4.52 + 3$, *onde* $a_0 = 3$.

2. $52 = 4.13 + 0$, *onde* $a_1 = 0$.

3. $13 = 4.3 + 1$, *onde* $a_2 = 1$.

4. $= 4.0 + 3$, *onde* $a_3 = 3$.

Desse modo, $211 = 52.4 + 3 = (13.4 + 0).4 + 3 = 13.4^2 + 0.4 + 3 = (3.4 + 1).4^2 + 0.4 + 3 = 3.4^3 + 1.4^2 + 0.4 + 3 = (3103)_4$.

Exemplo 3.1.6. *A expansão do número* 12345 *na base* 8 *é dada por:*

1. $12345 = 8.1543 + 1$, *onde* $a_0 = 1$.

2. $1543 = 8.192 + 7$, *onde* $a_1 = 7$.

3. $192 = 8.24 + 0$, *onde* $a_2 = 0$.

4. $24 = 8.3 + 0$, *onde* $a_3 = 0$.

5. $3 = 8.0 + 3$, *onde* $a_4 = 3$.

Desse modo, $12345 = 1543.8+1 = (192.8+7).8+1 = 192.8^2+7.8+1 = (24.8+0)8^2+7.8+1 = 24.8^3 + 0.8^2 + 7.8 + 1 = (3.8 + 0).8^3 + 0.8^2 + 7.8 + 1 = 3.8^4 + 0.8^3 + 0.8^2 + 7.8 + 1 = (30071)_8$.

Agora, apresentamos algoritmos para determinar a soma, subração e multiplicação (produto) e divisão em uma determinada base, que são extremamamente importantes na aritmética computacional. Das 4 operações aritméticas básicas, a soma é a mais simples. Na base 10 usamos o seguinte algoritmo.

1. Basicamente, alinhamos as parcelas a serem somas e executamos a adição algarismo a algarismo.

2. Da direita para a esquerda. O detalhe está no vai-um.

3. Se a soma de dois algarismos alinhados fornece um valor maior que 10, pegamos apenas o algarismo menos significativo

4. O mais significativo é carregado para a esquerda e somado com os próximos algarismos.

Exemplo 3.1.7. *A soma de* $x = 12345$ *e* $y = 56789$ *na base* 10 *é dada por*

$$\begin{array}{cccccc} & & 1 & 1 & 1 & \\ & 1 & 2 & 3 & 4 & 5 \\ + & 5 & 6 & 7 & 8 & 9 \\ \hline & 6 & 9 & 1 & 3 & 4 \end{array}$$

ou seja, $x + y = 69134$.

Este algoritmo da soma pode ser generalizado para outras bases. Para uma base b qualquer o algoritmo é dado da seguinte maneira.

1. Alinham-se as parcelas.

2. Somam-se os algarismos, um a um, da direita para a esquerda.

3. Se a soma de dois algarismos alinhados resulta em um valor com um único algarismo (na base b) e este é colocado no resultado (alinhado aos algarismos somados).

4. Caso contrário, coloca-se o algarismo menos significativo no resultado e vai um.

5. Caso a soma de dois algarismos resulte em vai-um, este deverá ser somado aos próximos algarismos.

O vai-um ocorre quando a soma dos coeficientes a_i e b_i de b^i é maior que b, ou seja, $a_i + b_i > b$. Neste caso, $a_i + b_i < 2b$, e assim, $a_i + c_i = b + d_i$, com $0 \leq d_i < b$. Observe que $(a_i + b_i)b^i = (b + d_i)b^i = 1.b^{i+1} + d_i b_i$, e portanto, ocorre uma potência aos coeficientes de b^{i+1}, o que justifica o vai-um.

Exemplo 3.1.8. *Se* $x = (22)_3$ *e* $y = (120)_3$, *então* $x = 0.3^2 + 2.3 + 2.3^0$ *e* $y = 1.3^2 + 2.3 + 03^0$. *Somando os coeficientes, segue que* $0 + 1 = 1$, $2 + 2 = (11)_3$ *e* $2 + 0 = 2$. *Assim,* $x + y = 1.3^2 + ((11)_3)3 + 2 = 1.3^2 + (1.3 + 1).3 + 2 = 1.3^2 + 1.3^2 + 1.3 + 2 = (1 + 1).3^2 + 1.3 + 2 = (212)_3$, *ou seja,*

$$\begin{array}{cccc} & 1 & & \\ & 0 & 2 & 2 \\ + & 1 & 2 & 0 \\ \hline & 2 & 1 & 2 \end{array}$$

Observamos que usamos a seguinte tábua para a soma.

+	0	1	2
0	0	1	2
1	1	2	10
2	2	10	11

Exemplo 3.1.9. *A soma de* $x = (10110)_2$ *e* $y = (01011)_2$ *na base* 2 *é dada por*

$$\begin{array}{cccccc} 1 & 1 & 1 & 1 & & \\ & 1 & 0 & 1 & 1 & 0 \\ + & 0 & 1 & 0 & 1 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 & 1 \end{array}$$

ou seja, $x + y = (100001)_2$.

Exemplo 3.1.10. *A soma de* $x = (12535)_8$ *e* $y = (33614)_8$ *na base* 8 *é dada por*

$$\begin{array}{cccccc} & & 1 & & 1 & \\ & 1 & 2 & 5 & 3 & 5 \\ + & 3 & 3 & 6 & 1 & 4 \\ \hline & 4 & 6 & 3 & 5 & 1 \end{array}$$

ou seja, $x + y = (46351)_8$.

A seguir, apresentamos o agoritmo para calcular a soma binária. Para isso, sejam

$$x = (a_n a_{n-1} \dots a_1 a_0)_2 \quad \text{e} \quad y = (b_n b_{n-1} \dots b_1 b_0)_2.$$

Para que x e y tenham $n + 1$ bits, colocamos bits iguais a 0 no começo dessas expressões.

1. Para somar x e y, primeiro somamos seus bits mais à direita. Assim,

   $$a_0 + b_0 = 2.c_0 + r_0,$$

   onde s_0 é o dígito mais a direita na expansão binária de $x + y$ e c_0 é 0 ou 1.

2. Adicione o próximo par de bits e o transporte, ou seja,

   $$a_1 + b_1 + c_0 = 2.c_1 + r_1,$$

   onde r_1 é próximo bit (da direita) na expansão binária de $x + y$ e c_1 é o transporte.

3. Continuando esse processo, adicinando os bits correspondentes nas duas expansões binárias e o transporte, para determinar o próximo bit sempre da direita para a esquerda na expansão binária de $x + y$.

4. Na última etapa, adicione a_{n-1},b_{n-1} e c_{n-2} para obter $1.c_{n-1} + r_{n-1}$.

5. O bit que termina a soma é $r_n = c_{n-1}$.

6. Este procedimento fornece a expansão binária da soma, ou seja, $x + y = (r_n r_{n-1} r_{n-2} \dots r_1 r_0)_2$.

Exemplo 3.1.11. *A soma de* $a = (1110)_2$ *e* $b = (1011)_2$ *é dada por*

$$a_0 + b_0 = 2.0 + 1,$$

onde $c_0 = 0$ *e* $r_0 = 1$*. Agora, como*

$$a_1 + b_1 + c_0 = 1 + 0 + 1 = 2.1 + 0,$$

onde $c_2 = 1$ *e* $r_2 = 0$*. Finalmente, como*

$$a_3 + b_3 + c_2 = 1 + 1 + 1 = 2.1 + 1.$$

segue que $c_3 = 1$ *e* $r_3 = 1$*. Assim,* $r_4 = c_3 = 1$*. Portanto,* $r = a + b = (11001)_2$.

A subtração de números em uma mesma base é realizada através da subtração dos respectivos coeficientes na base b. Quando o coeficiente a ser subtraido é maior, é preciso subtrair 1 do coeficiente de potência de b imediatamente maior para acrescentar naquela que tem falta. Desse modo, $a_i b^i = (a_i - 1)b^i + b.b^{i-1}$, ou seja, ficamos com coeficiente $a_i - 1$ para b^i, e no nível b^{i-1}, ficamos com coeficiente $b = (10)_b$ com a soma com a_{i-1}, totalizando $(1a_{i-1})_b$. Assim, $(1a_i)_b \geq b > c_{i-1}$, sendo possível efetuar a subtração.

Exemplo 3.1.12. *Se* $x = (1011)_2 = 1.2^3 + 0.2^2 + 1.2 + 1$ *e* $y = (101101)_2 = 1.2^5 + 0.2^4 + 1.2^3 + 1.2^2 + 0.2 + 1$*, então* $x < y$*. Observamos que para os coeficientes de* 2^1*, é necessário retirar* 1 *do coeficiente de* 2^2 *para fazer* $y - x$*.*

$$\begin{array}{cccccccc} & 1 & 0 & 1 & 1 & 0 & 1 \\ - & & & 1 & 0 & 1 & 1 \\ \hline \end{array}$$

Assim, $1.2^2 = 2.2 = (10)_2.2$*, e portanto,* $y - x = 1.2^5 + 0.2^4 + 1.2^3 + 1.2^2 + 0.2 + 1 - (1.2^3 + 0.2^2 + 1.2 + 1) = 1.2^5 + 1.2^3 + (10)_2.2 + 1 - (1.2^3 + 1.2 + 1) = 1.2^5 + (1-1).2^3 + ((10)_2 - 1).2 + (1-1) = 1.2^5 + 1.2 = (100010)_2$*, ou seja, no processo prático se empresta um e se subtraiu um, como a seguir.*

$$\begin{array}{cccccccc} & 1 & 0 & 1 & {}^{0}\not{1} & {}^{1}0 & 1 \\ - & & & 1 & 0 & 1 & 1 \\ \hline & 1 & 0 & 0 & 0 & 1 & 0 \end{array}$$

Assim, $y - x = (100010)_2$.

Exemplo 3.1.13. *Sejam* $x = (1012)_3 = 1.3^3 + 0.3^2 + 1.3 + 2$ *e* $y = (121)_3 = 1.3^2 + 2.3 + 1$*. Assim,*

$$\begin{array}{cccc} & 0 & 1 & 2 \\ - & 1 & 2 & 1 \\ \hline \end{array}$$

Para fazer a diferença $x - y$*, observamos que devemos emprestar* 1 *do coeficiente* 3^3 *para o coeficiente* 3^2 *de* x*, uma vez que este coeficiente é menor que o coeficiente correspondente de* y*.*

Em seguida, utilizamos do mesmo método para as potências inferiores. Desse modo,

$$\begin{array}{cccc} 1^{\rightarrow} & 0 & 1 & 2 \\ - & 1 & 2 & 1 \\ \hline \end{array} \Rightarrow \begin{array}{cccc} & (10)_3^{\rightarrow} & 1 & 2 \\ - & 1 & 2 & 1 \\ \hline \end{array} \Rightarrow \begin{array}{ccc} 2 & (11)_3 & 2 \\ - \; 1 & 2 & 1 \\ \hline 1 & 2 & 1 \end{array}$$

e assim, $x - y = (121)_3$.

Para a multiplicação binária, considere dois números inteiros x e y com n bits. Assim

$$xy = a(b_0 2^0 + b_1 2^1 + \cdots + b_{n-1} 2^{n-1}) = a(b_0 2^0) + a(b_1 2^1) + \cdots + a(b_{n-1} 2^{n-1}).$$

Pela distributiva, segue que $a_i b^i b_k b^k = (a_i b_k) b^{i+k}$. Como $0 \leq a_i, c_k < b$, segue que $0 \leq a_i b_k < b^2$. Assim, $a_i b_k = qb + d_{i+k}$, $0 \leq d_{i+k}, q < b$, e portanto, $a_i b^i . b_k b^k = (qb + d_{i+k}) b^{i+k} = qb^{i+k+1} + d_{i+k} b^{i+k}$. Portanto, acrecesta-se q ao coeficiente da potência b^{i+k+1} e o coeficiente de b^{i+k} é d_{i+k} que é o resto da divisão de $a_i . b_k$ por b. Um algoritmo para o produto na base binária é dado por.

1. Primeiro, observe que se $b_j = 1$, então $xb_j = x$, e se $b_j = 0$, então $xb_j = 0$.
2. Cada vez que multiplicamos um termo por 2, mudamos sua expansão binária uma casa para à esquerda e adicionamos zero ao final da expansão.
3. Assim, podemos obter $(xb_j)2^j$ pela substituição da expansão binária de xb_j com j casas à esquerda e pela adição de j bits zero no final desa expansão.
4. Finalmente, obtemos xy pela adição de n números inteiros $xb_j 2^j$, para $j = 0, 1, 2, \ldots, n-1$.

Exemplo 3.1.14. *Sejam* $x = (110)_2$ *e* $y = (101)_2$. *Primeiro,*

$$\begin{aligned} xb_0 . 2^0 &= (110)_2 . 1 . 2^0 = (110)_2 \\ xb_1 . 2^1 &= (110)_2 . 0 . 2^1 = (0000)_2 \\ xb_2 . 2^2 &= (110)_2 . 1 . 2^2 = (11000)_2. \end{aligned}$$

Para encontrar o produto, adicione $(110)_2$, $(0000)_2$ *e* $(11000)_2$ *fazendo uso do algoritmo da soma. Assim,* $xy = (11110)_2$.

A multiplicação em uma base b é dada da seguinte maneira. Se $x = a_s b^s + a_{s-1} b^{s-1} + \cdots + a_1 b + a_0$ e $y = b_j b^j + b_{j-1} b^{j-1} + \cdots + b_1 b + b_0$, então $a_i b^i b_k b^k = (a_i b_k) b^{i+k}$. Como $0 \leq a_i$, $b_k < b$, segue que $0 \leq a_i b_k < b^2$. Logo, $a_i b_k = qb + d_{i+k}$, onde $0 \leq d_{i+k}, q < b$, e desse modo, $a_i b^i b_k b^k = (qb + d_{i+k}) b^{i+k} = q . b^{i+k+1} + d_{i+k} b^{i+k}$. Portanto, devemos acrescentar q ao coeficiente da potência b^{i+k+1} e o coeficiente de b^{i+k} é d_{i+k} é o resto da divisão de $a_i b_k$ por b.

Exemplo 3.1.15. *Agora, consideramos a tábua da adição e multiplicação na base* 4*, ou seja,*

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	10
2	2	3	10	11
3	3	10	11	12

$\bullet$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	10	12
3	0	3	12	21

Sejam $x = (23)_4$ *e* $y = (32)_4$*. Assim,* $2_4.3_4 = (12)_4$ *e* $3_4.3_4 = (21)_4$*. Agora, multiplicando* 23 *por* 32 *na base* 4*, segue que*

$$\begin{array}{cccc} & & 2 & 3 \\ & & \times & 3 & 2 \\ \hline & & 1 & 1 & 2 \\ & 2 & 0 & 1 & + \\ \hline & 2 & 1 & 2 & 2 \end{array}$$

ou seja, $xy = (2122)_4$*. Observamos que* $3_4.3_4 = (21)_4$*, e assim, fica* 1 *3=e vai* 2*. Também,* $3..2_4 + 2_4$ *(*2_4 *que foi) totalizam* $(20)_4$*, e assim por diante.*

Para a divisão consideramos os números $x = (a_n a_{n-1} \dots a_1 a_0)_b$ e $y = (b_n b_{n-1} \dots b_1 b_0)_b$. Para fazer a divisão de x por y, consideramos $x_0 = a_n a_{n-1} \dots a_{n-m-1}$ que seja maior ou igual a y. Caso contrário, consideramos $x_0 = a_n a_{n-1} \dots a_{n-m-2}$ e dividimos x_0 por y. Assim, $x_0 = qy + r$, onde $0 \leq r < c$. Sejam $q = (q_k q_{k-1} \dots q{-}1 q_0)_b$ e $r = (r_s r_{s-1} \dots r_1 r_0)_b$. Agora, juntamos a r o próximo a_j da esquerda para a direita que não aparece em x_0, e assim, obtemos $R = r_s r_{s-1} \dots r_1 r_0 a_j$. Dividindo R por y obtemos q_1' como quociente e resto $R_1 = (d_t d_{t-1} \dots d_1)_b$. Novamente, juntamos a_{j-1} a R_1, e assim, obtemos $R_2 = d_t d_{t-1} \dots d_1 a_{j-1}$. Dividindo R_2 por y obtemos q_2' como quociente e resto $R_3 = (u_v u_{v-1} \dots u_1)_b$. Assim, repetimos o processo até chegar em a_0 e concluir a divisão. Neste caso, o quociente da divisão é dado por $Q = q_k q_{k-1} \dots q_1 q_0 q_1' q_2' \dots q_l'$ e o último resto será o resto.

Exemplo 3.1.16. *Se* $x = 231003$ *e* $y = 302$ *estão na base* 4*, então* $x > y$*. Seja* $x_0 = 2310$*. O quociente da divisão de* 2310 *por* 302 *é* 3*. Assim,* $2310_4 - 3_4.(302)_4 = (132)_4$*. Agora, juntando* $a_1 = 0$ *a* 132*, obtemos* 1320*, e dividimos novamente por* 302*, e assim por diante. Este processo é resumido na seguinte tabela:*

$$\begin{array}{cccccccc} & 2 & 3 & {}^{1}1 & {}^{1}0 & 0 & 3 & \quad | \; 3 \quad 0 \quad 2 \\ & & & & & & & \quad \overline{\qquad\qquad} \\ - & 2 & 1^{1} & 1^{1} & 2 & \downarrow & \downarrow & \quad 3 \quad 2 \quad 1 \\ & 0 & 1 & 3 & 2 & 0 & \downarrow & \\ & - & 1 & 2 & 1 & 0 & \downarrow & \\ & & 0 & 1 & 1 & 0 & 3 & \\ & & & - & 3 & 0 & 2 & \\ & & & & 2 & 0 & 1 & \end{array}$$

Para fazer conversão de um número n de uma base b para uma base c, um método é escrever

n na base decimal e aplicar divisões sucessivas por c. Considerando os restos $c_0, c_1, \ldots, c_s$ das divisões, segue que $n = (c_0, c_1, \ldots, c_s)_c$. No entanto, quando uma base é uma potência da outra, existe um processo prático para a conversão de um número de uma base à outra.

Para a conversão de um número da base 4 para a base binária, é suficiente converter cada dígito do número dado para a base binária, obtendo uma sequência de 2 dígitos de $0^{prime}s$ e $1's$, guardando suas posições. Reciprocamente, para a conversão de um número da base binária para a base 4, é suficiente agrupar os dígitos de 2 em 2 da direita para à esquerda e passar cada grupo para a base 4, guardando as posições dos números obtidos.

Exemplo 3.1.17. *Seja* $x = (1010111)_2$. *Como* $2^2 = 4$, *para escrever* x *na base* 4 *agrupamos os seus dígitos de* 2 *em* 2 *da direita para à esquerda, ou seja,* $(1010111)_2 = ((1)_2(01)_2(01)_2(11)_2)_4$. *Como* $(1)_2 = (1)_4$, $(01)_2 = (1)_4$ *e* $(11)_2 = (3)_4$, *seque que* $x = (1113)_4$.

Para a conversão de um número da base octal (base 8) para a base binária, é suficiente converter cada dígito do número dado para a base binária, obtendo uma sequência de 3 dígitos de $0's$ e $1's$, guardando suas posições. Reciprocamente, para a conversão de um número da base binária para a base octal, é suficiente agrupar os dígitos de 3 em 3 da direita para à esquerda e passar cada grupo para a base 8, guardando as posições dos números obtidos.

Exemplo 3.1.18. *Seja* $x = (1010111)_2$. *Como* $2^3 = 8$, *para escrever* x *na base octal agrupamos os seus dígitos de* 3 *em* 3 *da direita para à esquerda, ou seja,* $(1010111)_2 = ((1)_2(010)_2(111)_2)_8$. *Como* $(1)_2 = (1)_8$, $(010)_2 = (2)_8$ *e* $(111)_2 = (7)_8$, *seque que* $x = (127)_8$.

Para a conversão de um número da base hexadecimal (base 16) para a base binária, é suficiente converter cada dígito do número dado para a base binária, obtendo uma sequência de 4 dígitos de $0's$ e $1's$, guardando suas posições. Reciprocamente, para a conversão de um número da base binária para a base hexadecimal, é suficiente agrupar os dígitos de 4 em 4 da direita para à esquerda e passar cada grupo para a base 16, guardando as posições dos números obtidos.

Exemplo 3.1.19. *Seja* $x = (1010111)_2$. *Como* $2^4 = 16$, *para escrever* x *na base hexadecimal agrupamos os seus dígitos de* 4 *em* 4 *da direita para à esquerda, ou seja,* $(1010111)_2 = ((0101)_2(0111)_2)_{16}$. *Como* $(0101)_2 = (5)_{16}$ *e* $(111)_2 = (7)_{16}$, *seque que* $x = (57)_{16}$.

Proposição 3.1.4. *Seja* $x = (a_k a_{k-1} \ldots a_1 a_0)_{16}$, *onde* $0 \leq a_i \leq 15$, *a representação de* x *na base* 16. *Se* $a_i = (a_{i3}a_{i2}a_{i1}a_{i0})_2$, *com* $0 \leq a_{ij} \leq 1$, *é a representação de* a_i *na base* 2, *então* $x = (a_{k3}a_{k2}a_{k1}a_{k0} \ldots a_{13}a_{12}a_{11}a_{10}a_{03}a_{02}a_{01}a_{00})_2$.

Demonstração. Se $x = (a_k a_{k-1} \ldots a_1 a_0)_{16}$, com $0 \leq a_i \leq 15$, então $x = a_k 16^k + a_{k-1}16^{k-1} \cdots a_1 16 + a_0$. Agora, como $a_i = (a_{i3}a_{i2}a_{i1}a_{i0})_2$ e $2^4 = 16$, segue que $x = a_{k3}2^{4k+3} + a_{k2}2^{2k+2} + a_{k1}2^{2k+1} + a_{k0}2^{4k} + \cdots + a_{11}2^5 + a_{10}2^4 + a_{03}2^3 + a_{02}2^2 + a_{01}2 + a_{00}$, ou seja, $x = (a_{k3}a_{k2}a_{k1}a_{k0} \ldots a_{13}a_{12}a_{11}a_{10}a_{03}a_{02}a_{01}a_{00})_2$. □

Proposição 3.1.5. *Se* $x = (a_s a_{s-1} \ldots a_1 a_0)_2$, *então* $x = (c_k c_{k-1} \ldots c_1 c_0)_{16}$, *onde* $c_j = (a_{4j+3}2^{4j+3} + a_{4j+2}2^{4j+2} + a_{4j+1}2^{4j+1} + a_{4j}2^{4j})_{16}$.

Demonstração. Seja $x = (a_s a_{s-1} \dots a_1 a_0)_2 = a_2 2^2 + a_{s-1} 2^{s-1} + \cdots + a_7 2^7 + a_6 2^6 + a_5 2^5 + a_4 2^4 + a_3 2^3 + a_2 2^2 + a_1 2 + a_0$. Fazendo o agrupamento de 4 em 4 da direita para à esquerda, segue que

$$\begin{aligned} c_0 &= a_3 2^3 + a_2 2^2 + a_1 2 + a_0 \\ c_1 &= a_7 2^7 + a_6 2^6 + a_5 2^5 + a_4 2^4 \\ &\vdots \\ c_j &= a_{4j+3} 2^{4j+3} + a_{4j+2} 2^{4j+2} + a_{4j+1} 2^{4j+1} + a_{4j} 2^{4j}, \end{aligned}$$

ou seja, $x = (c_k c_{k-1} \dots c_1 c_0)_{16}$. □

Exemplo 3.1.20. *Seja* $x = (2(15)9)_{16}$. *Como* $2 = (0012)_2$, $15 = (1111)_2$ *e* $9 = (1001)_2$, *segue que* $x = (001011111001)_2$. *Agora, seja* $x = (0110001110111101)_2$. *Como* $(0110)_2 = 6_{16}$, $(0011)_2 = 3_{16}$, $(1011)_2 = B_{16}$ *e* $(1101)_2 = D_{16}$, *segue que* $x = (63BD)_{16}$.

A expansão de Cantor é uma soma na forma

$$a_n n! + a_{n-1}(n-1)! + \cdots + a_2 2! + a_1 1!.$$

3.1.4 Exercícios

1. Sejam os conjuntos $A = \{x \in \mathbb{N} : x = 24n, \text{ com } n \in \mathbb{N}\}$ e $B = \{n \in \mathbb{N} : 3n + 4 < 2n + 9\}$. Determine $A \cup B$ e $A \cap B$.

2. Representar analiticamente cada conjunto abaixo.

   (a) Conjunto $\mathbb{N}$ dos números naturais.

   (b) Conjunto P dos números naturais pares.

   (c) Conjunto I dos números naturais ímpares.

   (d) Conjunto E dos números naturais menores que 16.

   (e) Conjunto L dos números naturais maiores que 11.

   (f) Conjunto R dos números naturais maiores ou iguais a 28.

   (g) Conjunto C dos números naturais que estão entre 6 e 10.

3. Um gavião viu um grupo de pombos, chegou perto deles e disse: Olá minhas 100 pombinhas. Uma delas respondeu: Não somos 100 não meu caro gavião, seremos 100, com nós, mais dois tantos de nós e mais você meu caro gavião. Quantos pombos há neste grupo?

4. Três homens querem atravessar um rio. O barco que eles possuem suporta no máximo 150 kg. Um deles pesa 50 kg, o segundo pesa 75 kg e o terceiro pesa 120 kg. Qual será o processo para eles atravessarem o rio sem afundar?

5. Forme um quadrado mágico com os números $1, 2, 3, 4, 5, 6, 7, 8$ e 9 tal que, a soma dos números de qualquer linha, qualquer coluna ou qualquer diagonal deverá ser sempre igual a 15.

6. Mostre que:

   (a) a soma de dois números pares é um número par.

   (b) a soma de dois números impares é um número par.

   (c) a soma de um número par e um número impar é um número impar.

   (d) o produto de dois números pares é um número par.

   (e) o produto de dois números impares é um número impar.

7. Mostre que $(n-1)^3 - n^3$ é um número impar, para todo $n \in \mathbb{N}$.

8. Escrever:

   (a) O número 25 na base 3

   (b) O número 125 na base 2.

   (c) O número 743 na base 8.

9. Escreva o número

   (a) 25 na base 3.

   (b) 125 na base 2.

   (c) 743 na base 8.

10. Determine:

    (a) A respresentação de 177130 na base 16.

    (b) A respresentação de 177130 na base 2.

11. Converta os números da base decimal para a base 2.

    (a) $a = 231$, $b = 4532$ e $c = 1123$.

    (b) $a = 3452$, $b = 45673$ e $c = 2312$.

12. Converta os números da base binária para a base decimal.

    (a) $a = 11111$, $b = 101011$ e $c = 1101101$.

    (b) $a = 1110111$, $b = 111111$ e $c = 1011110$.

13. Converta os números da base decimal para a base 3.

    (a) $a = 231$, $b = 4532$ e $c = 1123$.

    (b) $a = 3452$, $b = 45673$ e $c = 2312$.

14. Calcule a soma dos seguintes números na base 3.

    (a) $a = (20111)_3$ e $b = (11022)_3$.

    (b) $a = (12122)_3$ e $b = (22112)_3$.

15. Converta os números da base decimal para a base 4.

    (a) $a = 231$, $b = 4532$ e $c = 1123$.

    (b) $a = 3452$, $b = 45673$ e $c = 2312$.

16. Converta os números da base decimal para a base 5.

    (a) $a = 231$, $b = 4532$ e $c = 1123$.

    (b) $a = 3452$, $b = 45673$ e $c = 2312$.

17. Mostre que:

    (a) Um número inteiro é divisível por 2 se, e somente se, o algorismo das unidades é par.

    (b) Um número inteiro é divisível por 3 se, e somsente se, a soma dos seus algorismos é divisível por 3.

    (c) Um número inteiro é divisível por 11 se, e somente se, a diferença da soma dos seus algarismos em posições pares e a soma de seus algarismos em posições ímpares for divisível por 11.

18. Econtre a expanssão de Cantor dos seguintes números:

    (a) $a = 2$, $b = 7$ e $c = 19$.

    (b) $a = 87$, $b = 1000$ e $c = 1000000$.

Capítulo

4

Números inteiros

O estudo de métodos para determinar se um número é primo ocupou matemáticos como Fermat e Euler. Por volta de 1970 surgiu o estudo dos métodos de criptografia de chave pública. O estudo nesta área levou os estudiosos a busca de obter algoritmos determinísticos de primalidade.

Neste capítulo, inicialmente, será feito um estudo sobre a teoria elementar dos números enfocando o princípio do menor inteiro ou axioma da boa ordem, alguns resultados importantes, indução matemática, divisibilidade, o algoritmo euclidiano, máximo divisor comum e mínimo múltiplo comum.

4.1 Princípio do menor inteiro ou axioma da boa ordem

Seja $S \subseteq \mathbb{Z}$ com $S \neq \emptyset$. O conjunto S é dito limitado inferiormente se existe $a \in \mathbb{Z}$ tal que $a \leq x$ para todo $x \in S$.

Definição 4.1.1. *O elemento a nestas condições é chamado limite inferior de S. O maior dos limites inferiores de A pertence a S e é chamado elemento mínimo de S.*

Exemplo 4.1.1. *Todo subconjunto de $\mathbb{N}$ é limitado inferiormente, o conjunto $S = \{\cdots, -3, -2 - 1, 0, 1, 2\}$ não é limitado inferiormente.*

O princípio da boa ordenação ou princípio da boa ordem diz que todo subconjunto não vazio formado por números naturais possui um menor elemento. Isso é o mesmo que dizer que todo subconjunto não vazio formado por números inteiros positivos possui um menor elemento. Em outras palavras, todo subconjunto $S \subseteq \mathbb{Z}$, com $S \neq \emptyset$, limitado inferiormente possui um

elemento mínimo, ou seja, um elemento $a \in S$ tal que $a \leq x$, para todo $x \in S$ (isto é, a é um limite inferior de S).

Se $a \in \mathbb{Z}$ é um limite inferior de S, então todo elemento inteiro menor que a também é um limite inferior. Além disso, se S é limitado inferiormente, então o elemento mínimo do conjunto S é único.

Exemplo 4.1.2. *O mínimo do conjunto* $S = \{-6, -4, -2, 0, 3\}$ *é* -6*, o mínimo do conjunto* $S = \{2, 4, 6, \cdots\}$ *é* 2 *e o o conjunto* $S = \{1, \frac{1}{2}, \frac{1}{3}, \cdots\}$ *é limitado inferiormente e não possui elemento mínimo.*

4.1.1 Exercícios

1. Determine o menor inteiro do conjunto $A = \{\pm 1, \pm 10, \pm 2\}$.
2. Determine o menor inteiro do conjunto $A = \{0, 1, -1, -3\}$.
3. Determine o menor inteiro do conjunto $A = \{\frac{1}{1/n} : n \in \mathbb{N}\}$.

4.2 Indução matemática

Usando o princípio do menor inteiro, segue os resultados sobre indução matemática.

Teorema 4.2.1. *(Primeiro Princípio de Indução) Sejam* $a \in \mathbb{Z}$ *e* $P(n)$ *uma sentença associada a cada* $n \geq a$*, com* $n \in \mathbb{Z}$*. Se*

1. $P(a)$ *é verdadeira, e*
2. *Se* $P(k)$ *é verdadeira, com* $k \geq a$*, então* $P(k+1)$ *é verdadeira,*

então $P(n)$ *é verdadeira para todo* $n \geq a$*.*

Demonstração. Seja o conjunto $S = \{n \geq a : P(n) \text{ é falsa}\}$. Suponhamos que $S \neq \emptyset$. Como S é limitado inferiormente, segue que S possui um elemento mínimo s. Neste caso, $s \geq a$, $P(s)$ é falsa e $s - 1 \notin S$. Assim, $P(s-1)$ é verdadeira. Por (2), segue que $P(s)$ é verdadeira, o que é uma contradição. Portanto, $S = \emptyset$, ou seja, $P(n)$ é verdadeira para todo $n \geq a$. □

Exemplo 4.2.1. *Mostre que* $2^n > n$ *para todo* $n \geq 0$*. De fato, se* $n = 1$*, então* $2^0 = 1 > 0$*. Por hipótese de indução, suponhamos que* $P(k)$*, com* $k \geq 0$*, é verdadeiro, ou seja,* $2^k > k$*. Agora, vamos mostrar que* $P(k+1)$ *é verdadeiro. Como* $2^k > k$*, segue que* $2.2^k > 2k$*, ou seja,* $2^{k+1} > 2k$*. Como* $k < 2^k$*, segue que* $k + 1 \leq 2^k$*. Assim,* $k + 1 \leq 2^k < 2.2^k = 2^{k+1}$*. Portanto,* $2^n > n$ *para todo* $n > 0$*.*

Teorema 4.2.2. *(Segundo Princípio de Indução) Sejam* $a \in \mathbb{Z}$ *e* $P(n)$ *uma sentença associada a cada* $n \geq a$*, com* $n \in \mathbb{Z}$*. Se*

1. $P(a)$ *é verdadeira, e*

2. $P(k)$ é verdadeira para todo k tal que $a \leq k < n$,

então $P(n)$ é verdadeira para todo $n \geq a$.

Demonstração. Seja o conjunto $S = \{n \geq a : P(n) \text{ é falsa}\}$. Suponhamos que $S \neq \emptyset$. Como S é limitado inferiormente, segue que S possui um elemento mínimo s. Neste caso, $s \geq a$, $P(s)$ é falsa e $s - 1 \notin S$. Assim, $P(s-1)$ é verdadeira. Por (2), segue que $P(s)$ é verdadeira, o que é uma contradição. Portanto, $S = \emptyset$, ou seja, $P(n)$ é verdadeira para todo $n \geq a$. □

4.2.1 Exercícios

1. Mostre por indução que $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$, para todo $n \geq 1$.
2. Mostre por indução que $1.2 + 2.3 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}$, para todo $n \geq 1$.
3. Mostre por indução que $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$, para todo $n \geq 1$.
4. Mostre por indução que $\frac{1}{1.2} + \frac{1}{2.3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$, para todo $n \in \mathbb{N}$.
5. Mostre por indução que $1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}$, para todo $n \in \mathbb{N}$.
6. Mostre por indução que $1^3 + 2^3 + 3^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2$, para todo $n \in \mathbb{N}$.
7. Mostre por indução que $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$, para todo $n \geq 1$.
8. Mostre por indução que $1 + 3 + 5 + \ldots + (2n-3) + (2n-1) = n^2$, para todo $n \geq 1$.
9. Mostre por indução que $1 + a + a^2 + a^3 + \ldots + a^{n-1} + a^n = \frac{a^{n+1}-1}{a-1}$, para todo $n \geq 0$ e $a \in \mathbb{R}$ com $a \neq 1$.
10. Mostre por indução que $2^n > n^2$, para todo $n \geq 5$.
11. Mostre por indução que $2^{n+1} \geq n + 2$, para todo $n \geq -1$.
12. Mostre por indução que $1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2$.
13. Mostre por indução que $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$, para todo $a \geq 1$ e para todo $n \geq 1$.
14. Mostre que $(n+1)^n \geq 3^n$, para todo $n \geq 4$.
15. Mostre que $n^2 + 1 \geq 2^n$, para todo inteiro n tal que $n = 1, 2, 3, 4$.
16. Sejam x e y são números reais positivos. A média aritmética de x e y é definida por $(x+y)/2$. A média geométrica de x e y é definida por $\sqrt{xy}$. A média harmônia de x e y é definida por $2xy/(x+y)$. A média quadrática aritmética de x e y é definida por $\sqrt{(x^2+y^2)/2}$.
    (a) Mostre que $(x+y)/2 > \sqrt{xy}$.
    (b) Encontre relações entre essas médias.

4.3 Divisibilidade

Seja $a \in \mathbb{Z}$. O conjunto $S = \{0, \pm a, \pm 2a, \cdots\}$ é chamado conjunto dos múltiplos de a.

Definição 4.3.1. *Sejam $a, b \in \mathbb{Z}$. O elemento a é dito que divide b se existe $c \in \mathbb{Z}$ tal que $b = ac$, ou seja, b é um múltiplo de a. Neste caso, a notação usada é $a \mid b$, e se a não divide b, usamos a notação $a \nmid b$.*

Exemplo 4.3.1. $5 \mid 15$, *pois* $15 = 3.5$ *e* $0 \mid 0$, *uma vez que* $0 = 0.k$ *para todo* $k \in \mathbb{Z}$.

Propriedades 4.3.1. *Sejam $a, b, c \in \mathbb{Z}$.*

1. $a \mid 0$, *uma vez que* $0 = a0$.
2. $a \mid a$, *uma vez que* $a = a.1$, *chamada propriedade reflexiva.*
3. *Se $a \mid b$ e $b \mid c$, então $a \mid c$, pois existem $c_1, c_2 \in \mathbb{Z}$ tal que $b = ac_1$ e $c = bc_2$. Assim, $c = bc_2 = a(c_1c_2)$, ou seja, $a \mid c$. Essa propriedade é chamada propriedade transitiva. s*
4. *Se $a \mid b$, então $a \mid bx$, para todo $x \in \mathbb{Z}$. De fato, existe $c_1 \in \mathbb{Z}$ tal que $b = ac_1$. Assim, $bx = a(c_1x)$, para todo $x \in \mathbb{Z}$. Portanto, $a \mid bx$, para todo $x \in \mathbb{Z}$.*
5. *Se $a \mid b$ e $a \mid c$, então $a \mid (bx + by)$, para todo $x, y \in \mathbb{Z}$. De fato, existem $c_1, c_2 \in \mathbb{Z}$ tal que $b = ac_1$ e $c = ac_2$. Assim, $bx = a(c_1x)$ e $cy = a(c_2y)$ para todo $x, y \in \mathbb{Z}$. Logo, $bx + cy = a(c_1x + c_2y)$, e portanto, $a \mid (bx + cy)$.*
6. *Se $a \mid b$ e $b \mid a$, então $a = \pm b$. De fato, por hipórese, existem $c_1, c_2 \in \mathbb{Z}$ tal que $b = ac_1$ e $a = bc_2$. Assim, $a = bc_2 = a(c_1c_2$, ou seja, $a \mid a$ e $c_1c_2 = \pm 1$. Portanto, $c_1 = c_2 = \pm 1$, e portanto, $a = \pm b$.*
7. *Se $a \mid b$ e $a \mid c$, então $a \mid (b \pm c)$. De fato, por hipórese, existem $c_1, c_2 \in \mathbb{Z}$ tal que $b = ac_1$ e $c = ac_2$. Assim, $b \pm c = a(c_1 \pm c_2)$, ou seja, $a \mid (b \pm c)$.*

O algoritmo da divisão é também chamado algoritmo euclidiano em homenagem a Euclides.

Teorema 4.3.1. *(Algoritmo Euclidiano ou da Divisão) Se $a, b \in \mathbb{Z}$, com $b > 0$, então existem e são únicos $q, r \in \mathbb{Z}$ tal que $a = bq + r$, com $0 \leq r < b$.*

Demonstração. Seja $S = \{a - bx : x \in \mathbb{Z} \text{ e } a - bx \geq 0\}$. O conjunto $\neq \emptyset$, pois $b \geq 1$ e tomando $x = - \mid a \mid$, segue que $a - bx = a + b \mid a \mid \geq a + \mid a \mid \geq 0$. Pelo Princípio do Menor Inteiro, segue que existe $r \in S$, mínimo, tal que $r \geq 0$ e $r = a - bq$, com $q \in \mathbb{Z}$. Assim, $a = bq + r$, com $q, r \in \mathbb{Z}$. Além disso, $r < b$, pois se $r \geq b$, então $0 \leq r - b = a - bq - b = a - b(q + 1) < r$. Assim, r não é o mínimo de S. Portanto, $0 \leq r < b$. Para a unicidade, suponhamos que existam $q_1, r_1 \in \mathbb{Z}$ tal que $a = bq_1 + r_1$ com $0 \leq r_1 < b$. Assim, $bq + r = bq_1 + r_1$, ou seja, $b(q - q_1) = r_1 - r$. Portanto, $b \mid r_1 - r$. Como $-b < -r \leq 0$ e $0 \leq r_1 < b$, segue que $-b < r_1 - r < b$, ou seja, $\mid r_1 - r \mid < b$. Como $b \mid r_1 - r$ e $\mid r_1 - r \mid < b$, segue que $r_1 - r = 0$, ou seja, $r_1 = r$. Finalmente, como $r_1 = r$, segue que $bq = bq_1$. Como $b \neq 0$, segue que $q = q_1$. □

Corolário 4.3.1. *Se $a, b \in \mathbb{Z}$, com $b \neq 0$, então existem e são únicos $q, r \in \mathbb{Z}$ tal que $a = bq + r$, com $0 \leq r <\mid b \mid$.*

Demonstração. Se $b > 0$, o resultado segue do Teorema 4.3.1. Se $b < 0$, então $\mid b \mid > 0$. Pelo Teorema 4.3.1, segue que existem $q_1, r \in \mathbb{Z}$ únicos tal que $a = \mid b \mid q_1 + r$, com $0 \leq r <\mid b \mid$. Como $\mid b \mid = -b$, segue que $a = b(-q_1) + r$, com $0 \leq r <\mid b \mid$. Portanto, existem $q = -q_1, r \in \mathbb{Z}$ únicos tal que $a = bq + r$ com $0 \leq r <\mid b \mid$. □

Definição 4.3.2. *O inteiros q e r são chamados, respectivamente, quociente e resto da divisão de a por b.*

4.3.1 Máximo divisor comum e mínimo múltiplo comum

Seja $a \in \mathbb{Z}$. O conjunto dos divisores de a será denotado por $D(a)$. Intuitivamente, o máximo divisor comum de $a, b \in \mathbb{Z}$ é o maior elemento de $D(a) \cap D(b)$.

Proposição 4.3.1. *Se $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$, então existe um único $d \in \mathbb{Z}$ tal que $d > 0$, $d \in D(a) \cap D(b)$ e é o maior inteiro positivo com essa propriedade.*

Demonstração. Seja $S = \{ax + by : x, y \in \mathbb{Z}\}$. Tomando $x = a$ e $y = b$, segue que $a^2 + b^2 > 0$, ou seja, S possui números estritamente positivos. Pelo Princípio do Menor Inteiro, segue que existe $d \in S$ um elemento mínimo. Assim, $d = ax_0 + by_0 > 0$, com $x_0, y_0 \in \mathbb{Z}$. Pelo algoritmo da divisão, segue que existem $q, r \in \mathbb{Z}$ tal que $a = dq + r$ com $0 \leq r < d$. Assim, $r = a - dq = a - (ax_0 + by_0)q = a(1 - qx_0) + b(-qy_0) \in S$. Como $0 \leq r < d$ e d é o mínimo de S, segue que $r = 0$. Portanto, $a = dq$, ou seja, $d \mid a$. De modo análogo, segue que $d \mid b$. Agora, se $d' \mid a$ e $d' \mid b$, segue que $d' \mid (ax_0 + by_0)$, ou seja, $d' \mid d$. Portanto, existe único $d > 0$, onde $d \in D(a) \cap D(b)$ e é o maior com essa propriedade. □

Definição 4.3.3. *Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$ ou $b \neq 0$. Um número $d \in \mathbb{Z}$ é chamado máximo divisor comum de a e b se:*

1. *$d > 0$.*
2. *$d \mid a$ e $d \mid b$.*
3. *Se existe $d' \in \mathbb{Z}$ tal que $d' \mid a$ e $d' \mid b$, então $d' \mid d$.*

A notação usada é $d = mdc(a, b)$.

Exemplo 4.3.2. *Se $0, -2, 4 \in \mathbb{Z}$, então $mdc(4, 0) = 4$ e $mdc(-2, 4) = 2$.*

Além disso, se $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$, então $mdc(a, b) = mdc(\mid a \mid, \mid b \mid) = mdc(b, a) = mdc(\mid a \mid, b) = mdc(a, \mid b \mid)$.

Teorema 4.3.2. *(Identidade de Bezout) Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. Se $d = mdc(a, b)$, então existem $x_0, y_0 \in \mathbb{Z}$ tal que $d = ax_0 + by_0$.*

Demonstração. Pela Proposição 4.3.1, segue que existem $x_0, y_0 \in \mathbb{Z}$ tal que $ax_0 + by_0 = mdc(a, b)$. Portanto, $d = ax_0 + by_0$, para algum $x_0, y_0 \in \mathbb{Z}$. □

Definição 4.3.4. *Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$ ou $b \neq 0$. Um número $m \in \mathbb{Z}$ é chamado mínimo múltiplo comum de a e b se:*

1. *$m > 0$.*
2. *$a \mid m$ e $b \mid m$.*
3. *Se existe $m' \in \mathbb{Z}$ tal que $a \mid m'$ e $b \mid m'$, então $m \mid m'$.*

A notação usada é $m = mmc(a, b)$.

Se $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$, então

$$mmc(a, b) = mmc(\mid a \mid, \mid b \mid) = mmc(b, a) = mmc(\mid a \mid, b) = mmc(a, \mid b \mid).$$

Exemplo 4.3.3. *Se $0, -2, 4 \in \mathbb{Z}$, então $mmc(4, 0) = 4$ e $mmc(-2, 4) = 4$.*

4.3.2 Processo prático para encontrar o máximo divisor comum

O algoritmo euclidiano, como o próprio nome diz, foi descrito por Euclides nas proposições 1 e 2 do Livro 7 dos *Elementos*, mas acredita-se que sua origem seja muito anterior a Euclides. Dados a e b inteiros positivos e que $a \geq b$, o algoritmo de Euclides tem a finalidade de encontrar o máximo divisor comum entre a e b. Assim, dividindo a por b, encontramos o resto r_1. Se $r_1 \neq 0$, dividimos b por r_1, obtendo o resto r_2. Se $r_2 \neq 0$, dividimos r_1 por r_2, obtendo o resto r_3, e assim, por diante. O último resto diferente de zero desta sequência de divisões é o máximo divisor comum entre a e b. O algoritmo de Euclides também é usado para achar a expressão do $mdc(a, b)$ como combinação linear de a e b. Neste caso, faz-se uma tabela para se calcular o máximo divisor comum entre dois números.

Exemplo 4.3.4. *Cálculo do $mdc(963, 657)$ pelo algoritmo de Euclides e a sua expressão como combinação linear de 963 e 657. Neste caso, $963 = 657.1 + 306$; $657 = 306.2 + 45$; $306 = 45.6 + 36$; $45 = 36.1 + 9$ e $36 = 9.4 + 0$. Assim,*

	1	2	6	1	4
963	657	306	45	36	9
306	45	36	9	0	

Portanto, $mdc(963, 657) = 9$ e a sua expressão como combinação linear de 963 e 657 se obtém eliminando os restos $36, 45$ e 306 entre as quatro primeiras igualdades do seguinte modo: $9 = 45 - 36 = 45 - (306 - 45.6) = -306 + 7.45 = -306 + 7.(657 - 306.2) = 7.657 - 15.306 = 7.657 - 15.(963 - 657) = 963.(-15) + 657.22$, ou seja, $9 = mdc(963, 657) = 963x_0 + 657y_0$, onde $x_0 = -15$ e $y_0 = 22$.

Esta representação do inteiro $9 = mdc(963, 657)$ como combinação linear de 963 e 657 não é unica, pois somando e subtraindo o produto 963.657 ao segundo membro da igualdade $9 = 963.(-15) + 657.22$, segue que $9 = 963(-15 + 657) + 657(22 - 963) = 963.642 + 657(-941)$, ou seja, é uma outra representação do inteiro $9 = mdc(963, 657)$ como combinação linear de 963 e 657. Um outro exemplo um pouco diferente pode ser o seguinte.

Exemplo 4.3.5. *O máximo divisor comum de dois inteiros positivos a e b é 74 e na sua determinação pelo algoritmo de Euclides os quocientes obtidos foram $1, 2, 2, 5, 1$ e 3. Assim, os inteiros positivos a e b, são obtidos pela seguinte tabela*

	1	2	2	5	1	3
a	b	r	r_1	r_2	r_3	74
r	r_1	r_2	r_3	74	0	

Assim, $a = b+r$, $b = 2r+r_1$, $r = 2r_1+r_2$, $r_1 = 5r_2+r_3$, $r_2 = r_3+74$ e $r_3 = 74.3 = 222$. Portanto, $r_2 = 222+74 = 296$, $r_1 = 5.296+222 = 1702$, $r = 2.1702+296 = 3700$, $b = 2.3700+1702 = 9102$ e $a = 9102 + 3700 = 12802$.

Agora, perguntamos, porquê o resultado destas divisões é o máximo divisor comum? Outra dúvida, precisamos verificar que a sequência de divisões chega sempre a um resto zero, ou o algoritmo continuaria para sempre. Começamos tratando da segunda questão. Assim, vamos verificar onde o algoritmo pára. Digamos que, para calcular o máximo divisor comum entre dois inteiros a e b, com $b \geq 0$, fazemos uma sequência de divisões como: $a = bq_1 + r_1$, onde $0 \leq r_1 < b$; $b = r_1q_2 + r_2$, onde $0 \leq r_2 < r_1$; $r_1 = r_2q_3 + r_3$ onde $0 \leq r_3 < r_2$; $r_2 = r_3q_4 + r_4$, onde $0 \leq r_4 < r_3 < \cdots$. Esquecendo por um instante o que está acontecendo no primeiro membro das igualdades, no segundo membro das igualdades tem-se uma sequência de restos, e observamos que o seguinte é sempre menor que o anterior, mas todos são maiores ou iguais a zero. Seja a sequência das desigualdades dos restos

$$b > r_1 > r_2 > r_3 > r_4 > \cdots \geq 0. \tag{4.1}$$

Como entre b e 0 existe apenas uma quantidade finita de inteiros, segue que esta sequência não pode continuar indefinidamente. Mas ela só chega ao final se um dos restos for zero, e é isto que garante que o algoritmo sempre pára. Agora, falta verificar que o último resto não nulo coincide com o máximo divisor comum. Para entendermos isto, precisamos de um resultado auxiliar que é dado pelo seguinte lema.

Lema 4.3.1. *Sejam a e b números inteiros positivos. Se existem inteiros q e r tal que $a = bq+r$, então $mdc(a, b) = mdc(b, r)$.*

Demonstração. Suponhamos que $d_1 = mdc(a, b)$ e $d_2 = mdc(b, r)$, e mostremos que $d_1 = d_2$. Para isso, o raciocínio usado será de mostrar que $d_1 \leq d_2$ e $d_2 \leq d_1$. Provamos que $d_1 \leq d_2$ pois a outra desigualdade é verificada de maneira análoga. Como $d_1 = mdc(a, b)$, segue que d_1 divide a e b. Assim, existem inteiros q_1 e q_2 tal que $a = d_1q_1$ e $b = d_1q_2$. Por hipótese, $a = bq+r$, e assim, $d_1q_1 = d_1q_2q + r$, ou seja, $r = d_1q_1 - d_1q_2q = d_1(q_1 - q_2q)$. Deste modo, d_1 divide

r, e portanto, $d_1 = mdc(b, r)$. Mas, como $d_2 = mdc(b, r)$, segue que $d_1 \leq d_2$. Analogamente, $d_2 \leq d_1$. Portanto, $d_1 = d_2$. □

Finalmente, agora vamos usar o Lema 4.3.1 para justificar que o último resto não nulo da sequência de divisões é o máximo divisor comum. De fato, sejam a e b dois inteiros com $a \geq b$ e $b \neq 0$. Aplicando o algoritmo de Euclides para a e b e supondo que o resto nulo ocorre após n divisões, segue que $a = bq_1 + r_1$, onde $0 \leq r_1 < b$; $b = r_1q_2 + r_2$, onde $0 \leq r_2 < r_1$; $r_1 = r_2q_3 + r_3$, onde $0 \leq r_3 < r_2$; $r_2 = r_3q_4 + r_4$, onde $0 \leq r_4 < r_3$; $\cdots$; $r_{n-4} = r_{n-3}q_{n-2} + r_{n-2}$, onde $0 \leq r_{n-2} < r_{n-3}$; $r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}$, onde $0 \leq r_{n-1} < r_{n-2}$ e $r_{n-2} = r_{n-1}q_n$, onde $r_n = 0$. Agora, da última divisão, segue que r_{n-1} divide r_{n-2}. Logo, o maior divisor comum entre r_{n-1} e r_{n-2} é r_{n-1}. Portanto, $mdc(r_{n-2}, r_{n-1}) = r_{n-1}$. Pelo Lema 4.3.1, na penúltima divisão, segue que $mdc(r_{n-3}, r_{n-2}) = mdc(r_{n-2}, r_{n-1} =)r_{n-1}$. Novamente aplicando o Lema 4.3.1 na ante-penúltima divisão, segue que $mdc(r_{n-4}, r_{n-3}) = mdc(r_{n-3}, r_{n-2}) = r_{n-1}$. Fazendo este mesmo processo na igualdade anterior, segue que $mdc(a, b) = r_{n-1}$, que é o que queriamos provar.

4.3.3 Exercícios

1. Sejam $a = 2^3.3^2.7^3.11^5$ e $b = 2^2.3^3.5^4.7.11^2.13^3$.
   (a) Determine o $mdc(a, b)$.
   (b) Determine o $mmc(a, b)$.
2. Determine $x_0, y_0 \in \mathbb{Z}$ tal que:
   (a) $3x_0 + 7y_0 = 1$.
   (b) $21x_0 + 14y_0 = 7$.
3. Determine $x_0, y_0, z_0 \in \mathbb{Z}$ tal que:
   (a) $3x_0 + 7y_0 + 11z_0 = 1$.
   (b) $36x_0 + 6y_0 + 64z_0 = 2$.
4. Sejam $a, b \in \mathbb{Z}$, com ambos não nulos.
   (a) Mostre que $mdc(a, b)mmc(a, b) = ab$.
   (b) Mostre que $mdc(a, 0) = a$, com $a > 0$.
5. Sejam $a, b, c \in \mathbb{Z}$.
   (a) Mostre que $mdc(a, b, c) = mdc(a, mdc(b, c))$.
   (b) Mostre que $mmc(a, b, c) = mmc(a, mmc(b, c))$.
6. Sejam $a_1, \ldots, a_n \in \mathbb{Z}$, onde são não todos nulos.
   (a) Defina $mdc(a_1, a_2, \ldots, a_n)$ e $mmc(a_1, a_2, \ldots, a_n)$.

(b) Se $d = mdc(a_1, a_2, \ldots, a_n)$, mostre que existem $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ tal que $d = a_1x_1 + a_2x_2 + \cdots + a_nx_n$.

(c) Mostre $1 = mdc(a_1, a_2, \ldots, a_n)$ se, e somente se, existem $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ tal que $1 = a_1x_1 + a_2x_2 + \cdots + a_nx_n$.

(d) Se $d = mdc(a_1, a_2, \ldots, a_n)$, mostre que $mdc(a_1/d, a_2/d, \ldots, a_n/d) = 1$.

7. Usando o processo prático, determine os seguintes máximos divisores comuns:

(a) $mdc(4, 12)$ e $mdc(15, 35)$.

(b) $mdc(40, 84)$ e $mdc(32, 72)$.

8. Determine:

(a) $mdc(3, mdc(9, 15))$ e $mdc(mdc(4, 12), 6)$.

(b) $mmc(mmc(3, 5), 7)$ e $mmc(4, mmc(6, 8))$.

9. Mostre por indução que $80 \mid 3^{4n} - 1$, para todo $n \in \mathbb{N}$.

10. Mostre por indução que $9 \mid 4^n + 6n - 1$, para todo $n \in \mathbb{N}$.

11. Mostre por indução que $8 \mid 3^{2n} + 7$, para todo $n \in \mathbb{N}$.

12. Mostre por indução que 9 divide $n4^{n+1} - (n + 1)4^n + 1$, para todo $n \in \mathbb{N}$.

13. Mostre por indução que $8 \mid 3^{2n} - 1$, para todo $n \geq 0$.

14. Mostre por indução que $7 \mid n^7 - n$, para todo $n \geq 1$.

15. Mostre por indução que $3^{2n+1} + 2^{m+2}$ é divisível por 7, para todo $n \in \mathbb{N}$.

16. Mostre por indução que $2^{2n} + 15n - 1$ é divisível por 9, para todo $n \geq 0$.

17. Seja 7 o resto da divisão de um inteiro n por 12. Determine:

(a) O resto da divisão de $2n$ por 12.

(b) O resto da divisão de n por 4.

(c) O resto da divisão de n por 8.

18. Mostre que n ou $n + 2$ ou $n + 4$ é divisível por 3.

19. Se n é impar, mostre que 8 divide $n^2 - 1$.

20. Se m e n são números impares, mostre que 8 divide $m^2 - n^2$.

21. Se $d = mdc(m, n)$, onde $m, n \in \mathbb{N}$, mostre que $mdc(m/d, n/d) = 1$.

Capítulo

5

Teorema fundamental da aritmética

O estudo de métodos para determinar se um nuúmero é primo ocupou matemáticos como Fermat e Euler. Seja $a \in \mathbb{Z}$ com $a \neq 0$ e $a \neq \pm 1$. O número a tem pelo menos quatro divisores, ou seja, $\{1, -1, a, -a\} \subseteq D(a)$. Estes divisores são chamados divisores triviais de a.

Neste capítulo, apresentamos o conceito de número primo e de número composto, e também, veremos um importante resultado que os envolvem chamado Teorema Fundamental da Aritmética. O Teorema Fundamental da Aritmética mostra que todo número inteiro maior que 1 se escreve de maneira única como um produto de números primos. Apresentamos, também, um estudo de congruências, função de Euler e abordamos alguns resultados importantes da teoria dos números, tais como os Teoremas de Euler, Wilson e Fermat.

5.1 Números primos

Nesta seção, apresentamos o conceito de número primo e veremos um importante resultado que os envolvem chamado Teorema Fundamental da Aritmética que é indispensável para os estudos que seguirá.

Definição 5.1.1. *Um número $p \in \mathbb{Z}$, onde $p \neq 0$ e $p \neq \pm 1$, é chamado um número primo se os únicos divisores p são os divisores triviais. Um número $a \in \mathbb{Z}$, onde $a \neq 0$ e $a \neq \pm 1$, é chamado composto se não é um número primo, ou seja, se adimite outros divisores aém dos triviais.*

Em geral, usamos simplesmente os termos primos ou compostos. Por exemplo, os números $2, 3, 5$ e 7 são primos e os números $4, 6$ e 8 são compostos.

Exemplo 5.1.1. *Considerando o número* 19 *o conjunto* $D(19) = \{\pm 1, \pm 19\}$ *e, portanto, é primo. Para o número* 20*, segue que* $D(20) = \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20\}$*, e assim,* 20 *é composto.*

Definição 5.1.2. *Dois números* $a, b \in \mathbb{Z}$ *são chamados relativamente primos (ou primos entre si) se* $mdc(a, b) = 1$*.*

Proposição 5.1.1. *Sejam* $a, b, c \in \mathbb{Z}$*. Se* $a \mid bc$ *e se* $mdc(a, b) = 1$*, então* $a \mid c$*.*

Demonstração. Pela identidade de Bezout, segue que existem $x_0, y_0 \in \mathbb{Z}$ tal que $1 = ax_0 + by_0$. Multiplicando por c, segue que $c = a(cx_0) + (bc)y_0$. Portanto, $a \mid c$. □

Lema 5.1.1. *(Lema de Euclides) Se* $p \in \mathbb{Z}$ *é um número primo e* $p \mid ab$*, com* $a, b \in \mathbb{Z}$*, então* $p \mid a$ *ou* $p \mid b$*.*

Demonstração. Se $p \nmid a$, então $mdc(a, p) = 1$. Pelo Teorema 4.3.2, segue que existem $x_0, y_0 \in \mathbb{Z}$ tal que $1 = ax_0 + py_0$. Multiplicando por b em ambos os lados, segue que $b = (ab)x_0 + p(by_0)$. Como $p \mid ab$ e $p \mid p$, segue que $p \mid b$. □

Lema 5.1.2. *Se* $a \in \mathbb{Z}$ *e* $a \geq 2$*, então* a *admite um divisor primo* p*, onde* $p > 0$*.*

Demonstração. A demonstração é feita através do segundo princípio de indução com $a > 0$. Para $a = 2$ é suficiente tomar $p = 2$, uma vez que $2 \mid 2$. Agora, suponha que todo m tal que $2 \leq m < a$ tem um divisor primo. Temos que provar que a tem um divisor primo. Se a for primo, então $a \mid a$, e o resultado segue. Se a for composto, então a tem um divisor não trivial $m > 1$. Assim, $a = mq$, para algum $q \in \mathbb{Z}$. Logo, $2 \leq m < a$. Por hipótese de indução, segue que existe um número primo p tal que $m = pq_1$, para algum $q_1 \in \mathbb{Z}$. Portanto, $a = pqq_1$, ou seja, a tem um fator primo p. Logo, $p \mid a$. Finalmente, se $a < 0$, segue que $-a > 0$, e o resultado segue de modo análogo. □

Teorema 5.1.1. *(Teorema Fundamental da Aritmética) Se* $a \in \mathbb{Z}$*, com* $a \neq 0$ *e* $a \neq \pm 1$*, então* a *é decomposto de modo único como o produto de números primos, ou seja, existem* $p_1, p_2, \cdots, p_r$ *primos tal que* $a = \pm p_1 p_2 \cdots p_r$ *e que a menos da ordem dos fatores a decomposição é única.*

Demonstração. A demonstração é feita através do segundo princípio de indução com $a > 0$. Se $a = 2$, como 2 é primo, o resultado segue. Suponhamos que $a > 2$ e que o resultado é verdadeiro para todo m tal que $2 \leq m < a$. Pelo Lema 5.1.2, segue que a admite um fator primo p_1, ou seja, $a = p_1 m$, para algum $m \in \mathbb{Z}$. Assim, se $m = 1$ ou m é primo, o resultado segue. Caso contrário, como $2 \leq m < a$, segue por hipótese de indução que existem $r - 1$ primos $p_2, p_3, \cdots, p_r$, com $r - 1 \geq 1$, tal que $m = p_2 p_3 \cdots p_r$. Portanto, $a = p_1 p_2 \cdots p_r$. Para a unicidade, se $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ são duas fatorações de a, então $p_1 \mid q_1 q_2 \cdots q_s$. Como p_1 é primo, pelo Lema 5.1.1 segue que $p_1 \mid q_j$, para algum $j = 1, 2, \cdots, s$. Sem perda de generalidade, suponhamos que $j = 1$. Assim, $q_1 = p_1$, e desse modo, cancelando p_1 segue que $p_2 \cdots p_r = q_2 q_3 \cdots q_s$. Repetindo esse procedimento o quanto for necessário, segue que $r = s$ e $p_i = q_i$ para todo $i = 1, 2, \cdots, r$. Finalmente, se $a < 0$, segue que $-a > 0$, e o resultado segue de modo análogo. □

Na decomposição $a = p_1 p_2 \cdots p_r$, segundo o Teorema 5.1.1, em geral, os fatores não são distintos. Assim, reunindo os fatores primos iguais, segue que $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, onde $1 \leq s \leq r$, $p_i \neq p_j$ sempre que $i \neq j$ e $\alpha_i \geq 1$ para todo $i = 1, 2, \cdots, s$. Além disso, muitas vezes é conveniente na fatoração de dois números tomar potências nulas para que a fatoração possua potências dos mesmos primos. Finalmente, se m é um divisor de $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, então $m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$, onde $0 \leq \beta_i \leq \alpha_i$ para todo $i = 1, 2, \cdots, s$. Além disso, $mdc(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s}$, onde $\gamma_i = \min\{\alpha_i, \beta_i\}$, para $i = 1, 2, \cdots, s$ e $mmc(a, b) = p_1^{\delta_1} p_2^{\delta_2} \cdots p_s^{\delta_s}$, onde $\delta_i = \max\{\alpha_i, \beta_i\}$, para $i = 1, 2, \cdots, s$. Desse modo, para fatorarmos um número a é preciso que dividamos n pelo menor primo divisor. O quociente q_1 deve ser dividido pelo menor primo divisor de q_1, e assim, por diante, até que q_n seja 1. Feito isso, todos os primos que foram divisores no processo dado acima, quando multiplicados, terão a como produto, ou seja, eles são os fatores de a.

Exemplo 5.1.2. *O número* 315 *possui a seguinte fatoração:* $3^2 \times 5 \times 7$.

Proposição 5.1.2. *Se* $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ *e* $b = p_1^{\beta_1} \cdots p_n^{\beta_n}$, *então* $b \mid a$ *se, e somente se,* $0 \leq \beta_i \leq \alpha_i$, *para todo* $i = 1, 2, \cdots, n$.

Demonstração. Se $b \mid a$, então existe $q \in \mathbb{Z}$ tal que $a = bq$, ou seja, $p_1^{\alpha_1} \cdots p_n^{\alpha_n} = p_1^{\beta_1} \cdots p_n^{\beta_n} q$. Assim, $p_1^{\alpha_1 - \beta_1} \cdots p_n^{\alpha_n - \beta_n} = q$. Como $q \in \mathbb{Z}$, segue que $0 \leq \beta_1 \leq \beta_i$, para todo $i = 1, 2, \cdots, n$. Reciprocamente, se $0 \leq \beta_i \leq \alpha_i$, então $\beta_i = \alpha_i + x_i$, com x_i um inteiro positivo, para todo $i = 1, 2, \cdots, n$. Assim, $p_i^{\alpha_i} = p_i^{\beta_i + x_i} = p_i^{\beta_i} p_i^{x_i}$, ou seja, $p_i^{\beta_i}$ divide $p_i^{\alpha_i}$, para $i = 1, 2, \cdots, n$. Portanto, $b \mid a$. □

Exemplo 5.1.3. *As decomposições canônica dos números* $a = 42336$ *e* $b = 1270080$ *são dadas por* $a = 42336 = 2^5.3^3.7^2$ *e* $b = 1270080 = 2^6.3^4.5.7^2$. *O número b possui um fator* 2 *e um fator* 3 *a mais do que o número a e possui um fator* 5 *não presente em a. Multiplicando esses três fatores, obtemos o número* 30, *que é a divisão de* 1270080 *por* 42336.

Exemplo 5.1.4. *O número* $b = 17640$ *divide* $a = 13852800$, *uma vez que* $b = 17640 = 2^3.3^2.5.7^2$ *e* $a = 13582800 = 2^4.3^2.5^2.7^3.11$.

É possível descobrir quantos divisores positivos tem um número a partir da sua fatoração, ou seja, o número de divisores de $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ é dado por $D(a) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_n + 1)$.

Exemplo 5.1.5. *O número de divisores* 1500 *é dado por* $D(1500) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_n + 1) = (2 + 1)(1 + 1)(3 + 1) = 3.2.4 = 24$, *onde* $1500 = 2^2.3^1.5^3$. *Portanto, o número* 1500 *possui* 24 *divisores.*

Teorema 5.1.2. *Se Se* $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ *e* $b = p_1^{\beta_1} \cdots p_n^{\beta_n}$ *e* $\gamma_i = min\{\alpha_i, \beta_i\}$, *para* $i = 1, 2, \cdots, n$, *então* $mdc(a, b) = p_1^{\gamma_1} \cdots p_n^{\gamma_n}$.

Demonstração. Seja $d = p_1^{\gamma_1} \cdots p_n^{\gamma_n}$. Como $\gamma_i = min\{\alpha_i, \beta_i\}$, para $i = 1, 2, \cdots, n$, segue que $\gamma_i \leq \alpha_i$ e $\gamma_i \leq \beta_i$. Pela Proposição 5.1.2, segue que $d \mid a$ e $d \mid b$. Agora, se d' é um divisor comum de a e b, então $d' = p_1^{\delta_1} \cdots p_n^{\delta_n}$, onde $\delta_i \leq \gamma_i$, para $i = 1, 2, \cdots, n$. Pela Proposição 5.1.2, segue que $d^{|'} \mid d$. Portanto, $d = mdc(a, b)$. □

Exemplo 5.1.6. *O máximo divisor* $a = 3896200 = 2^3.5^2.7.11^2.23$ *e* $b = 592480 = 2^5.5.7.23^2$ *é dado por* $d = mdc(a, b) = 2^3.5^1.7^1.11^0.23^1 = 6440$.

De modo análogo segue que o $m = mmc(a, b)$, onde $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ e $b = p_1^{\beta_1} \cdots p_n^{\beta_n}$ é dado por $m = p_1^{\gamma_1} \cdots p_n^{\gamma_n}$, onde $\gamma_i = max\{\alpha_i, \beta_i\}$, para todo $i = 1, 2, \cdots, n$.

Corolário 5.1.1. *Se* $a, b \in \mathbb{Z}$ *são ambos não nulo e diferente de* ± 1*, então* a/d *e* b/d *são primos entre si, onde* d *é um máximo divisor comum de* a *e* b.

Demonstração. Se $p_i^{\alpha_i}$ é um fator de a e $p_i^{\beta_i}$ é um fator de b, então $p_i^{\gamma_i}$ é um fator de d, onde $\gamma_i = \min\{\alpha_i, \beta_i\}$. Além disso, $p_i^{\alpha_i - \gamma_i}$ é um fator de a/d e $p_i^{\beta_i - \gamma_i}$ é um fator de b/d. Assim, $\alpha_i - \gamma_i = 0$ ou $\beta_i - \gamma_i = 0$, e portanto, $min\{\alpha_i - \gamma_i, \beta_i - \gamma_i\} = 0$. Como esse mínimo é o expoente de p_i em a/d e b/d, segue que não existem fatores comuns primos em a/d e em b/d. □

Teorema 5.1.3. *O conjunto de números primos é infinito.*

Demonstração. Suponhamos que o conjunto de números primos seja finito. Logo, existe p_n tal que p_n é o maior de todos os demais $p_1, p_2, \cdots, p_{n-1}$. Consideremos o inteiro $m > 1$ tal que:

$$m = p_1 p_2 \cdots p_n + 1.$$

Pelo Teorema Fundamental da Aritmética, segue que m admite pelo menos um divisor primo p. Mas, como $p_1, p_2, \cdots, p_n$ é conjunto de todos os primos, segue que $p = p_i$, para algum $i = 1, 2, \cdots, n$. Assim, $p \mid m$ e $p \mid p_1 p_2 \cdots p_n$. Logo, $p \mid 1$, pois $1 = m - p_1 p_2 \cdots p_n$, o que é um absurdo. Portanto, o conjunto de primos é infinito. □

Teorema 5.1.4. *(Fermat) Se um inteiro* $n > 1$ *é composto, então* n *possui um divisor primo* p *tal que* $p \leq \sqrt{n}$.

Demonstração. Seja $n = ab$, com $1 < a \leq b < n$. Se $a < b$, então

$$n = ab \geq a^2,$$

ou seja, $a \leq \sqrt{n}$. Como $b > 1$, segue que b possui pelo menos um divisor primo p. Agora, como $p \mid a$, segue que $p^2 \mid a^2$, e assim, $p^2 \leq a^2$. Como $p \mid a$ e $a \mid n$, segue que $p \mid n$, ou seja, $p \leq \sqrt{n}$. □

Exemplo 5.1.7. *O número* 211 *é um número primo. Como* $\sqrt{211} \approx 15$*, segue que para sabermos se é composto é suficiente verificarmos se existe um inteiro entre* 2 *e* $\sqrt{211}$ *(inclusive) que divida* 211*. Sabendo que não existe esse divisor, segue pelo Teorema 5.1.4, segue que* 211 *é um número primo.*

Exemplo 5.1.8. *O método chamado Crivo de Eratóstenes é utilizado para determinar os números primos de* 1 *até um certo* n*. O método consiste em eliminar os múltiplos dos primos que*

são menores que $\sqrt{n}$. *Por exemplo, encontremos os números primos menores que* 50. *Como* $7 < \sqrt{50}$, *é suficiente eliminar os múltiplos de* $2, 3, 5$ *e* 7. *Dessa forma,*

	2	3	$\not{4}$	5	$\not{6}$	7	$\not{8}$	$\not{9}$	$\not{10}$
11	$\not{12}$	13	$\not{14}$	$\not{15}$	$\not{16}$	17	$\not{18}$	19	$\not{20}$
$\not{21}$	$\not{22}$	23	$\not{24}$	$\not{25}$	$\not{26}$	$\not{27}$	$\not{28}$	29	$\not{30}$
31	$\not{32}$	$\not{33}$	$\not{34}$	$\not{35}$	$\not{36}$	37	$\not{38}$	$\not{39}$	$\not{40}$
41	$\not{42}$	43	$\not{44}$	$\not{45}$	$\not{46}$	47	$\not{48}$	$\not{49}$	$\not{50}$.

Assim, o números primos menores que 50 *são* $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$ *e* 47.

Um número da forma $F_k = 2^{2^k} + 1$ é chamado número de Fermat. Fermat observou que $F_0 = 2^{2^0} + 1 = 3$, $F_1 = 2^{2^1} + 1 = 5$, $F_2 = 2^{2^2} + 1 = 17$, $F_3 = 2^{2^3} + 1 = 257$ e $F_4 = 2^{2^4} + 1 = 65537$ são números primos. Com isso, Fermat acabou conjecturando que todos os inteiros da forma $F_k = 2^{2^k} + 1$ são números primos. Mas, Euler descobriu que $F_5 = 2^{2^5} + 1$ não é um número primo, mostrando que 641 é um fator de F_5, ou seja,

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 2^{28}(5^4 + 2^4) - (5.2^7)^4 + 1 = 2^{28}.641 - (640^4 - 1) = 641(2^{28} - 639(640^2 + 1)).$$

Os númeos da forma $M_k = 2^k - 1$, para $k \geq 2$, são chamados de números de Mersene. Se M_k for primo, então k é primo, mas a reciproca é falsa, uma vez que $M_{11} = 2047 = 23.89$. Se M_k for primo, M_k é chamado primo de Mersene.

5.1.1 Exercícios

1. Sejam $a = 2^3.3^2.7^3.11^5$ e $b = 2^2.3^3.5^4.7.11^2.13^3$.
   (a) Determine o $mdc(a, b)$.
   (b) Determine o $mmc(a, b)$.
2. Se $p \in \mathbb{Z}$ é um número primo tal que $p \mid a_1 \dots a_n$, mostre que $p \mid a_i$ para algum $i = 1, 2, \dots, n$.
3. Mostre que $6 \mid n(2n + 7)(7n + 1)$, para todo $n \in \mathbb{Z}$.
4. Mostre que 30 divide $n(n^2 - 49)(n^2 + 49)$, para todo $n \in \mathbb{Z}$.
5. Se p é primo e $p \mid ab$, mostre que $p \mid a$ ou $p \mid b$.
6. Se $a^k - 1$ for primo, mostre que $a = 2$ e k é primo.
7. Determine os primos menores que 50.
8. Verifique que 271 é primo ou composto.
9. Se abc é o maior número de 3 algarismos divisível por 3, determine $a + b + c$.
10. Determine o números de elementos entre 1 e 1000 que é divisível por 9.

11. Determine a tau que $mdc(a, 384) = 48$, onde $a < 384$.

12. Se $n > 4$ é composto, mostre que n divide $(n-1)!$.

13. Se $p > 1$ e p divide $(p-1)! + 1$, mostre que p é primo.

14. Mostre que $n! + 1$ adimite um fator primo $p > n$, para todo n.

15. Se $n > 2$, mostre que existe um primo p entre n e $n!$.

16. Se $2^n - 1$, com $n \geq 2$, é primo, mostre que n é primo.

5.2 Congruências

Apresentamos, nesta seção, o conceito da relação de congruência introduzido por Karl Friedrich Gauss $(1777 - 1855)$ em 1801, que é uma importante ferramenta para Teoria dos Números. Veremos ainda que desta relação segue uma partição de $\mathbb{Z}$ em classes de equivalência que facilita o trabalho com congruências. Se o Natal em 2015 foi numa sexta feira, em que dia da semana será o Natal em 2050?

Definição 5.2.1. *Sejam $a, b, m \in \mathbb{Z}$ tal que $m > 1$. O elemento a é dito côngruo a b módulo m se $m \mid a - b$. Neste caso, a notação usada é $a \equiv b (mod\ m)$. Se a não é côngruo a b módulo m, usamos a notação $a \not\equiv b (mod\ m)$.*

Exemplo 5.2.1. *Tem-se que $24 \equiv 3 (mod\ 7)$, uma vez que $7 \mid 24 - 3 = 21$, mas $16 \not\equiv 9 (mod\ 4)$, uma vez que $4 \nmid 16 - 9 = 5$.*

Segue diretamente das propriedades de divisibilidade que se $a, b, c, d, m \in \mathbb{Z}$ com $m > 1$, então

1. $a \equiv a (mod\ m)$, ou seja, é reflexiva. Segue do fato que $m \mid 0 = a - a$, para todo $a \in \mathbb{Z}$.

2. Se $a \equiv b (mod\ m)$, então $b \equiv a (mod\ m)$, ou seja, é simétrica. Com efeito, por hipótese, $m \mid (a - b)$, e assim, $a - b = mq$, onde $q \in \mathbb{Z}$. Assim, $b - a = m(-q)$. Logo, $m \mid (b - a)$, ou seja, $b \equiv a (mod\ m)$.

3. Se $a \equiv b (mod\ m)$ e $b \equiv c (mod\ m)$, então $a \equiv c (mod\ m)$, ou seja, é transitiva. Com efeito, por hipótese, $m \mid (a - b)$ e $m \mid (b - c)$, ou seja, $a - b = mq_1$ e $b - c = mq_2$, onde $q_1, q_2 \in \mathbb{Z}$. Subtraindo, segue que $a - c = m(q_1 + q_2)$, ou seja, $a \equiv c (mod\ m)$.

Portanto, a relação de congruência é uma relação de equivalência.

Propriedades 5.2.1. *Sejam $a, b, c, m \in \mathbb{Z}$ com $m > 1$.*

1. *$a \equiv b(mod\ m)$ se, e somente se, a e b fornecem o mesmo resto quando divididos por m. De fato, se $a \equiv b(mod\ m)$, então $m \mid a-b$, ou seja, $a-b=mq$, para algum $q \in \mathbb{Z}$. Na divisão euclidiana de b por m, segue que $b=mq_1+r$, onde $q_1, r \in \mathbb{Z}$ com $0 \leq r < m$. Assim, $a=b+mq=m(q+q_1)+r$. Como $0 \leq r < m$, segue que r também é o resto da divisão de a por m. Reciprocamente, se $a=mq_1+r$ e $b=mq_2+r$, com $q_1, q_2, r \in \mathbb{Z}$ e $0 \leq r < m$, então $a-b=m(q_1-q_2)$. Portanto, $a \equiv b(mod\ m)$.*

2. *Se $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$, então $a \pm c \equiv b \pm d(mod\ m)$. De fato, Por hipótese, $m \mid a-b$ e $m \mid c-d$. Assim, $m \mid (a-b) \pm (c-d)$, ou seja, $m \mid (a \pm c)-(b \pm d)$. Portanto, $a \pm c \equiv b \pm d(mod\ m)$.*

3. *Se $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$, então $ac \equiv bd(mod\ m)$. De fato, por hipótese, $m \mid a-b$ e $m \mid c-d$. Assim, $m \mid (a-b)c$ e $m \mid b(c-d)$, ou seja, $m \mid ac-bc$ e $m \mid bc-bd$. Assim, $m \mid ac-bd$, e portanto, $ac \equiv bd(mod\ m)$.*

4. *Se $a \equiv b(mod\ m)$, então $a \pm c \equiv b \pm c(mod\ m)$ e $ac \equiv bc(mod\ m)$. De fato, por hipótese, $a-b=qm$, onde $q \in \mathbb{Z}$. Logo, $a=qm+b$, e assim, $a \pm c = qm+(b \pm c)$. Deste modo, $(a \pm c)-(b \pm c)=qm$, implicando que $a \pm c \equiv b \pm c(modm)$. Por outro lado, como $a-b=qm$, segue que $c(a-b)=cqm$. Assim, $ac-bc=(cq)m$, ou seja, $ac \equiv bc(mod\ m)$.*

5. *Se $a \equiv b(mod\ m)$, então $a^n \equiv b^n(mod\ m)$, para todo $n \geq 1$. De fato, a prova é feita por indução sobre n. Por hipótese, para $n=1$ a afirmação é verdadeira. Agora, suponhamos verdadeira para $n=k$, ou seja, $a^k \equiv b^k(mod\ m)$. Para $n=k+1$, como $a^{k+1}=a^k a$, $b^{k+1}=b^k b$, $a \equiv b(mod\ m)$ e $a^k \equiv b^k(mod\ m)$, segue que $a^{K+1} \equiv b^{k+1}(mod\ m)$.*

6. *Se $ca \equiv cb(mod\ m)$ e $mdc(m,c)=d$, então $a \equiv b(mod\ \frac{m}{d})$. De fato, por hipótese, $c(a-b)=qm$, onde $q \in \mathbb{Z}$. Logo, $\frac{c}{d}(a-b)=q\frac{m}{d}$ e como $mdc(\frac{c}{d}, \frac{m}{d})=1$, segue que $\frac{m}{d} \mid (a-b)$, ou seja, $a \equiv b(mod\ \frac{m}{d})$.*

7. *Se $ca \equiv cb(mod\ m)$ e $mdc(m,c)=1$, então $a \equiv b(mod\ m)$. De fato, segue diretamente da propriedade anterior tomando $d=1$.*

8. *Se $ca \equiv cb(mod\ p)$, onde p é primo e $p \nmid c$, então $a \equiv b(mod\ p)$. De fato, como p é primo e $p \nmid c$, segue que $mdc(p,c)=1$. Assim, o resultado segue da propriedade anterior.*

9. *Se $a+b \equiv c(mod\ m)$, então $a \equiv c-b(mod\ m)$. De fato, como $a+b \equiv c(mod\ m)$ e $-b \equiv -b(mod\ m)$, segue que $a \equiv c-b\ (mod\ m)$.*

Exemplo 5.2.2. *Se $27 \equiv 9\ (mod\ 9)$, então $27=9.3+0$ e $9=9.1+0$ e, portanto, 27 e 9 deixam o mesmo resto quando divididos por 9. Além disso, como $33 \equiv 15(mod\ 9)$, ou seja, $3.11 \equiv 3.5(mod\ 9)$ e $mdc(3,9)=3$, segue que $11 \equiv 5(mod\ 3)$.*

Proposição 5.2.1. *Se $a \equiv b(mod\ m_1)$, $a \equiv b(mod\ m_2)$ e $mdc(m_1,m_2)=1$, então $a \equiv b(mod\ m_1m_2)$.*

Demonstração. Como $a \equiv b(mod\ m_1)$, segue que $a-b=m_1q$, para algum $q \in \mathbb{Z}$. Além disso, como $a \equiv b(mod\ m_2)$, segue que $m_2 \mid a-b$, ou seja, $m_2 \mid m_1q$. Como $mdc(m_1,m_2)=1$, segue

que $m_2 \mid q$, ou seja, $q = m_2 q_1$, com $q_1 \in \mathbb{Z}$. Assim, $a - b = m_1 m_2 q_1$, ou seja, $m_1 m_2 \mid a - b$ e, portanto, $a \equiv b (mod\ m_1 m_2)$. □

A relação de congruência é bastante útil para saber se um certo número divide outro, ou seja, para verificar se um número é divisível por outro. Por exemplo, será que 11 divide $10^{200} - 1$? Como $10 \equiv -1\ (mod\ 11)$, segue que $10^{200} \equiv (-1)^{200} (mod\ 11)$, ou seja, $10^{200} \equiv 1 (mod\ 11)$. Portanto, $10^{200} - 1 \equiv 0\ (mod\ 11)$, e assim, 11 divide $10^{200} - 1$.

5.2.1 Exercícios

1. Mostre que a soma de dois números pares é um número par.
2. Mostre que a soma de dois números ímpares é um número par.
3. Mostre que a soma de um número par com um número impar é um número impar.
4. Mostre que a soma de dois números racionais é um número racional.
5. Mostre que o produto de dois números racionais é um número racional.
6. Mostre que o quadrado de um número impar é da forma $8n + 1$, onde $n \in \mathbb{Z}$.
7. Determine o resto da divisão de: 7^{12} por 4, 4^{15} por 7, 7^{30} por 11 e $2^{20} - 1$ por 41.
8. Determine o resto da divisão de 1073.640.2650 por 7.
9. Determine o último dígito dos números 345271^{79399} e 4321^{4321}.
10. Determine o resto da divisão de $531.31^2.2$ por 7.
11. Determine o algarismo das unidades de 9^{9^9} e 7^{7^7}.
12. Determine um critério de divisibilidade por 2.
13. Determine um critério de divisibilidade por 3.
14. Determine um critério de divisibilidade por 4.
15. Determine um critério de divisibilidade por 5.
16. Determine um critério de divisibilidade por 6.
17. Determine um critério de divisibilidade por 7.
18. Determine um critério de divisibilidade por 8.
19. Determine um critério de divisibilidade por 9.
20. Determine um critério de divisibilidade por 10.
21. Determine um critério de divisibilidade por 11.

5.3 Função de Euler

A função que apresentamos a seguir foi introduzida por Leonhard Euler $(1707 - 1783)$ em 1760, motivado por um problema proposto por Fermat. Vejamos a definição e as propriedades dessa importante função para a teoria dos números.

Definição 5.3.1. *A função $\varphi : \mathbb{N} - \{0\} \to \mathbb{N} - \{0\}$ associa cada $n \in \mathbb{N} - \{0\}$ ao número de elementos de $\{k \in \mathbb{N} - \{0\} | 1 \leq k \leq n$ e $mdc(k, n) = 1\}$ é chamada função φ de Euler.*

Exemplo 5.3.1. *Para $n = 8$, segue que $\varphi(8) = 4$, uma vez que são 4 os números de 1 a 8 que são primos com 8 são $1, 3, 5$ e 7.*

Teorema 5.3.1. *Se p é um primo e k um inteiro positivo, então $\varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$.*

Demonstração. Como entre 1 e p^k os únicos elementos não primos com p^k são $p, 2p, 3p, \cdots, (p^{k-1})p$, segue que existem p^{k-1} não primos com p. Assim, $\varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$. □

Exemplo 5.3.2. *Se $n = 8 = 2^3$, então $\varphi(2^3) = 2^3(1 - \frac{1}{2}) = 4$.*

Corolário 5.3.1. *Se p é um primo, então $\varphi(p) = p - 1$.*

Demonstração. Seja p um primo. Como de 1 a p o único elemento não primo com p é o próprio p, segue que $\varphi(p) = p - 1$. □

Corolário 5.3.2. *Se $\varphi(p) = p - 1$, então p é um primo.*

Demonstração. Se p fosse composto, então p teria pelo menos um divisor d tal que $1 < d < p$. Assim, no mínimo dois inteiros entre 1 e p não seriam primos com p. Portanto, $\varphi(p) \leq p - 2$, o que é uma contradição. Assim, p é um primo. □

Proposição 5.3.1. *Se m e n são números naturais não-nulos e primos entre si, então $\varphi(mn) = \varphi(m)\varphi(n)$, ou seja, a função φ de Euler é multiplicativa.*

Demonstração. Seja o seguinte tabela formada por todos os naturais de 1 a mn

$$\begin{array}{ccccccc}
1 & 2 & 3 & \cdots & h & \cdots & n \\
n+1 & n+2 & n+3 & \cdots & n+h & \cdots & 2n \\
2n+1 & 2n+2 & 2n+3 & \cdots & 2n+h & \cdots & 3n \\
\vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
(m-1)n+1 & (m-1)n+2 & (m-1)n+3 & \cdots & (m-1)n+h & \cdots & mn
\end{array}$$

Como $mdc(qn + h, n) = mdc(h, n)$, segue que os inteiros da h-ésima coluna são primos com n se, e somente se, h é primo com n. Como, na primeira linha, o número de inteiros que são primos com n é $\varphi(n)$, segue que existem somente $\varphi(n)$ colunas formadas com inteiros que são primos com n. Por outro lado, em cada uma dessas $\varphi(n)$ colunas existem $\varphi(m)$ elementos que são primos com m. Assim, o número total de inteiros que são primos com n e com m, ou seja, o núneri de primos com mn é exatamente $\varphi(m)\varphi(n)$, ou seja, $\varphi(mn) = \varphi(m)\varphi(n)$. □

Teorema 5.3.2. *Se $n > 1$ é um inteiro cuja decomposição em primos é $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$, então $\varphi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r})$.*

Demonstração. Pelo Teorema 5.3.1, segue que $\varphi(p_i^{k_i}) = p_i^{k_i}(1-\frac{1}{p_i})$. Pela Proposição 5.3.1, segue que $\varphi(m) = \varphi(p_1^{k_1})\varphi(p_2^{k_2})\cdots\varphi(p_r^{k_r}) = p_1^{k_1}(1-\frac{1}{p_1})p_2^{k_2}(1-\frac{1}{p_2})\cdots p_r^{k_r}(1-\frac{1}{p_r}) = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r}) = m(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r})$. □

Exemplo 5.3.3. *Para o número 28, segue que $\varphi(28) = \varphi(2^2.7) = 2^2(1-\frac{1}{2}).7(1-\frac{1}{7}) = 12$.*

Corolário 5.3.3. *Se $d \mid n$, então $\varphi(d) \mid \varphi(n)$.*

Demonstração. Seja d um inteiro tal que $d \mid n$. Assim, a decomposição em primos de d é dada por $d = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$. Como $d \mid n$, segue que $n = dq_1$, onde $q_1 \in \mathbb{Z}$. Assim, a decomposição de n em fatores primos é dada por $n = (p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r})p_{r+1}^{k_{r+1}}p_{r+2}^{k_{r+2}}\cdots p_s^{k_s}$, onde $r < s$. Assim, pelo Teorema 5.3.2, segue que $\varphi(d) = d(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r})$, e desse modo, $\varphi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r})(1-\frac{1}{p_{r+1}})\cdots(1-\frac{1}{p_s})$. Logo, $\varphi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r})(1-\frac{1}{p_{r+1}})\cdots(1-\frac{1}{p_s}) = dq_1(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r})(1-\frac{1}{p_{r+1}})\cdots(1-\frac{1}{p_s}) = \varphi(d)q_1(1-\frac{1}{p_{r+1}})\cdots(1-\frac{1}{p_s})$. Portanto, $\varphi(d) \mid \varphi(n)$. □

Corolário 5.3.4. *Se $n > 1$, então $\varphi(n^2) = n\varphi(n)$.*

Demonstração. A decomposição em primos de n é dada por $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$. Assim, a decomposição em primos de n^2 é dada por $n^2 = p_1^{2k_1}p_2^{2k_2}\cdots p_r^{2k_r}$. Pelo Teorema 5.3.2, segue que $\varphi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r})$. Portanto, $\varphi(n^2) = nn(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r}) = n\varphi(n)$. Logo, $\varphi(n^2) = n\varphi(n)$. □

Teorema 5.3.3. *(Euler) Se $m > 1$ e $a \in \mathbb{Z}$ é tal que $mdc(m,a) = 1$, então $a^{\varphi(m)} \equiv 1 \ (mod\ m)$.*

Demonstração. Sejam s_i os inteiros entre 1 e m, com $1 \leq i \leq k$, tal que $mdc(m, s_i) = 1$. Assim, $k = \varphi(m)$. A divisão de as_i por m é dada por $as_i = mq_i + r_i$, onde $0 \leq r_i < m$. Assim, m e r_i são primos entre si, para todo i, uma vez que se existisse um primo p tal que $p \mid m$ e $p \mid r_i$, então $p \mid as_i$, e assim, $mdc(k,m) = 1$. Ainda, entre os $r_1, r_2, \cdots, r_k$ não existem elementos repetidos, pois se $r_i = r_j$, com $i \leq 1, j \leq k; i \neq j$, então $as_i - mq_i = as_j = mq_j$ ou seja, $a(s_i - s_j) = m(q_i - q_j)$. Como $mdc(a,m) = 1$, segue que $m \mid (s_i - s_j)$. Agora, como $1 \leq s_i, s_j \leq m$, segue que teríamos $s_i = s_j$, o que é impossível, uma vez que $i \neq j$. Desse modo, $\{s_1, s_2, \cdots, s_k\} = \{r_1, r_2, \cdots, r_k\}$. Assim, $as_i \equiv r_i \pmod m$. Se multiplicarmos todos as congruências, para $1 \leq i \leq k$, então $a^k s_1 s_2 \cdots s_k \equiv r_1 r_2 \cdots r_k \pmod m$. Como m é primo com cada s_i e r_i e ainda como $s_1 s_2 \cdots s_k = r_1 r_2 \cdots .r_k$, segue que $a^k = a^{\varphi(m)} \equiv 1 \pmod m$. □

Exemplo 5.3.4. *O valor de x tal que $7^{1000} \equiv x \ (mod\ 54)$ é 7, uma vez que como $\varphi(54) = 18$, segue que $7^{18} \equiv 1 \ (mod\ 54)$. Como $1000 = 18.55 + 10$, segue que $7^{1000} \equiv 7^{10} \ (mod\ 54)$. Mas, $7^2 \equiv -5 \ (mod\ 54)$, $7^4 \equiv 25 \ (mod\ 54)$, $7^8 \equiv 31 \ (mod\ 54)$, e assim, $7^{10} \equiv 7 \ (mod\ 54)$. Portanto, $x = 7$.*

Teorema 5.3.4. *Se $n > 2$, então $\varphi(n)$ é um inteiro par.*

Demonstração. Se n possui na sua decomposição uma potência de 2, ou seja, $n = 2^k m$ para algum $k \in \mathbb{Z}$, $k > 1$, e $mdc(2, m) = 1$, então $\varphi(n\varphi(2m)) = 2^k(1 - \frac{1}{2})\varphi(m) = 2^{k-1}\varphi(m)$, e portanto, $2 \mid \varphi(n)$, ou seja, $varphi(n)$ é par. Agora, n não possui uma potência de 2 como fator, então n é divisível por um primo ímpar p tal que $n = p^k m$, onde $k \geq 1$ e $mdc(p^k, m) = 1$. Logo, $\varphi(n) = \varphi(p^k)\varphi(m) = p^k(1 - \frac{1}{p})\varphi(m) = p^{k-1}(p - 1)\varphi(m)$. Como p é um primo ímpar, segue que $2 \mid (p - 1)$, ou seja, $\varphi(n)$ é par. Portanto, $\varphi(n)$ é par para todo $n > 2$. □

Teorema 5.3.5. *Se p é um primo, então* $\sum_{i=0}^{k} \varphi(p^i) = p^k$.

Demonstração. Como p é um primo, segue que $\varphi(p) = p - 1$, $\varphi(p^2) = p(p - 1)$, $\cdots$, $\varphi(p^k) = p^{k-1}(p - 1)$. Somando as igualdades, segue que $\sum_{i=1}^{k} \varphi(p^i) = (p - 1)(1 + p + p^2 + \cdots + p^{k-1}) = (p - 1)(\frac{p^k - 1}{p - 1}) = p^k - 1$. Mas, $\sum_{i=0}^{k} \varphi(p^i) = \varphi(1) + \sum_{i=1}^{k} \varphi(p^i) = 1 + p^k - 1 = p^k$. □

Teorema 5.3.6. *(Gauss) Se $n \geq 1$, então* $\sum_{d|n} \varphi(d) = n$.

Demonstração. Separamos o conjunto $S = 1, 2, 3, \cdots, n$ em classes A_d tal que d divida n. Agora, em cada classe A_d colocamos todos os elementos m tal que $1 \leq m \leq n$ e $mdc(m, n) = d$. Assim, $mdc(\frac{m}{d}, \frac{n}{d}) = 1$, ou seja, m está em A_d se $\frac{m}{d}$ for primo com $\frac{n}{d}$. Logo, A_d tem $\varphi(\frac{n}{d})$ elementos. Como cada elemento se encontra em somente uma das classes, segue que $\sum_{d|n} \varphi(\frac{n}{d}) = n$. O fato de que quando d percorre todos os divisores de n, o mesmo acontece com $\frac{n}{d}$. Portanto, $\sum_{d|n} \varphi(d) = n$. □

Exemplo 5.3.5. *Se $n = 18$, então $\varphi(18) = 6$ e $D_{(18)} = \{d \in \mathbb{Z} |\ d \mid 18\} = \{1, 2, 3, 6, 9, 18\}$. Assim,* $\sum_{d|18} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) + \varphi(9) + \varphi(18) = 1 + 1 + 2 + 2 + 6 + 6 = 18$.

Teorema 5.3.7. *Se $n > 1$, então a soma dos inteiros menores do que n que são primos com n é $\frac{1}{2}n\varphi(n)$.*

Demonstração. Sejam $a_1, a_2, \cdots, a_{\varphi(n)}$ os inteiros menores que n e que são primos com n. Como $mdc(a, n) = 1$, para todo a_i onde $i = 1, 2, \cdots, \varphi(n))$, segue que $mdc(n - a, n) = 1$, e assim, os a_i podem serem expressos pelas diferenças $(n - a_1, n - a_2, \cdots, n - a_{\varphi(n)})$. Assim, $a_1 + a_2 + \cdots + a_{\varphi(n)} = (n - a_1) + (n - a_2) + \cdots + (n - a_{\varphi(n)}) = n\varphi(n) - (a_1 + a_2 + \cdots . + a_{\varphi(n)})$. Portanto, $2(a_1 + a_2 + \cdots + a_{\varphi(n)}) = n\varphi(n)$, ou seja, $\sum_{i=1}^{\varphi(n)} a_i = \frac{1}{2}n\varphi(n)$. □

Exemplo 5.3.6. *Se $n = 2^k$, onde $k \geq 1$, então* $\sum_{i=1}^{4} \varphi(2^k) = \varphi(1) + \varphi(2) + \varphi(4) + \varphi(8) + \varphi(16) = 1+1+2+4+8 = 16 = 2^4$. *Em particular, se $n = 8$, então $\{k \in \mathbb{N} - \{0\} | 1 \leq k \leq m$ e $mdc(k, m) = 1\} = \{1, 3, 5, 7\}$. Portanto, a soma dos elementos desse conjunto é $16 = \frac{1}{2}.8.4$.*

5.3.1 Exercícios

1. Calcule $\varphi(15)$, $\varphi(420)$, $\varphi(5040)$ e $\varphi(8316)$.
2. Mostre que $\varphi(n)$ é um número par para todo $n > 2$.
3. Se p é um primo, calcule $(\varphi(p)\sigma(p) + 1)/p$.
4. Mostre que $\varphi(n^2) = n\varphi(n)$, para todo n.
5. Se n é um inteiro positivo ímpar, mostre que $\varphi(2n) = \varphi(n)$ e $\varphi(4n) = 2\varphi(n)$.
6. Se $mdc(m, n) = 2$, mostre que $\varphi(m, n) = 2\varphi(m)\varphi(n)$.
7. Se n é par, mostre que $\varphi(2n) = 2\varphi(n)$.
8. Mostre que $\varphi(3n) = 3\varphi(n)$ se, e somente se, $3 \mid n$.
9. Mostre que $\varphi(n) = n/2$ se, e somente se, $n = 2^k$, onde $k \geq 1$.
10. Mostre que $\sqrt{n}/2 \leq \varphi(n) \leq n$, para todo n.
11. Se $n > 1$, tem k fatores primos distintos, mostre que $\varphi(n) \geq n/2^k$.
12. Se $n > 1$ é composto, mostre que $\varphi(n) \leq n - \sqrt{n}$.
13. Se n tem k fatores primos ímpares distintos, mostre que $2^k \mid \varphi(n)$.
14. Se n e $n + 2$ são primos gêmeos, mostre que $\varphi(n + 2) = \varphi(n) = 2$.
15. Se $n = 2^k$ ou $n = 2^k 3^j$, onde k e j são inteiros positivos, mostre que $\varphi(n) \mid n$.
16. Sejam m e n números inteiros positivos. Mostre que:
    (a) $\varphi(m)\varphi(n) = \varphi(mn)\varphi(d)/d$, onde $d = mdc(m, n)$.
    (b) $\varphi(m)\varphi(n) = \varphi(mdc(m, n))\varphi(mmc(m, n))$.
17. Mostre que não existe n tal que $\varphi(n) = 14$.
18. Seja $f(n) = (n + \varphi(n))/2$. Se $n = 2^k$, onde $k \geq 2$, mostre que $f(f(n)) = \varphi(n)$.
19. Determine todas as soluções de $\varphi(n) = 4$.
20. Se 6 divide n, mostre que $\varphi(n) \leq n/3$.
21. Determine os valores de n tal que
    (a) $\varphi(n) = 16$
    (b) $\varphi(n) = 20$
    (c) $\varphi(n) = 30$.

(d) Se p é um primo e $2p+1$ é composto, mostre que não existe n tal que $\varphi(n) = 2p$.

22. Mostre que $\varphi(n) = n/3$ se, e somente se, $n = 2^k 3^l$, onde $k, l \in \mathbb{N}$.

23. Calcule $\sum_{d|n} (-1)^{n/d} \varphi(d)$, onde

(a) $n = 11, 13, 14, 15, 16$.

(b) $n = p$ com p um primo.

(c) $n = 2^k$, onde $k \geq 1$.

(d) $n = p^k$, onde $k \geq 1$ e p um primo ímpar.

5.4 Teoremas de Euler, Fermat e Wilson

O objetivo desta seção é o estudo dos teoremas de Euler, Fermat e Wilson que propõem informações importantes sobre primalidade e que auxiliam no trabalho das congruências. O resultado, conhecido por Pequeno Teorema de Fermat, foi proposto por Fermat em 1640, porém não deixou nenhuma demonstração do resultado. Assim, em 1736, Euler apresenta a primeira demonstração do teorema e alguns anos depois consegue uma generalização do resultado, que recebe o nome de Teorema de Euler. Para tanto, Euler precisou introduzir a função φ.

Teorema 5.4.1. *(Euler) Para todo inteiro $m > 1$ e para todo $a \in \mathbb{Z}$, primo com m, vale a congruência*

$$a^{\varphi(m)} \equiv 1 \ (mod\ m).$$

Demonstração. Consideremos o conjunto

$$S = \{s \in \mathbb{Z} : \ 1 \leq s \leq m \ e \ mdc(s, m) = 1\} = \left\{s_1, s_2, \cdots, s_{\varphi(m)}\right\}.$$

Para cada s_i, onde $i = 1, 2, \cdots, \varphi(m)$, façamos a divisão de as_i por m. Logo,

$$as_i = mq_i + r_i, \ onde \ q_i, r_i \in \mathbb{Z} \ e \ 0 \leq r_i < m.$$

Assim, $mdc(r_i, m) = 1$, para $i = 1, 2, \cdots, \varphi(m)$, pois se existisse $p \in \mathbb{Z}$ tal que $p \mid m$ e $p \mid r_i$, então $p \mid as_i$. Assim, $p \mid a$ ou $p \mid s_i$, o que é impossível, já que $mdc(a, m) = 1$ e $mdc(s_i, m) = 1$. Ainda, do conjunto $R = \left\{r_1, r_2, \cdots, r_{\varphi(m)}\right\}$ não existe elementos repetidos, pois se $r_i = r_j$, para $i \neq j$ com $0 \leq i, j < \varphi(m)$, então $as_i - mq_i = as_j - mq_j$, implicando em $a(s_i - s_j) = m(q_i - q_j)$. Como $mdc(m, a) = 1$, segue que $m \mid (s_i - s_j)$. Mas, $1 \leq s_i, s_j < m$, o que resultaria em $s_i = s_j$, o que não é possível, pois $i \neq j$. Logo, $S = R$. Assim, multiplicando as congruências $as_i \equiv r_i \ (mod\ m)$, para $i = 1, 2, \cdots, \varphi(m)$, segue que

$$(as_1)(as_2)\cdots(as_{\varphi(m)}) = a^{\varphi(m)} s_1 s_2 \cdots s_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} \ (mod\ m).$$

Como m é primo com cada elemento do produto $s_1 s_2 \cdots s_{\varphi(m)}$ que é igual a $r_1 r_2 \cdots r_{\varphi(m)}$, segue que

$$a^{\varphi(m)} \equiv 1 \ (mod\ m),$$

o que prova o resultado. □

Exemplo 5.4.1. *Tomando $p = 8$ e $a = 5$, verifiquemos que o teorema é válido. Assim, $\varphi(8) = 4$ e $mdc(8, 5) = 1$, e desse modo, $5^4 = 5^2.5^2 = 25.25 \equiv 1.1\ (mod\ 8)$.*

Teorema 5.4.2. *(Pequeno Teorema de Fermat) Se $p > 1$ é um inteiro primo e a um inteiro tal que $p \nmid a$, então*

$$a^{p-1} \equiv 1\ (mod\ p).$$

Demonstração. Como p é primo, segue, do Corolário 4.3 do relatório anterior, que $\varphi(p) = p-1$. Assim, sendo a primo com p, pelo Teorema de Euler, segue que

$$a^{\varphi(p)} = a^{p-1} \equiv 1\ (mod\ p),$$

o que prova o resultado. □

Teorema 5.4.3. *(Fermat) $p > 1$ é um inteiro primo, então*

$$a^p \equiv a\ (mod\ p),$$

para todo $a \in \mathbb{Z}$.

Demonstração. Se $p \mid a$, então $a \equiv 0\ (mod\ p)$ e, daí, $a^p \equiv 0\ (mod\ p)$. Desse modo, $a^p \equiv a\ (mod\ p)$. Se, ao invés, $p \nmid a$, então, pelo Pequeno Teorema de Fermat, $a^{p-1} \equiv 1\ (mod\ p)$. Multiplicando a congruência por a segue que $a^p \equiv a\ (mod\ p)$. Portanto, $a^p \equiv a\ (mod\ p)$, para todo $a \in \mathbb{Z}$. □

Exemplo 5.4.2. *Mostremos que $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1\ (mod\ p)$, para $p > 2$ primo. Como, pelo Teorema 5.4.3, $1^{p-1} \equiv 1\ (mod\ p)$, $2^{p-1} \equiv 1\ (mod\ p)$, $\cdots$, $(p-1)^{p-1} \equiv 1\ (mod\ p)$, então somando todas as parcelas segue que $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv p - 1 \equiv -1\ (mod\ p)$.*

Teorema 5.4.4. *Sejam p e q dois primos positivos distintos e $a \in \mathbb{Z}$. Se $a^p \equiv a\ (mod\ q)$ e $a^q \equiv a\ (mod\ p)$, então $a^{pq} \equiv a\ (mod\ pq)$.*

Demonstração. Do Teorema 5.4.3, segue que

$$(a^p)^q \equiv (a^p)\ (mod\ q)\ e\ (a^q)^p \equiv (a^q)\ (mod\ p).$$

Da hipótese, $a^p \equiv a\ (mod\ q)$ e $a^q \equiv a\ (mod\ p)$, logo, $a^{pq} \equiv a\ (mod\ q)$ e $a^{pq} \equiv a\ (mod\ p)$, ou seja, $q \mid (a^{pq} - a)$ e $p \mid (a^{pq} - a)$. Como $mdc(p, q) = 1$, segue que $pq \mid (a^{pq} - a)$, isto é, $a^{pq} \equiv a\ (mod\ pq)$, como queríamos. □

Exemplo 5.4.3. *Vamos verificar o Pequeno Teorema de Fermat com $a = 3$ e $p = 17$. O número 17 é um primo e não divide 3. Pelo Teorema 5.4.2, segue que $3^{17-1} = 3^{16} \equiv 1(mod\ 17)$. Sem usar o Teorema 5.4.2 também podemos chegar a esta conclusão facilmente, pois, como:*

$$3^3 = 27 \equiv 10(mod\ 17) \rightarrow 3^6 \equiv 100 \equiv -2(mod\ 17)$$

e

$$3^{12} \equiv 4(mod\ 17),$$

segue que

$$3^{17-1} = 3^{16} = 3^{12}.3^3.3 \equiv 4.10.3 \equiv 120 \equiv 1(mod\ 17).$$

Exemplo 5.4.4. *Mostramos que* $5^{38} \equiv 4(mod\ 11)$. *De fato, pelo Teorema* 5.4.2*:*

$$5^{10} \equiv 1(mod\ 11) \ \rightarrow \ 5^{38} = 5^{10.3+8} = (5^{10})^3(5^2)^4 \equiv 1^3.3^4 \equiv 81 \equiv 4(mod\ 11).$$

Exemplo 5.4.5. *O número* 117 *é composto. Para mostrarmos essa afirmação, basta acharmos um inteiro a tal que* a^{117} *não seja côngruo à a módulo* 117. *Tomando* $a = 2$, *segue que*

$$2^{117} = 2^{7.16+5} = (2^7)^{16}.2^5$$

Por outro lado, observemos que

$$2^7 = 128 \equiv 11(mod\ 117).$$

Assim,

$$2^{117} \equiv 11^{16}.2^5 \equiv (121)^8.2^5 \equiv 4^8.2^5 \equiv 2^{21}(mod\ 117).$$

Ainda, $2^{21} = (2^7)^3$, *o que nos dá que:*

$$2^{21} \equiv 11^3 \equiv 121.11 \equiv 4.11 \equiv 44(mod\ 117).$$

Portanto,

$$2^{117} \equiv 44$$

e 44 *não é côngruo a* 2 *módulo* 117, *e desse modo, o inteiro* 117 *é composto* $(117 = 9.13)$.

Vejamos agora um exemplo interessante, o qual mostra que a recíproca do Pequeno Teorema de Fermat, isto é: se $a^{n-1} \equiv 1(mod\ n)$, então n é primo, é falsa.

Exemplo 5.4.6. *O inteiro* $2^{340} \equiv 1(mod\ 341)$. *Com efeito, observe que:*

$$341 = 11.31 \quad e \quad 2^{10} = 1024 = 31.33 + 1 = 11.93 + 1.$$

Mas isto significa que

$$2^{10} \equiv 1(mod\ 31) \quad e \quad 2^{10} \equiv 1(mod\ 11).$$

Portanto,

$$2^{11} = 2.2^{10} \equiv 2.1 \equiv 2(mod\ 31) \ \ e \ \ 2^{31} = 2(2^{10})^3 \equiv 2.1^3 \equiv 2(mod\ 11).$$

Ainda, os inteiros 11 *e* 31 *são primos. Dai, que pelo Teorema 5.4.4, segue que*

$$2^{11.31} \equiv 2(mod\ 11.31) \quad ou \quad 2^{341} \equiv 2(mod\ 341)$$

de onde segue que $2^{340} \equiv 1(mod\ 341)$.

No que segue, veremos um resultado que foi enunciado pela primeira vez em *Meditationes Algebraicae* (1770) no trabalho do matemático inglês Edward Waring. A interessante propriedade informada por John Wilson (1741-1793) a Waring não foi provada, cabendo, em 1771, a Lagrange a demonstração do que hoje é conhecido como Teorema de Wilson.

Proposição 5.4.1. *Se* $p > 2$ *é um inteiro primo e* $2 \leq a \leq p-2$*, então existe um único* $b \in \{2, 3, \cdots, p-3, p-2\}$*, com* $b \neq a$*, tal que* $ab \equiv 1\ (mod\ p)$.

Demonstração. Considerando a congruência linear $ax \equiv 1\ (mod\ p)$, sendo $mdc(a,p) = 1$, pois $2 \leq a \leq p-2$, segue que a congruência admite uma única solução $b \in \{1, 2, \cdots, p-1\}$. De fato, $b \neq a$, pois se tivéssemos $b = a$, então $a^2 \equiv 1\ (mod\ p)$
$rightarrowa^2 - 1 = (a-1)(a+1) \equiv 0\ (mod\ p)$ e daí, $p \mid (a-1)$ ou $p \mid (a+1)$, o que não ocorre, já que $2 \leq a \leq p-2$. Ainda, $b \neq 1$ e $b \neq p-1$, pois caso $b = 1$ segue que $a \equiv 1\ (mod\ p)$, ou seja, $p \mid (a-1)$, o que já vimos anteriormente que não acontece. No caso $b = p-1$, segue que $a(p-1) = ap - a \equiv 1\ (mod\ p)$ e daí, $p \mid ap - (a+1)$, implicando em $p \mid (a+1)$, o que também não acontece. □

Teorema 5.4.5. *(Wilson) Se* $p > 1$ *é primo, então* $(p-1)! \equiv -1\ (mod\ p)$.

Demonstração. Sendo p um inteiro primo, consideremos o fatorial $(p-1)!$. Pela proposição anterior, segue que para todo $a \in \{2, 3, \cdots, p-2\}$, existe um único $b \in \{2, 3, \cdots, p-2\}$ tal que $ab \equiv 1\ (mod\ p)$. Desse modo, podemos agrupar dois a dois os inteiros $2, 3, \cdots, p-2$ de forma que $a_i b_i \equiv 1\ (mod\ p)$, para $i = 1, 2, \cdots, \frac{p-3}{2}$. e $a_i, b_i \in \{2, 3, \cdots, p-2\}$. Assim,

$$(p-1)! = 1.2.\cdots(p-2)(p-1) = 1.a_1b_1.a_2b_2\cdots a_{\frac{p-3}{2}}b_{\frac{p-3}{2}}.(p-1)$$
$$\equiv 1.1.1\cdots(p-1) \equiv p-1 \equiv -1\ (mod\ p).$$

Portanto, para todo primo p positivo, segue que $(p-1)! \equiv -1\ (mod\ p)$. □

Exemplo 5.4.7. *Para* $p = 7$*, pelo Teorema de Wilson, segue que* $(7-1)!+1 = 6!+1 = 720+1 = 721 = 7.103$*. Assim,*

$$(7-1)! + 1 \equiv 0(mod\ 7), \quad \textit{ou seja}, \quad (7-1)! \equiv -1(mod\ 7).$$

Veremos no próximo resultado que a recíproca do Teorema de Wilson também é válida.

Teorema 5.4.6. *Se* $(p-1)! \equiv -1\ (mod\ p)$*, então* p *é primo.*

Demonstração. Se p não é primo, então existe um divisor q com $1 < q < p$. Como q é um fator de p, segue que q é um dos fatores de $(p-1)!$, ou seja, $q \mid (p-1)!$. Ainda, pela hipótese, segue que $(p-1)! \equiv -1\ (mod\ p)$, ou seja, $(p-1)! = -1 + pk$, para algum $k \in \mathbb{Z}$. Assim, como $q \mid (p-1)!$ e $q \mid p$, segue que $q \mid 1$, o que é absurdo e, portanto, n é primo. □

Exemplo 5.4.8. *Utilizando a recíproca do Teorema de Wilson, vamos reconhecer se o inteiro 11 é primo. Mas isto é claro, pois observe que:*

$$(11-1)!+1 = 10!+1 = 1.2.3\cdots 10+1 = 3628801 = 11.329891.$$

Portanto, $(11-1)! \equiv -1(mod\ 11)$*, o que nos leva a conclusão de que o inteiro* 11 *é primo.*

Exemplo 5.4.9. *Da mesma forma, o inteiro* 13 *é primo, uma vez que*

$$(13-1)!+1 = 12!+1 = 1.2.3\cdots 12+1 = 479001601 = 13.36846277,$$

e portanto,

$$(13-1)! \equiv -1(mod\ 13).$$

5.4.1 Exercícios

1. Se p é um primo ímpar, mostre que $1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}}(mod/p)$.
2. Mostre que as soluções de $x^2+1 \equiv 0(mod\ p)$, onde $p = 4m+1$ é um primo, são $\pm 1 \cdot 2 \cdot \cdots \cdot 2m(mod\ p)$.
3. Seja p um número primo ímpar. Mostre que $1^2 \cdot 3^2 \cdots (p-2)^2 \equiv 2^2 \cdot 4^2 \cdots (p-1)^2(mod\ p)$.
4. Mostre que $p > 1$ é primo se, e somente se, $(p-2)! \equiv 1(mod\ p)$.
5. Mostre que todo número elevado a quarta potência deixa resto 0 ou 1 quando dividido por 5.
6. Mostre que $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1(mod\ p)$, onde p é um primo impar.
7. Se $mdc(a,5) = 1$, onde $a > 0$, mostre que $a^{8n} + 3a^{4n} + 1 \equiv 0(mod\ 5)$, para todo $n > 0$.
8. Seja p um primo impar. Mostre que a equação $x^2 + 1 \equiv 0(mod\ p)$ admite solução se, e somente se, $p \equiv 1(mod\ 4)$.
9. Mostre que $n > 1$ é um primo se, e somente se, $(n-2)! \equiv 1(mod\ n)$.
10. Se p e q são primos distintos tais que $a^p \equiv a(mod\ q)$ e $a^q \equiv a(mod\ p)$, mostre que $a^{pq} \equiv a(mod\ pq)$.

Capítulo

6

Dígitos verificadores

A maioria dos documentos oficiais tais como CPF, RG, CNPJ, Título de Eleitor, CNH e conta corrente, possuem, mesmo que de forma não explícita, alguns dígitos que verificam a validade dos demais. Esses dígitos são conhecidos como dígitos verificadores (DV) ou de controle de paridade. Em geral, esses dígitos verificadores vem no final e servem para validar a autenticidade do número de documento evitando assim erros de digitação, fraudes, etc.

Neste capítulo, apresentamos o processo para determinar os números verificadores do RG, CPF, ISBN, CNPJ e de algumas agências e contas bancárias.

6.1 Cálculo do RG

O número de um RG, em geral, é composto de 9 dígitos, onde oúltimo dígito é chamado de dígito verificador ou de controle (dígito que vem após o traço), ou seja,

$$x_1x_2.x_3x_4.x_5.x_6x_7x_8 - c_1c_2.$$

Esse dígito tem a função de verificar a validade e a autenticidade do número de um RG, evitando dessa forma fraudes ou erros de transmissão ou digitação.

O algoritmo é dado por

1. Começamos utilizando os 8 primeiros dígitos multiplicando-os pela sequência crescente de 2 à 9 e somamos esse resultado, ou seja,

$$L_1 = 2x_1 + 3x_2 + 4x_3 + 5x_4 + 6x_5 + 7x_6 + 8x_7 + 9x_8.$$

2. Dividindo L_1 por 11 obtemos r_1 como resto. O dígito c_1 é dado por $c_1 = 11 - r_1$ se $2 \leq r_1 < 10$, $c_1 = 0$ se $r_1 = 0$ e $c_1 = x$ se $r_1 = 1$.

Exemplo 6.1.1. *Seja* $56.843.539 - c_1$ *o número de um RG. Aplicando o algoritmo, segue que*

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	*Soma*
RG	*5*	*6*	*8*	*4*	*3*	*5*	*3*	*9*	
Peso	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	
Produto	*10*	*18*	*32*	*20*	*18*	*35*	*24*	*81*	*238*

Dividindo 238 *por* 11 *segue que o resto é* 7*, e assim,* $c_1 = 11 - 7 = 4$*. Portanto, o número do RG é dado por* $56.843.539 - 4$*.*

6.1.1 Exercícios

1. Determine o dígito verificador c dos seguintes RGs.
   (a) $11.786.234 - c$.
   (b) $33.221.321 - c$.
   (c) $12.321.332 - c$.
   (d) $65.324.322 - c$.
2. Determine o valor de x para que os seguintes números sejam números de RGs.
   (a) $1x.726.134 - 3$.
   (b) $32.2x1.331 - 7$.
   (c) $14.351.x32 - 9$.
   (d) $23.321.432 - 0$.

6.2 Cálculo do CPF

O CPF (Cadastro de Pessoa Física) é composto por 11 dígitos, onde os 2 últimos são os dígitos verificadores ou de controle de paridade, ou seja,

$$x_1x_2x_3x_4x_5x_6x_7x_8x_9 - c_1c_2,$$

onde c_1c_2 são os dígitos de controle. O cálculo desses dois dígitos de verificação é bem direto e realizado através de pesos associados a cada dígito e uma divisão pelo número primo 11 ao final.

O algoritmo é dado por

1. Começamos utilizando os 9 primeiros dígitos multiplicando-os pela sequência decrescente de 10 à 2 e somamos esse resultado, ou seja,

$$L_1 = 10x_1 + 9x_2 + 8x_3 + 7x_4 + 6x_5 + 5x_6 + 4x_7 + 3x_8 + 2x_9.$$

Dividindo L_1 por 11 obtemos r_1 como resto. O dígito c_1 é dado por $c_1 = 11 - r_1$ se $2 \leq r_1 < 10$ e $c_1 = 0$ se $r_1 = 0$ ou 1.

2. O cálculo do dígito c_2 é feito de modo semelhante considerando o primeiro dígito verificador c_1. Para isso, começamos utilizando os 10 primeiros dígitos multiplicando-os pela sequência decrescente de 11 à 2 e somamos esse resultado, ou seja,

$$L_2 = 11x_1 + 10x_2 + 9x_3 + 8x_4 + 7x_5 + 6x_6 + 5x_7 + 4x_8 + 3x_9 + 2c_1.$$

Novamente, dividimos L_2 por 11 e obtemos o resto r_2. O dígito $c_2 = 11 - r_2$ se $0 \leq r_2 < 10$ e $r_2 = 0$ se $r_1 = 0$ ou 1.

Exemplo 6.2.1. *Seja* $145.382.206 - c_1c_2$ *o número de um CPF. Aplicando o algoritmo para o cálculo de* c_1*, segue que*

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	*Soma*
CPF	*1*	*4*	*5*	*3*	*8*	*2*	*2*	*0*	*6*	
Peso	*10*	*9*	*8*	*7*	*6*	*5*	*4*	*3*	*2*	
Produto	*10*	*36*	*40*	*21*	*48*	*10*	*8*	*0*	*12*	*185*

O resto da divisão de 185 *por* 11 *é* 9*, e assim,* $c_1 = 11 - 9 = 2$*. Para o cálculo de* c_2*, segue que*

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	c_1		*Soma*
CPF	*1*	*4*	*5*	*3*	*8*	*2*	*2*	*0*	*6*	*2*	
Peso	*11*	*10*	*9*	*8*	*7*	*6*	*5*	*4*	*3*	*2*	
Produto	*11*	*40*	*45*	*24*	*56*	*12*	*10*	*0*	*18*	*4*	*220*

O resto da divisão de 220 *por* 11 *é* 0*, e assim,* $c_2 = 0$*. Portanto, o número do CPF é dado por* $145.382.206 - 20$

Oservamos que outra regra muito importante é que um CPF não pode ter todos os dígitos iguais, ou seja, da forma $111.111.111 - 11$, $222.222.222 - 22$, entre outros. Esses CPFs são válidos pelo algoritmo mas não existem no registro oficial, e assim, estes tipos de CPFs não podem ser usados. Também, em geral, dependendo da Região Fiscal onde é emitido o CPF (definida pelo nono dígito) tem as seguintes identificações:

1. DF, GO, MS, MT e TO: 1.
2. AC, AM, AP, PA, RO e RR: 2.
3. CE, MA e PI: 3.
4. AL, PB, PE, RN: 4.
5. BA e SE: 5.
6. MG: 6.

7. ES e RJ: 7.
8. SP: 8.
9. PR e SC: 9.
10. RS: 0.

6.2.1 Exercícios

1. Determine os dígitos verificadores c_1c_2 dos seguintes CPFs.
   (a) $212.785.254 - c_1c_2$.
   (b) $143.111.224 - c_1c_2$.
   (c) $412.331.322 - c_1c_2$.
   (d) $210.321.456 - c_1c_2$.
2. Determine o dígito x para que os seguintes números sejam números de CPFs.
   (a) $x11.286.214 - 01$.
   (b) $331.2x1.341 - 23$.
   (c) $121.33x.331 - 05$.
   (d) $432.235.12x - 30$

6.3 Cálculo do ISBN de livros

Os livros são identificados por um número de registro denominado ISBN (International Standard Book Number) que identifica os livros segundo o título, o autor, o país e a editora. O sistema é controlado pela Agência Internacional do ISBN, que orienta e delega poderes às agências nacionais. A agência brasileira é representada pela Fundação Biblioteca Nacional. O ISBN é composto por dígitos da forma

$$x_1x_2x_3\ldots x_{13}$$

e os dígitos são divididos em 5 blocos, conforme o seguinte exemplo

$$978 - 0 - 306 - 40615 - 7,$$

onde

1. O primeiro bloco é especificado pela Agência Internacional do ISBN, em conformidade com o sistema global de numeração de produtos.
2. O segundo bloco identifica os grupos nacionais geográficos.

3. O terceiro bloco refere-se ao editor.

4. O quarto bloco é um elemento de publicação, alocado para o editor da publicação.

5. O quinto bloco corresponde ao dígito verificador.

O último bloco é denominado de dígito de controle de paridade ou de verificação, com o objetivo de evitar erros vindos de transcrições indevidas de ISBN. Por exemplo, se o ISBN de um livro é

$$978 - 85 - 25 - 5600 - 9,$$

então 978 indique que é um livro, 85 indica que é do Brasil, 25 indical a Editora, 5600 indica a expecifibilidade do livro e 9 o dígito verificador. O último bloco é composto de 1 dígito alfanumérico de valores de 0 à 9 e a determinação é calculada da seguinte maneira:

1. Os 12 primeiros dígitos do ISBN são multiplicados alternadamente por 1 e 3, ou seja, calculamos a soma

$$L = x_1 + 3x_2 + x_3 + 3x_4 + x_5 + 3x_6 + x_7 + 3x_8 + x_9 + 3x_{10} + x_{11} + 3x_{12}.$$

2. A soma desses produtos é dividido por 10, obtendo um resto r entre 0 e 9.

3. Em seguida, faça $10 - r$, que é o dígito de verificação.

Exemplo 6.3.1. *Seja* $978 - 0 - 306 - 40615 - c$ *o ISBN de um livro. Fazendo uso do algoritmo, segue que*

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	*Soma*
ISBN	*9*	*7*	*8*	*0*	*3*	*0*	*6*	*4*	*0*	*6*	*1*	*5*	
Peso	*1*	*3*	*1*	*3*	*1*	*3*	*1*	*3*	*1*	*3*	*1*	*3*	
Produto	*9*	*21*	*8*	*0*	*3*	*0*	*6*	*12*	*0*	*18*	*1*	*15*	*93*

Dividindo 93 *por* 10*, segue que o resto é* 3*, e assim,* $10 - 3 = 7$ *que é o dígito de controle de paridade. Portanto, o número do CNPJ é dado por* $978 - 0 - 306 - 40615 - 7$*.*

6.3.1 Exercícios

1. Determine o digíto de controle de paridade dos seguintes ISBNs:

   (a) $978 - 65 - 00 - 30502 - c$.

   (b) $979 - 85 - 38 - 34772 - c$.

   (c) $978 - 65 - 00 - 26540 - c$.

   (d) $979 - 85 - 35 - 49684 - c$.

2. Determine x para que os seguintes números sejam o ISBN de um livro.

(a) $978 - 65 - x0 - 25788 - 5$.

(b) $97x - 85 - 36 - 36798 - 8$.

(c) $978 - 6x - 00 - 21279 - 2$.

(d) $979 - 85 - 36 - 9x098 - 2$.

6.4 Cálculo do CNPJ

O Cadastro Nacional de Pessoa Jurídica (CNPJ) segue uma regra muito parecida com as já vistas acima, mas é um número maior e pode ser dividido em blocos, ou seja,

$$x_1x_2.x_3x_4x_5.x_6x_7x_8/x_9x_{10}x_{11}x_{12} - c_1c_2,$$

onde c_1c_2 são os dígitos de controle. Por exemplo, o CNPJ

$$59.541.264/0001 - 03$$

está dividido em blocos. Neste caso,

1. o primeiro bloco 59.541.264 representa a inscrição do CNPJ.
2. o segundo bloco 0001 representa um código para a matriz ou a filial.
3. o terceiro bloco 03 são os dígitos verificadores.

Os dígitos verificadores são calculados usando como base os 12 primeiros dígitos.

O algoritmo é dado por

1. O primeiro passo é inerter a ordem do número do CNPJ, ou seja, considerar

   $$x_{12}x_{11}x_{10}x_9x_8x_7x_6x_5x_4x_3x_2x_1.$$

2. Para o cálculo de c_1, multiplicamos pela sequência crescente de 2 à 9, com repetição, e somamos esse resultado, ou seja,

   $$L_1 = 2x_{12} + 3x_{11} + 4x_{10} + 5x_9 + 6x_8 + 7x_7 + 8x_6 + 9x_5 + 2x_4 + 3x_3 + 4x_2 + 5x_1.$$

   Dividindo L_1 por 11 obtemos r_1 como resto. O dígito c_1 é dado por $c_1 = 11 - r_1$ se $2 \leq r_1 < 10$ e $c_1 = 0$ se $r_1 = 0$ ou 1.

3. O cálculo do dígito c_2 é feito de modo semelhante considerando o primeiro dígito verificador c_1. Para isso, utilizamos os 13 dígitos, na ordem invertida, e multiplicando-os pela sequência crescente de 2 à 9, com repetição, e somamos esse resultado, ou seja,

   $$L_2 = 2c_1 + 3x_{12} + 4x_{11} + 5x_{10} + 6x_9 + 7x_8 + 8x_7 + 9x_6 + 2x_5 + 3x_4 + 4x_3 + 5x_2 + 6x_1.$$

Novamente, dividimos L_2 por 11 e obtemos o resto r_2. O dígito $c_2 = 11 - r_2$ se $0 \leq r_2 < 10$ e $r_2 = 0$ se $r_1 = 0$ ou 1.

Exemplo 6.4.1. *Seja* $59.541.264/0001 - c_1c_2$ *o número de um CNPJ. Aplicando o algoritmo, para o cálculo de* c_1*, segue que*

													Soma
CNPJ	*1*	*0*	*0*	*0*	*4*	*6*	*2*	*1*	*4*	*5*	*9*	*5*	
Peso	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*2*	*3*	*4*	*5*	
Produto	*2*	*0*	*0*	*0*	*24*	*42*	*16*	*9*	*8*	*15*	*36*	*25*	*177*

Dividindo 177 *por* 11*, segue que o resto é* 1*. Como* $11 - 1 = 10$*, segue que o primeiro dígito verificador é* $c_1 = 0$*. Agora, o cálculo do segundo dígito verificador é utilizado a mesma regra do primeiro dígito, mas agora a partir do* 13^{o} *dígito, ou seja,*

	c_1	x_{12}	x_{11}	x_{10}	x_9	x_8	x_7	x_6	x_5	x_4	x_3	x_2	x_1	*Soma*
CNPJ	*0*	*1*	*0*	*0*	*0*	*4*	*6*	*2*	*1*	*4*	*5*	*9*	*5*	
Peso	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*2*	*3*	*4*	*5*	*6*	
Produto	*0*	*3*	*0*	*0*	*0*	*28*	*48*	*18*	*2*	*12*	*20*	*45*	*30*	*206*

Dividindo 206 *por* 11*, segue que o resto é* 8*, e assim,* $c - 2 = 11 - 8 = 3$*. Portanto, o número do CNPJ é dado por* $59.541.264/0001 - 03$

Observamos que a mesma regra de CPF com dígitos iguais se aplica aqui também, ou seja, CNPJs como 11.111.111/1111-11 não são válidos.

6.4.1 Exercícios

1. Determine os dígitos verificadores c_1c_2 dos seguintes CNPJs.

   (a) $11.786.234/0001 - c_1c_2$.

   (b) $33.221.311/0001 - c_1c_2$.

   (c) $22.311.132/0001 - c_1c_2$.

   (d) $21.342.701/0001 - c_1c_2$.

2. Determine o valor de x de modo que os seguintes números representem um CNPJ.

   (a) $1x.286.134/0001 - 12$.

   (b) $13.x21.311/0001 - 23$.

   (c) $21.351.1x2/0001 - 30$.

   (d) $31.3x2.711/0001 - 44$.

6.5 Agência e conta corrente

Os números das agências e das contas correntes também possuem um dígito de controle. Mas, cada banco possui o seu método de cálculo, uma vez que o número das agências e das contas corretnes possuem quantidades de números diferentes de banco para banco.

6.5.1 Banco do Brasil

Para o Banco do Brasil as agências possuem 5 dígitos, sendo o último d'ıgito de controle, ou seja,

$$x_1x_2x_3x_4 - c.$$

Para o cálculo desse dígito de controle, usamos o seguinte algoritmo.

1. Multiplicamos os 4 primeiros dítos pelos números $5, 4, 3$ e 2 e somamos, ou seja,

$$L = 5x_1 + 4x_2 + 3x_3 + 2x_4.$$

2. Dividindo L por 11 obtemos r como resto. O dígito c é dado $c = 11 - r$ se $2 \leq r < 11$, $c = 0$ se $r = 0$ e $c = x$ se $r = 1$.

Exemplo 6.5.1. *Seja* $1584 - c$ *o número de uma agência do Banco do Brasil. Aplicando o algoritmo, segue que*

	x_1	x_2	x_3	x_4	*Soma*
Agência	*1*	*5*	*8*	*4*	
Peso	*5*	*4*	*3*	*2*	
Produto	*5*	*20*	*24*	*8*	*57*

Dividindo 57 *por* 11*, segue que o resto é* 2*. Assim,* $c = 11 - 2 = 9$*. Portanto, o número correto da agência é dado por* $1584 - 9$*.*

O número de uma conta corrente do Banco do Brasil possui 9 dígitos, onde o último dígito é de controle de paridade, ou seja,

$$x_1x_2x_3x_4x_5x_6x_7x_8 - c.$$

Para o cálculo desse dígito de controle, usamos o seguinte algoritmo.

1. Multiplicamos os 8 primeiros dítos pelos números $9, 8, 7, 6, 5, 4, 3$ e 2 e somamos, ou seja,

$$L = 9x_1 + 8x_2 + 7x_3 + 6x_4 + 5x_5 + 4x_6 + 3x_7 + 2x_8.$$

2. Dividindo L por 11 obtemos r como resto. O dígito c é dado $c = 11 - r$ se $2 \leq r < 11$, $c = 0$ se $r = 0$ e $c = x$ se $r = 1$.

Exemplo 6.5.2. *Seja* $00210169 - c$ *o número de uma conta corrente do Banco do Brasil. Aplicando o algoritmo, segue que*

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	*Soma*
Conta	*0*	*0*	*2*	*1*	*0*	*1*	*6*	*9*	
Peso	*9*	*8*	*7*	*6*	*5*	*4*	*3*	*2*	
Produto	*0*	*0*	*14*	*6*	*0*	*4*	*18*	*18*	*60*

Dividindo 60 *por* 11*, segue que o resto é* 5*. Assim,* $c = 11 - 5 = 6$*. Portanto, o número correto da agência é dado por* $00210169 - 6$*.*

6.5.2 Banco Santander

O Banco Santander possui uma maneira diferente do cálculo do dígito de controle, ou seja, existe apeanas um dígito de controle que depende de todos os dígitos que compõem a agência e os demais dígitos. A agência possui 4 dígitos e a conta corrente possui 9 dígitos, onde os 2 primeiros dígitos corresponde ao tipo de conta, os 6 dígitos seguintes da conta e o último dígito é o dígito de controle que depende dos 12 dígitos anteriores, ou seja,

$$a_1a_2a_3a_4\ t_5t_6\ x_7x_8x_9x_{10}x_{11}x_{12} - c.$$

Para o cálculo desse dígito de controle, usamos o seguinte algoritmo.

1. Multiplicamos os dítos da agência, os dígitos do tipo da conta e da conta corrente pelos números $9, 7, 3, 1, 9, 7, 1, 3, 1, 9, 7$ e 3 e somamos, ou seja,

$$L = 9a_1 + 7a_2 + 3_3 + 1a_4 + 9t_5 + 7t_6 + 1x_7 + 3x_8 + 1x_9 + 9_{10} + 7x_{11} + 3x_{12}$$

2. Dividindo L por 10 obtemos r como resto. O dígito c é dado $c = 10 - r$ se $1 \leq r < 10$ e $c = 0$ se $r = 0$.

Exemplo 6.5.3. *Seja* 0189 *o número da agência e* $0101741 - c$ *o número de uma conta corrente no Banco Santander. Aplicando o algoritmo, segue que*

	a_1	a_2	a_3	a_4	t_5	t_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	*Soma*
Dítos	*0*	*1*	*8*	*9*	*0*	*1*	*0*	*1*	*7*	*4*	*1*	*7*	
Peso	*9*	*7*	*3*	*1*	*9*	*7*	*1*	*3*	*1*	*9*	*7*	*3*	
Produto	*0*	*7*	*4*	*9*	*0*	*7*	*0*	*3*	*7*	*6*	*7*	*1*	*51*

Dividindo 51 *por* 10*, segue que o resto é* 1*. Assim,* $c = 10 - 1 = 9$*.*

6.5.3 Exercícios

1. Determine os dígitos verificadores c das seguintes agências e contas correntes do Banco do Brasil.

(a) $1186 - c$ e $123 - c$.

(b) $3322 - c$ e $21.311 - c$.

(c) $22311 - c$ e $132.001 - c$.

(d) $2134 - c$ e $27.011 - c$.

2. Determine o valor de x de modo que os seguintes números representem agência e conta corrente do Banco do Brasil.

(a) $1x28 - 2$ e $13.4x1 - 2$.

(b) $13x2 - 1$ e $31.1x1 - 3$.

(c) $21x1 - 2$ e $1x2.011 - 3$.

(d) $313x - 2$ e $71.x01 - 4$.

3. Determine os dígitos verificadores c de modo que os seguintes números representem agência e conta corrente do Banco Santander.

(a) 0156 e $01012113 - c$.

(b) 0322 e $01012131 - c$.

(c) 0231 e $01011321 - c$.

(d) 0134 e $01012702 - c$.

4. Determine o valor de x de modo que os seguintes números representem agência e conta corrente do Banco Santander.

(a) $1x28$ e $01013421 - 2$.

(b) 0132 e $01011x12 - 3$.

(c) $21x2$ e $01012201 - 2$.

(d) 3132 e $0101701x - 4$.

Capítulo

7

Introdução a criptografia

A criptografia, palavra que vem do grego cryptos cujo significado é secreto ou oculto, e é a arte de codificar mensagens de modo que somente o destinatário seja capaz de interpretá-la, ou seja, decifrá-la. Assim, a criptografia estuda os métodos para codificar e transmitir uma mensagem de modo que somente seu destinatário legítmo consiga interpretá-la, ou seja, é a arte dos códigos secretos, o qual já estamos acostumados. Criptografia é uma área da matemática que estuda métodos de codificação e decodificação de uma mensagem com o objetivo de que apenas o remetente e o destinatário saibam compreender seu significado. Apesar de se ter conhecimento sobre a sua grande importância na período das Guerras Mundiais a criptografia foi usada há muitos anos, onde existem relatos do seu uso pelo imperador romano Julio César para combates na Europa. No entanto, o uso da criptografia tornou mais evidente após o advento dos computadores, e principalmente, da internet, sendo hoje muito utilizada em transações comerciais.

A criptografia começou com métodos simples a fim de ocultar um texto. O mais simples destes algoritmos consiste em substituir uma letra por uma outra letra seguinte, isto é, transladar o alfabeto uma casa para diante. Esse método de criptografia é muito antigo e simples, que foi utilizado por Júlio César em suas cartas, que consistia em substituir uma letra por outra a fim de transmitir uma mensagem sigilosa.

Por volta de 1970 surgiu muitos estudos de métodos de criptografia de chave pública, onde foi descoberto outro algoritmo muito utilizado atualmente, chamado algoritmo RSA, que é um método criptográfico de chave pública onde todos tem a chave de codificação (chave pública), mas isto não implica o conhecimento da chave de decodificação, e assim, saber decodificar.

A descrição do RSA consiste em explicitar o algoritmo de codificação e decodificação de

mensagens. Este método faz uso de números primos e da congruência modular. Desse modo, o estudo de métodos para determinar se um número é primo ocupou matemáticos como Fermat e Euler. O estudo nesta área levou os estudiosos a busca de algoritmos determinísticos de primalidade. Atualmente, esta técnica possui grande importância nas comunicações com o objetivo de transmitir informações com segurança, por exemplo, em transações bancárias e comerciais.

O primeiro passo em um algoritmo de criptografia é decodificar uma mensagem a ser transmitida. Em seguida devemos decodificar a mensagem, ou seja, passar da mensagem codificada para a mensagem original.

O objetivo, deste capítulo, é apresentar dois métodos de criptografia (Júlio César e RSA) fazendo uso da teoria elementar dos números, ou seja, o uso dos números primos e da congruência modular. Assim, nestes algoritmos, apresentamos métodos de como descrever as receitas de codificação e decodificação, onde precisamos também verificar que se aplicadas nesta ordem voltamos a obter à mensagem original.

7.1 Criptografia de Júlio César

As congruências possuem muitas aplicações na matemática discreta, na computação e nas engenharias. Uma das aplicações da congruência é a criptografia, que é o estudo de como transmitir mensagens secretas. Um dos mais antigos e pioneiros métodos de criptografia é de Júlio César, onde nas mensagens secretas cada letra é substituída pela letra que está três posições adiante no alfabeto usado. Por exemplo, a letra A é enviada como D, a letra B é enviada como a letra E, e assim por diante. Isto é feito ciclicamente de modo que as três últimas letras do alfabeto passam a ser, respectivamente, as três primeiras letras do alfabeto, no processo de decodificação. Isto é um exemplo de codificação, ou seja, o processo de construir uma mensagem secreta.

7.1.1 Pré-codificação

Para expressar matematicamente o processo de codificação de Júlio César, primeiro fazemos a pré-codificação substituindo cada letra por um número inteiro de 0 a 25, com base em sua posição no alfabeto. Por exemplo, substitua A por 0, B por 1, C por 2, e assim por diante, ou seja,

A	B	C	D	E	F	G	H	I	J	K	L	M
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
13	14	15	16	17	18	19	20	21	22	23	24	25.

7.1.2 Codificação

O método de codificação do algoritmo de Júlio César pode ser representado por uma função bijetora $f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$, onde $\mathbb{Z}_{26} = \{0, 1, 2, 3, \ldots, 25\}$, ou seja, se $n \in \mathbb{Z}_{26}$, então

$$f(n) \equiv (n + 3)(mod\ 26).$$

Neste caso, na versão codificada da mensagem, a letra representada por n é substituída pela letra representada por $(n+3)(mod\ 26)$. Observamos que o método de Júlio César não apresenta um alto nível de segurança.

Exemplo 7.1.1. *Seja a mensagem MEET YOU IN THE PARK. A pré-codificação é através da substituição das letras por números, e assim, obtemos a seguinte sequência*

$$12\ 4\ 4\ 19 \quad 24\ 14\ 20 \quad 8\ 13 \quad 19\ 7\ 4 \quad 15\ 0\ 17\ 10.$$

Agora, para a codificação, substituimos cada número n por $f(n) \equiv (n + 3)(mod\ 26)$*, e assim, obtemos a seguinte sequência*

$$15\ 7\ 7\ 22 \quad 1\ 17\ 23 \quad 11\ 16 \quad 22\ 10\ 7 \quad 18\ 3\ 20\ 13.$$

Agora, transcrevendo para letras, obtemos a mensagem codificada que é dada por PHHW BRW LQ KKH SDUN.

Existem várias maneiras de generalizar o algoritmo Júlio de César. Por exemplo, em vez de substituir cada letra por uma que esteja três posições a frente, podemos substituir cada letra por uma que esteja k posições a frente fazendo uso de uma função bijetora dada da seguinte forma

$$f(n) \equiv (n + k)(mod\ 26).$$

Esse algoritmo é também chamado de algoritmo de substituição.

Outra maneira de generalizar o algoritmo de Júlio César é fazendo uso de uma função afim $f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ que seja bijetora, definida por $f(n) \equiv (an + b)(mod\ 26)$, onde $\overline{an + b}$ é o resto da divisão de $an + b$ por 26, com $a, b \in \mathbb{Z}$. Neste caso, podemos codificar sentenças fazendo uso da função f. A função f deve deve ser bijetora para que:

1. cada letra seja enviada em uma única letra,
2. letras distintas sejam enviadas em letras distintas e,
3. toda letra seja imagem de uma outra letra.

Teorema 7.1.1. *Sejam* $a, b \in \mathbb{Z}$*, com* $a \neq 0$*. A função* $f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ *definida por* $f(n) \equiv (an + b)(mod\ 26)$ *é bijetora se, e somente se,* $mdc(a, 26) = 1$*.*

Demonstração. Suponhamos que f é bijetora. Seja $b \in \mathbb{Z}$. Pelo algoritmo da divisão, segue que existem $q, r \in \mathbb{Z}$ únicos tal que $b = 26q + r$, onde $0 \leq r < 26$. Assim, $(r + 1)(mod\ 26) \in \mathbb{Z}_{26}$.

Como f é sobrejetora, segue que existe $n_{\in}\mathbb{Z}_{26}$ tal que $f(n_0) \equiv (r+1)(mod\ 26)$, ou seja, $an_0 + b \equiv (r+1)(mod\ 26)$. Como $b = 26q + r$, segue que

$$(an_0 + b) \equiv (an_0 + 26q + r) \equiv (r+1)(mod\ 26),$$

e desse modo, $an_0 \equiv 1(mod\ 26)$. Logo, existe $y_0 \in \mathbb{Z}$ tal que $26y_0 + an_0 = 1$. Portanto, $mdc(a, 26) = 1$. Reciprocamente, como o resto da divisão de $an + b$ por 26 é único, segue que a função f está bem definida. Agora, se $f(m) = f(n)$, com $m, n \in \mathbb{Z}_{26}$, então $(am + b) \equiv (an + b)(mod\ 26)$, ou seja,

$$a(m-n) \equiv 0(mod\ 26). \tag{7.1}$$

Como $mdc(a, 26) = 1$, pela identidade de Bezout, segue que existem $x_0, y_0 \in \mathbb{Z}$ tal que $ax_0 + 26y_0 = 1$, ou seja,

$$ax_0 \equiv 1(mod 26). \tag{7.2}$$

Multiplicando ambos os membros da Equação (7.1) por x_0, segue que $ax_0(m-n) \equiv 0(mod\ 26)$. Pela Equação (7.2), segue que $m - n \equiv 0(mod\ 26)$. Como $m, n \in A$, segue que $|m-n| < 26$. Assim, $m = n$, e portanto, f é injetora. Como $\mathbb{Z}_{26}$ é um conjunto finito, segue que f é sobrejetora, e portanto, f é bijetora. □

Exemplo 7.1.2. *Como $mdc(3, 26) = 1$, segue que a função $f(n) \equiv (3n+5)(mod\ 26)$ é bijetora, e assim, a função f pode ser usada no processo de codificação da frase BOM DIA MEUS AMIGOS. Primeiramente, faremos a pré-codificação fazendo uso das substituições das letras pelas suas posições no alfabeto $\mathbb{Z}_{26} = \{0, 1, 2, 3, \ldots, 25\}$, ou seja,*

B	O	M		D	I	A		M	E	U	S		A	M	I	G	O	S
$\updownarrow$	$\updownarrow$	$\updownarrow$		$\updownarrow$	$\updownarrow$	$\updownarrow$		$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$		$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
1	14	12		3	8	0		12	4	20	18		0	12	8	6	14	18.

Através da f essa sequência é levada em $f(n) = 3n + 5(mod\ 26)$, ou seja,

$f(1)$	$f(14)$	$f(12)$			$f(3)$	$f(8)$	$f(0)$		$f(12)$	$f(4)$	$f(20)$	$f(18)$				
$\updownarrow$	$\updownarrow$	$\updownarrow$			$\updownarrow$	$\updownarrow$	$\updownarrow$		$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$				
8	21	15			14	3	5		15	17	13	7				

$f(0)$	$f(12)$	$f(8)$	$f(6)$	$f(14)$	$f(18)$
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
5	15	3	23	21	7.

Assim, a sequência de números é codificada através da função f na seguinte sequência de números

$$8\ 21\ 15\ \ 14\ 3\ 5\ \ 15\ 17\ 13\ 5\ \ 5\ 15\ 3\ 23\ 21\ 5,$$

que corresponde à seguinte sequência de letras

$$IVP\ ODF\ PRNF\ FPDXVF,$$

através da substituições dos números pelas letras.

7.1.3 Decodificação

Para recuperar a mensagem original a partir de uma mensagem secreta codificada pelo código de Júlio César é através da função inversa da função f, ou seja, através de f^{-1}. Neste caso, se f é definida por $f(n) = (n+3)(mod\ 26)$, então a sua função inversa é dada por

$$f^{-1}(n) \equiv (n-3)(mod\ 26),$$

ou seja, $f^{-1}(n) = (n+23)(mod\ 26)$, onde $n = 0, 1, 2, \ldots, 25$. Assim, para encontrar a mensagem original, cada letra é substituída pela terceira letra anterior, onde as primeiras três letras é referida como às três últimas do alfabeto. O processo de determinar a mensagem original a partir da mensagem codificada é chamado de decodificação.

Se a função f é definida por $f(n) \equiv (n+k)(mod\ 26)$, então a sua inversa é dada por

$$f^{-1}(n) \equiv (n-k)(mod\ 26).$$

Agora, se a função é definida por

$$f(n) \equiv (an+b)(mod\ 26),$$

onde $a, b \in \mathbb{Z}$ são escolhidos de tal forma que f seja bijetora, então a função inversa $f^{-1} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ é dada por $f^{-1}(n) = (cn+d)(mod\ 26)$, onde $c, d \in \mathbb{Z}$ e $mdc(c, 26) = 1$. Neste caso, $(f \circ g)(n) = n(mod\ 26)$, ou seja,

$$f(g(\overline{n})) = f(\overline{cn+d}) = \overline{a(cn+d)+b} = \overline{acn+ad+b} = \overline{n}$$

e $(g \circ f)(n) = n(mod\ 26)$, ou seja,

$$g(f(\overline{n})) = g(\overline{an+b}) = \overline{c(an+b)+d} = \overline{acn+bc+d} = \overline{n},$$

para todo $n \in \mathbb{Z}_{26}$. Em particular, $f(g(0)) = 0$, e assim, $ad+b \equiv 0(mod\ 26)$ e $bc+d \equiv 0(mod\ 26)$. Desse modo, $\overline{acn} \equiv \overline{n}$, e assim, $ac \equiv 1(mod\ 26)$.

Exemplo 7.1.3. *Se a função f é definida por $f(n) \equiv (3n+3)(mod\ 26)$, então a sua inversa f^{-1} é dada por $f^{-1}(n) \equiv (9n+25)(mod\ 26)$.*

Exemplo 7.1.4. *A inversa da função $f(n) = (3n+5)(mod\ 26)$ do Exemplo 7.1.2, é dada por*

$f^{-1}(n) = (9n + 7)(mod\ 26)$. *Assim,*

$$\begin{array}{cccccccccc} f^{-1}(8) & f^{-1}(21) & f^{-1}(15) & f^{-1}(14) & f^{-1}(3) & f^{-1}(0) & f^{-1}(15) & f^{-1}(17) & f^{-1}(13) & f^{-1}(7) \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 1 & 14 & 12 & 3 & 8 & 0 & 12 & 4 & 20 & 18 \end{array}$$

$$\begin{array}{cccccc} f^{-1}(5) & f^{-1}(15) & f^{-1}(3) & f^{-1}(23) & f^{-1}(21) & f^{-1}(7) \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 0 & 12 & 8 & 6 & 14 & 18, \end{array}$$

que corresponde a frase BOM DIA MEUS AMIGOS.

7.1.4 Exerçícios

1. Pré-codifique e codifique usando o código de Júlio César às seguintes mensagens.
   (a) Good monrning my friends.
   (b) Adoro os métodos de criptografia.
   (c) Feliz ano novo para todos.
2. Decodifique as mensagens abaixo usando o código de Júlio César.
   (a) EOXH MHDQV
   (b) WHVW WRGDB
   (c) HDW GLP VXP
3. Pré-codifique e codifique a mensagem DO NOT PASS GO fazendo uso do algoritmo de Júlio César através das seguintes funções.
   (a) $f(n) \equiv (n + 3)(mod\ 26)$.
   (b) $f(n) \equiv (n + 13)(mod\ 26)$.
   (c) $f(n) \equiv (3n + 7)(mod\ 26)$.
4. Fazendo uso do código de Júlio César.
   (a) Construa uma tabela de pré-codificação diferente de Júlio César.
   (b) Pré-codifique, codifique e decodifique a frase: minha vida é uma maravilha.
   (c) Pré-codifique, codifique e decodifique a frase: rua das flores coloridas.
   (d) Pré-codifique, codifique e decodifique a frase: minhas aventuras são gratificantes.
5. Fazendo uso do algoritmo de Júlio César.
   (a) Construa uma tabela de pré-codificação diferente de Júlio César.
   (b) Pré-codifique, codifique e decodifique a frase: eu gosto de matemática.

(c) Pré-codifiquem codifique e decodifique a frase: hoje está fazendo sol.

(d) Pré-codifique, codifique e decodifique a frase: minha família está viajando.

6. Fazendo o uso do algoritmo de Júlio César.

(a) Construa uma tavela de pré-decofificação.

(b) Pré-codifique, codifique e decodifique a frase: adoro minhas filhas.

(c) Pré-codifique, codifique e decodifique a frase: minha vida é uma maravilha.

(d) Pré-codifique, codifique e decodifique a frase: meu caminho difere do seu.

7.2 Criptografia RSA

O método de codificação de César e sua construção funcionam pela substituição de cada letra do alfabeto por outra. Métodos de codificação desse tipo são vulneráveis a ataques baseados na frequência de ocorrência das letras na mensagem. Métodos de codificação mais sofisticados são baseados na substituição de blocos de letras, onde existem várias técnicas baseadas na aritmétia modular para codificar blocos de letras.

Nesta seção, apresentamos o conceito de criptografia RSA juntamente com suas principais propriedades, onde apresentamos método dado por R. L. Rivest, A. Shamir e L. Adleman em 1978, do Massachussets Institute of Technology (MIT), chamado Criptografia com chave pública, conhecido como Criptografia RSA.

Em um método criptográfico com chave pública, cada usuário publica em uma lista pública um procedimento C para que os outros usuários possam codificar as mensagens que lhe são dirigidas. Cada usuário guarda o procedimento D para decodificar as mensagens que lhe são enviadas. Dada uma mensagem M, os procedimentos C e D devem ter as seguintes propriedades:

1. $D(C(M)) = M$, ou seja, se codificamos e depois decoficamos, obtemos a mensagem original de volta;

2. $C(D(M)) = M$, ou seja, se decodificamos e depois codificamos, obtemos a mensagem original;

3. é praticamente impossível descobrir D a partir de C.

O algoritmo RSA é um método criptográfico de chave pública que todos tem a chave de codificação (chave pública), porém isto não implica em ter a chave de decodificação, e assim, saber decodificar. Neste método é usado dois parâmetros que são dois números primos distintos os quais são responsáveis pela segurança do método. Quando usamos um método de criptografia temos três etapas básicas a saber: *a pré-codificação, a codificação e a decodificação.* A seguir, apresentamos, cada uma dessas etapas, descrevendo, assim, o algoritmo RSA de criptografia.

7.2.1 Pré-codificação

Na pré-codificação é feita a conversão das letras em números. Por exemplo, podemos utilizar a seguinte tabela:

$$\begin{array}{cccccccccccc} A & B & C & D & E & F & G & H & I & J & K & L & M \\ 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 \\ \\ N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 & 31 & 32 & 33 & 34 & 35 \end{array} \tag{7.3}$$

Para isso, usamos o número 99 no lugar do espaço entre as palavras. Dessa forma, fazemos a conversão da mensagem obtendo, assim, o bloco de números correspondente a mensagem que chamamos de M.

Exemplo 7.2.1. *Utilizando a Tabela 7.3, a frase NOÇÕES SOBRE CRIPTOGRAFIA fica convertida como*

N	O	C	O	E	S		S	O	B	R	E		C	R	I	P	T	O	G	R	A	F	I	A
23	24	12	24	14	28	99	28	24	11	27	14	99	12	27	18	25	29	24	16	27	10	15	18	10,

e agrupando,

$$232412241428992824112714991227182529241627101518 10.$$

Observação 7.2.1. *Observamos que podemos utilizar outras tabelas de conversão, porém ressaltamos a vantagem de fazer a conversão das letras por números com dois algarismos, por exemplo, se fizermos $A \mapsto 1$, $B \mapsto 2$, e assim por diante, segue que 12 pode corresponder a AB ou a 12^a letra do alfabeto, que é L, nos trazendo problemas na hora da decodificação.*

Como vimos, o método utiliza parâmetros que denotamos por p e q. Seja o número $n = pq$. Feita a conversão, devemos agora quebrar o bloco M em blocos menores que o número n.

Exemplo 7.2.2. *No Exemplo 7.2.1 obtemos o seguinte bloco*

$$M = 232412241428992824112714991227182529241627101518 10,$$

que corresponde a frase NOÇÕES SOBRE CRIPTOGRAFIA. Tomando, por exemplo, como parâmetros $p = 11$ e $q = 13$, e desta forma, $n = 143$, então devemos quebrar M em blocos com números menores que 143. Assim, obtemos os blocos

$$23-24-122-41-42-89-92-82-41-127-14-99-122-71-82-52-92-41-62-7-101-51-8-10.$$

Observação 7.2.2. *Observamos que o modo de quebrar o bloco M em blocos menores não é única, porém devemos evitar que um bloco comece por 0, pois isso pode nos trazer problemas na hora da decodificação. Por exemplo, não temos como distinguir o bloco 071 do bloco 71.*

7.2.2 Codificação

Para codificar a mensagem que convertemos, precisamos de n e de um inteiro e que seja inversível módulo $\varphi(n)$, ou seja, $mdc(e, \varphi(n)) = 1$. Pelo Teorema 5.3.2, segue que

$$\varphi(n) = (p-1)(q-1).$$

Logo, usamos (n, e) chamado chave de codificação para codificar bloco a bloco que obtemos anteriormente. Seja b um bloco obtido ao final da pré-codificação e chamamos de $C(b)$ a codificação do bloco b. Assim, temos que $C(b) \in \{0, 1, 2, ..., n-1\}$ e $C(b) \equiv b^e \ (mod\ n)$, ou seja, $C(b)$ é o resto da divisão de b^e por n. Ao final da codificação de cada bloco temos a mensagem codificada.

Exemplo 7.2.3. *A frase noções sobre criptografia fica convertida como*

N	O	C	O	E	S		S	O	B	R	E		C	R	I	P	T	O	G	R	A	F	I	A
23	24	12	24	14	28	99	28	24	11	27	14	99	12	27	18	25	29	24	16	27	10	15	18	10

e agrupando,

$$232412241428992824112714991227182529241627101518 10.$$

Tomando como parâmetros $p = 11$ e $q = 13$, segue que $n = 143$. Desse modo, devemos quebrar M em blocos com números menores que 143. Assim, $23-24-122-41-42-89-92-82-41-127-14-99-122-71-82-52-92-41-62-7-101-51-8-10$.

Exemplo 7.2.4. *Pelo Exemplo 7.2.3, obtemos os seguintes blocos*

$$23-24-122-41-42-89-92-82-41-127-14-99-122-71-82-52-92-41-62-7-101-51-8-10.$$

Como $n = 143$, segue que $\varphi(143) = 120$. Assim, precisamos escolher e de modo que $mdc(e, 120) = 1$. Por exemplo, tomamos $e = 7$ e codificamos bloco a bloco da seguinte forma:

$$\begin{array}{c|c} 23^7 \equiv 23 \ (mod\ 143) & 122^7 \equiv 34 \ (mod\ 143) \\ 24^7 \equiv 106 \ (mod\ 143) & 71^7 \equiv 124 \ (mod\ 143) \\ 122^7 \equiv 34 \ (mod\ 143) & 82^7 \equiv 69 \ (mod\ 143) \\ 41^7 \equiv 24 \ (mod\ 143) & 52^7 \equiv 13 \ (mod\ 143) \\ 42^7 \equiv 81 \ (mod\ 143) & 92^7 \equiv 27 \ (mod\ 143) \\ 89^7 \equiv 67 \ (mod\ 143) & 41^7 \equiv 24 \ (mod\ 143) \\ 92^7 \equiv 27 \ (mod\ 143) & 62^7 \equiv 127 \ (mod\ 143) \\ 82^7 \equiv 69 \ (mod\ 143) & 7^7 \equiv 6 \ (mod\ 143) \\ 41^7 \equiv 24 \ (mod\ 143) & 101^7 \equiv 62 \ (mod\ 143) \\ 127^7 \equiv 140 \ (mod\ 143) & 51^7 \equiv 116 \ (mod\ 143) \\ 14^7 \equiv 53 \ (mod\ 143) & 8^7 \equiv 57 \ (mod\ 143) \\ 99^7 \equiv 44 \ (mod\ 143) & 10^7 \equiv 10 \ (mod\ 143). \end{array}$$

Assim,

$$23-106-34-24-81-67-27-69-24-140-53-44-34-124-69-13-27-24-127-6-62-116-57-10,$$

que é a mensagem Noções sobre criptografia codificada utilizando a chave de codificação $(143, 7)$.

Observação 7.2.3. *Observamos que ao final da codificação os blocos já codificados não podem ser agrupados formando um grande número pois se assim ocorrer será impossível decodificar a mensagem.*

7.2.3 Decodificação

Apresentamos, agora, como decodificar uma mensagem codificada. Para isso precisamos de n e de um inteiro d que é o inverso de e módulo $\varphi(n)$. Assim, o par (n, d) é chamado de chave de decodificação. Seja D o processo de decodificação. Assim, sendo a um bloco de mensagem codificado, temos que $D(a) \in \{0, 1, 2, ..., n-1\}$ e $D(a) \equiv a^d \ (mod\ n)$, ou seja, $D(a)$ é o resto da divisão de a^d por n.

Observação 7.2.4. *Observe que sendo b um bloco obtido na pré-codificação e $C(b)$ o bloco b codificado, devemos ter $D(C(b)) = b$. Mostramos que $D(C(b)) \equiv b \ (mod\ n)$ para que tenhamos certeza de que o algoritmo realmente funciona. Considerando os primos p e q, e a chave de codificação (n, e), logo, sendo b um bloco com $1 \leq b \leq n-1$, temos $D(C(b)) \equiv (b^e)^d \equiv b^{ed} \ (mod\ n)$ e como $p \mid n$, temos $D(C(b)) \equiv b^{ed} \ (mod\ p)$. Ainda, como d é o inverso de e módulo $\varphi(n)$, segue que existe $k \in \mathbb{Z}$ de modo que $ed = 1 + k\varphi(n) = 1 + k(p-1)(q-1)$. Assim, tomando o primo p temos*

$$b^{ed} \equiv b^{1+k\varphi(n)} \equiv b^{1+k(p-1)(q-1)} \equiv b(b^{p-1})^{k(q-1)} \ (mod\ p).$$

Agora, se $p \mid b$, então $b \equiv 0 \ (mod\ p)$, e deste modo, $b^{ed} \equiv 0 \equiv b \ (mod\ p)$. Caso $p \nmid b$, como $b^{ed} \equiv b(b^{p-1})^{k(q-1)} \ (mod\ p)$, segue, pelo Pequeno Teorema de Fermat, que $b^{ed} \equiv b(b^{p-1})^{k(q-1)} \equiv b.1^{k(q-1)} \equiv b \ (mod\ p)$. Logo, para todo $1 \leq b \leq n-1$, temos que $b^{ed} \equiv b \ (mod\ p)$ e usando raciocínio análogo para o primo q, concluímos que $b^{ed} \equiv b \ (mod\ q)$. Dessa forma, sendo $mdc(p, q) = 1$ segue que $b^{ed} \equiv b \ (mod\ n)$, para todo $1 \leq b \leq n-1$. Portanto, o método é realmente eficaz.

Exemplo 7.2.5. *Tomando ainda o Exemplo 7.2.3 o qual tínhamos $p = 11$, $q = 13$ e $e = 7$, como $\varphi(143) = 120$, segue que resolver a seguinte equação diofantina $7d + 120k = 1$ para encontrar o inteiro d. Como o par $(-17, 1)$ é solução da equação, segue que $d \equiv -17 \ (mod\ 120)$, e portanto, $d = 103$. Dessa forma, usando os blocos obtidos anteriormente na codificação*

$$23-106-34-24-81-67-27-69-24-140-53-44-34-124-69-13-27-24-127-6-62-116-57-10,$$

temos que a decodificação é feita da seguinte forma:

$$\begin{array}{r|l} 23^{103} \equiv 23 \ (mod\ 143) & 34^{103} \equiv 122 \ (mod\ 143) \\ 106^{103} \equiv 24 \ (mod\ 143) & 124^{103} \equiv 71 \ (mod\ 143) \\ 34^{103} \equiv 122 \ (mod\ 143) & 69^{103} \equiv 82 \ (mod\ 143) \\ 24^{103} \equiv 41 \ (mod\ 143) & 13^{103} \equiv 52 \ (mod\ 143) \\ 81^{103} \equiv 42 \ (mod\ 143) & 27^{103} \equiv 92 \ (mod\ 143) \\ 67^{103} \equiv 89 \ (mod\ 143) & 24^{103} \equiv 41 \ (mod\ 143) \\ 27^{103} \equiv 92 \ (mod\ 143) & 127^{103} \equiv 62 \ (mod\ 143) \\ 69^{103} \equiv 82 \ (mod\ 143) & 6^{103} \equiv 7 \ (mod\ 143) \\ 24^{103} \equiv 41 \ (mod\ 143) & 62^{103} \equiv 101 \ (mod\ 143) \\ 140^{103} \equiv 127 \ (mod\ 143) & 116^{103} \equiv 51 \ (mod\ 143) \\ 53^{103} \equiv 14 \ (mod\ 143) & 57^{103} \equiv 8 \ (mod\ 143) \\ 44^{103} \equiv 99 \ (mod\ 143) & 10^{103} \equiv 10 \ (mod\ 143). \end{array}$$

Assim, obtemos na decodificação os blocos

$$23-24-122-41-42-89-92-82-41-127-14-99-122-71-82-52-92-41-62-7-101-51-8-10,$$

e agrupando

$$232412241428992824112714991227182529241627101518 10,$$

donde usando a tabela de conversão temos a frase Noções sobre criptografia.

Observação 7.2.5. *Como vimos anteriormente, a chave de codificação (n, e) do RSA é pública, assim, o algoritmo só será seguro se for difícil encontrar a chave (n, d) de decodificação, em particular, calcular o inteiro d. Observamos que a única maneira de calcularmos d é, como vimos, encontrando $\varphi(n)$. No entanto, para isto precisamos dos fatores de n, isto é, p e q, pois $\varphi(n) = (p-1)(q-1)$. Suponhamos que fosse possível decodificar uma mensagem do RSA sem fatorarmos n, assim só teríamos três possibilidades:*

1. *encontrarmos $\varphi(n)$ a partir de n e e;*
2. *encontrar d sem conhecer $\varphi(n)$;*
3. *encontrar o bloco b a partir de b^e módulo n sem conhecer d.*

As duas primeiras são equivalentes a fatorarmos n e a última é praticamente impossível. Desse modo, temos que a segurança do método RSA está na dificuldade de fatorarmos n, logo, quanto maior n, maior a segurança do método. Assim, a escolha dos parâmetros p e q é um ponto crucial quando o RSA é usado, porém não basta que os primos escolhidos sejam grandes, alguns outros cuidados devem ser seguidos, pois existem técnicas de fatoração muito eficazes que podem comprometer a segurança do método.

Já vimos como o método RSA funciona, vimos também como utilizá-lo, porém suponhamos a seguinte situação: imagine que uma empresa realiza transações bancárias através de um

computador e que tanto a empresa quanto o banco utilizam do método RSA para garantirem a segurança de suas informações. A empresa precisa fazer uma transferência de saldos e envia essa instrução ao banco, como o banco terá a certeza de que os dados são realmente enviados pela empresa, já que a chave de codificação do RSA é pública? Para isso o banco precisa que a mensagem enviada pela empresa seja assinada. Esse é um recurso dos métodos de criptografia de chave pública, chamado *assinaturas*.

7.2.4 Assinaturas

Suponhamos os usuários 1 e 2. Sejam C_1 e D_1, respectivamente, os processos de codificação e decodificação do usuário 1 e C_2 e D_2 os processos correspondentes do usuário 2. Para que um bloco a de mensagem seja assinada pelo usuário 1 é necessário que ele envie ao usuário 2 o $C_2(D_1(a))$. O usuário 2 tendo recebido $C_2(D_1(a)) = b$, ele primeiramente usa o processo D_2 e em seguida o processo C_1, ou seja, ele faz $C_1(D_2(b))$. Se ao final desse procedimento a mensagem tiver sentido, significa que o bloco recebido pelo usuário 2 foi decodificada com os processos certos, e portanto, a mensagem enviada é realmente do usuário 1.

Observação 7.2.6. *Lembramos que o processo D_1 só é conhecido do usuário 1, porém C_2 é de chave pública, por isso o usuário 1 tem conhecimento. Analogamente, temos que D_2 só é conhecido do usuário 2 e C_1 é de chave pública, e deste modo, o usuário 2 tem conhecimento. Dessa forma, a assinatura no método RSA é bastante segura, pois a probabilidade de que uma mensagem produzida sem D_1 seja decodificada por C_1 de modo que esta faça sentido é praticamente nula.*

Exemplo 7.2.6. *Vejamos um simples exemplo das assinaturas usando o método RSA. Suponhamos as chaves de codificação $(323, 5)_1$ e $(143, 7)_2$ dos usuários 1 e 2. Temos que $323 = 17.19$ e $143 = 11.13$, e assim, as chaves de decodificação são $(323, 173)_1$ e $(143, 103)_2$. Desejamos mandar a mensagem RSA assinada pelo usuário 1, como a mensagem pré-codificada usando a tabela de conversão do início da seção é 272810, temos que quebrá-la em blocos menores que 323, por exemplo, $272 - 8 - 10$. Logo, codificamos como*

$$272^{173} \equiv 17 \ (mod\ 323) \ \mid \ 8^{173} \equiv 145 \ (mod\ 323) \ \mid \ 10^{173} \equiv 147 \ (mod\ 323),$$

e deste modo,

$$17^7 \equiv 30 \ (mod\ 143) \ \mid \ 145^7 \equiv 128 \ (mod\ 143) \ \mid \ 147^7 \equiv 82 \ (mod\ 143).$$

Dessa maneira, o usuário 1 enviará a seguinte mensagem codificada $30 - 128 - 82$. Para o usuário 2 decodificar a mensagem deve proceder da seguinte maneira:

$$30^{103} \equiv 17 \ (mod\ 143) \ \mid \ 128^{103} \equiv 145 \ (mod\ 143) \ \mid \ 82^{103} \equiv 147 \ (mod\ 143)$$

e

$$17^5 \equiv 272 \ (mod\ 323) \ \mid \ 145^5 \equiv 8 \ (mod\ 323) \ \mid \ 147^5 \equiv 10 \ (mod\ 323).$$

O usuário 2 após decodificar a mensagem recebida terá a seguinte mensagem 272810 que

convertendo é RSA, como queríamos.

7.2.5 Exercícios

1. Pré-codifique, codifique e decodifique às seguintes mensagens, usando o algoritmo RSA:
   (a) Eu gosto de matemática.
   (b) Hoje está fazendo sol.
   (c) Minha família está viajando.
2. Fazendo uso do algoritmo RSA.
   (a) Construa uma tabela de pré-codifcação.
   (b) Pre-codifique, codifique e decodifique a frase: eu gosto de matemática.
   (c) Pré-codifique, codifique e decodifique a frase: hoje está fazendo sol.
   (d) Pré-codifique, codifique e decodifique a frase: minha casa está reformando.
3. Fazendo uso do algoritmo RSA.
   (a) Construa uma tabela de pré-codificação.
   (b) Pré-codifique, codifique e decodifique a frase: gostei muito desse livro.
   (c) Pré-codifique, codifique e decodifique a frase: este ano não vai chover.
4. Fazendo uso do algoritmo RSA.
   (a) Construa uma tabela de pré-codificação.
   (b) Pré-codifique, codifique e decodifique a frase: todos juntos venceremos.
   (c) Pré-codifique, codifique e decodifique a frase: amigos com fraternidade.
   (d) Pré-codifique, codifique e decodifique a frase; usando o algoritmo RSA.
5. Analise os seguintes problemas.
   (a) Se as chaves públicas de duas pessoas diferentes têm um primo em comum, então é possível quebrar o algoritmo RSA?
   (b) Se usamos o algoritmo RSA, mas codificamos a mensagem partindo-a em blocos que consistem de uma única letra, então é possível decodificar a mensagem e que o código não seja quebrado.
6. Fazendo o uso do algoritmo RSA.
   (a) Construa uma tavela de pré-decofificação.
   (b) Pré-codifique, codifique e decodifique a frase: adoro minhas filhas.
   (c) Pré-codifique, codifique e decodifique a frase: minha vida é uma maravilha.
   (d) Pré-codifique, codifique e decodifique a frase: meu caminho difere do seu.

Capítulo

8

Relações binárias

Conhecemos as operações fundamentais nos números naturais: a adição, a subtração, a multiplicação e a divisão. Mais explicitamente, dados dois números naturais, m e n, a adição associa o número $m + n$, chamado soma ou total de m com n; a subtração associa o número $m - n$, chamado de diferença entre m e n; a multiplicação, aos dois números, associa o número mn, chamado de produto de m por n; e a divisão associa o número m/n, chamado de quociente entre m e n. Observamos que a adição e a multiplicação de números naturais são sempre possíveis, isto é, dados dois números naturais é sempre possível encontrar um número natural que represente sua soma ou seu produto, o mesmo não ocorre quando se trata da subtração e da divisão.

Este capítulo tem como propósito de abordar os conceitos básicos que serão fundamentais para o entendimento dos demais capítulos do presente texto. Os conteúdos abordados são algumas noções sobre relações binárias, relações de equivalência, classes de equivalência, conjunto quociente e relações de ordem. Deste modo, neste capítulo, apresentamos as relações binárias juntamente com domínio e imagem, relação inversa, relações e equivalências, classes de equivalências, conjunto quociente e partição de um conjunto, e em seguida, apresentamos as relações de ordens juntamente com os limites superiores de um conjunto, máximo de um conjunto, limites inferiores de um conjunto, mínimo de um conjunto, supremo e ínfimo de um conjunto, elementos maximais e elementos minimais de um conjunto.

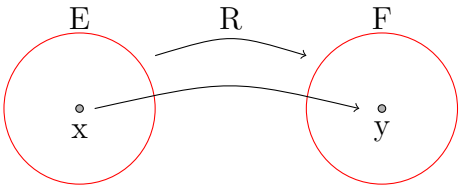
8.1 Relações binárias

Sejam E e F dois conjuntos não vazios. O produto cartesiano de E por F, denotado por $E \times F$, é definido por $E \times F = \{(x, y) : x \in E \text{ e } y \in F\}$. Neste caso, $(a, b) = (c, d)$ se, e somente

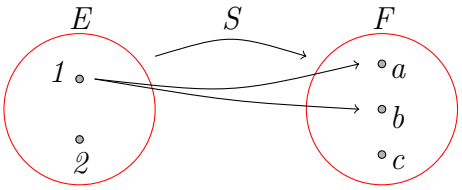
se, $a = c$ e $b = d$. Além disso, se $E = F$, então $E \times E = E^2$.

Definição 8.1.1. *Uma relação (binária) de E em F é um subconjunto R de $E \times F$. Se $E = F$, então R é chamada uma relação sobre E. De um modo geral, uma relação binária é qualquer conjunto de pares ordenados.*

Podemos representar E e F por meio do diagrama de Venn e indicamos cada par $(x, y) \in R$ por uma flecha com origem x e extremidade y, conforme a figura abaixo.



Exemplo 8.1.1. *Seja $E \times F = \{(1, x), (1, y), (1, z), (2, x), (2, y), (2, z)\}$, onde $E = \{1, 2\}$ e $F = \{a, b, c\}$. Assim, $R = \emptyset$, $S = \{(1, a); (1, b)\}$ e $T = E \times F$ são relações binárias. O diagrama de Venn da relação S é dada por:*



8.1.1 Domínio e imagem

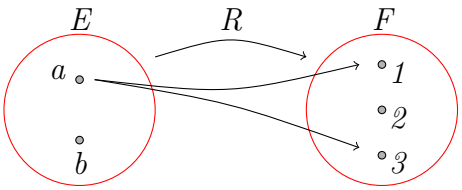
Sejam E e F conjuntos não vazios e R uma relação de E em F. Dados $a \in E$ e $b \in F$, se $(a, b) \in R$, dentotamos aRb, e se $(a, b) \notin R$, dentotamos aR_nb.

Exemplo 8.1.2. *Se $E = F = \{1, 2\}$ e $R = \{(1, 2), (2, 1)\}$, então $1R2$ e $2R1$. Mas, como $(1, 1), (2, 2) \notin R$, segue que $1R_n1$ e $2R_n2$.*

Definição 8.1.2. *Seja $R \subseteq E \times F$ uma relação.*

1. *O domínio de R é definido como $Dom(R) = \{x \in E :$ existe $y \in F$ tal que $(x, y) \in R\}$.*
2. *A imagem de R é definida como $Im(R) = \{y \in F :$ existe $x \in E$ tal que $(x, y) \in R\}$.*
3. *O contra-domínio de R é definido por $Cdom(R) = F$.*

Exemplo 8.1.3. *Se $E = \{a, b\}$, $F = \{1, 2, 3\}$ e $R = \{(a, 1), (a, 3)\}$, então $Dom(R) = \{a\}$, $Im(R) = \{1, 3\}$ e $Cdom(R) = \{1, 2, 3\}$. O diagrama de Venn é dado por:*



8.1.2 Relação inversa

Sejam E e F conjuntos não vazios e R uma relação de E em F.

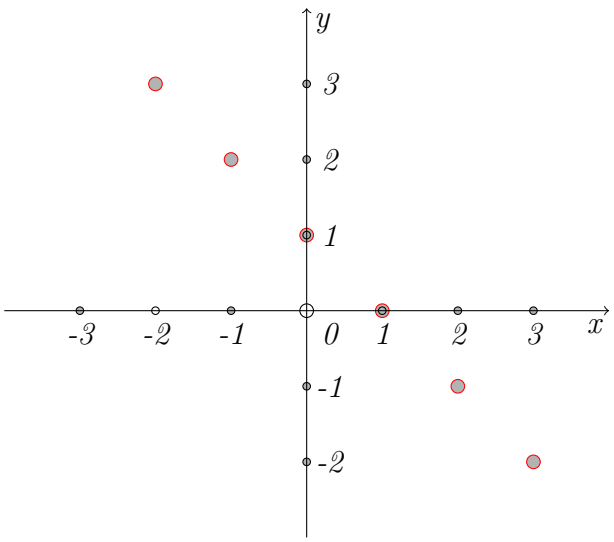
Definição 8.1.3. *A relação inversa de R é definida como $R^{-1} = \{(y, x) \in F \times E : (x, y) \in R\}$.*

Exemplo 8.1.4. *Se $E = \{a, b\}$, $F = \{1, 2, 3\}$ e $R = \{(a, 1), (a, 2)\}$, então $R^{-1} = \{(1, a), (2, a)\}$. Os diagramas de Venn de R e R^{-1} são dados, respectivamente, por:*

Exemplo 8.1.5. *Seja a relação $R \subseteq \mathbb{Z}^2$ definida por $R = \{(x, y) \in \mathbb{Z}^2 : x + y = 1\}$. Neste caso,*

1. *$Dom(R) = \{x \in \mathbb{Z} :$ existe $y \in \mathbb{Z}$ tal que $x + y = 1\} = \mathbb{Z}$,*
2. *$Im(R) = \{y \in \mathbb{Z} :$ existe $x \in \mathbb{Z}$ tal que $x + y = 1\} = \mathbb{Z}$ e*
3. *$R^{-1} = \{(y, x) \in \mathbb{Z}^2 : (x, y) \in R\} = \{(y, x) \in \mathbb{R}^2 : x + y = 1\} = R$.*

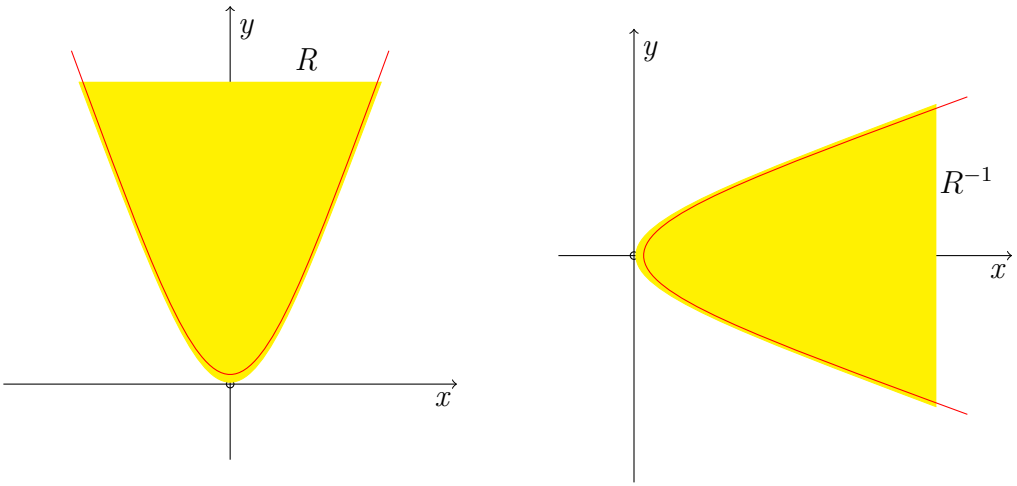
Graficamente, $R = R^{-1}$ é dada por



Exemplo 8.1.6. *Seja a relação $R \subseteq \mathbb{R}^2$ definida por $R = \{(x, y) \in \mathbb{R}^2 : y \geq x^2\}$. Neste caso,*

1. *$Dom(R) = \{x \in \mathbb{R} :$ existe $y \in \mathbb{R}$ tal que $y \geq x^2\} = \mathbb{R}$,*
2. *$Im(R) = \{y \in \mathbb{R} :$ existe $x \in \mathbb{R}$ tal que $y \geq x^2\} = \mathbb{R}_+$ e*
3. *$R^{-1} = \{(y, x) \in \mathbb{R}^2 : (x, y) \in R\} = \{(y, x) \in \mathbb{R} : y \geq x^2\} = \{(x, y) \in \mathbb{R}^2 : x \geq y^2\}$.*

Graficamente, R e R^{-1} são dadas, respectivamente, por



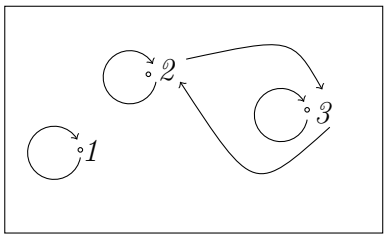
8.1.3 Relação de equivalência

O conceito de relação de equivalência é bastante intuitivo, mas de fundamental importância para o estudo de qualquer área da matemática. Para isso, sejam E um conjuntos não vazio e R uma relação sobre E.

Definição 8.1.4. *A relação R é chamada relação de equivalência se:*

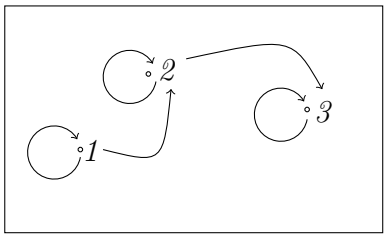
1. *xRx, para todo $x \in E$, ou seja, R é reflexiva.*
2. *Se xRy, então yRx, para todo $x, y \in E$, ou seja, R é simétrica.*
3. *Se xRy e yRz, então xRz, para todo $x, y \in E$, ou seja, R é transitiva.*

Exemplo 8.1.7. *Seja $E = \{1, 2, 3\}$. A relação $R = \{(1,1), (2,2), (3,3), (2,3), (3,2)\}$ é uma relação de equivalência, uma vez que é reflexiva, simétrica e transitiva.*



Exemplo 8.1.8. *Seja $E = \{1, 2, 3\}$. A relação $S = \{(1,1), (2,2), (3,3), (1,2), (2,3)\}$ não é uma*

relação de equivalência, pois S não é simétrica, uma vez que $(1,2) \in S$, mas $(2,1) \notin S$.

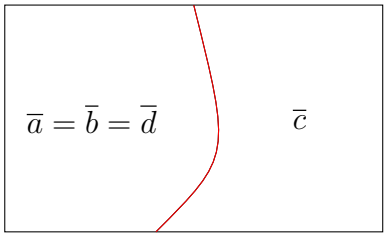


8.1.4 Classe de equivalência

A partir das relações de equivalência surgem as classes de equivalências que são de suma importância para gerar os conjuntos quocientes que veremos na próxima seção. Para isso, seja R uma relação de equivalência sobre um conjunto não vazio E.

Definição 8.1.5. *A classe de equivalência de um elemento $a \in E$, indicada por $\overline{a}$, é definida por $\overline{a} = \{x \in E : xRa\}$.*

Exemplo 8.1.9. *Seja $R = \{(a,a),(b,b),(c,c),(d,d),(a,b),(b,a),(b,d),(d,b),(a,d),(d,a)\}$ uma relação de equivalência sobre $E = \{a,b,c,d\}$. Neste caso, $\overline{a} = \{a,b,d\}$, $\overline{b} = \{a,b,d\}$, $\overline{c} = \{c\}$, $\overline{d} = \{a,b,d\}$, $\overline{a} \cap \overline{c} =$ e $\overline{a} \cup \overline{c} = E$. Graficamente, o conjunto E é dado por:*



Proposição 8.1.1. *Se R é uma relação de equivalência sobre E, então*

1. *$a \in \overline{a}$, para todo $a \in E$.*
2. *$E = \cup_{a \in E} \overline{a}$.*
3. *$\overline{a} \cap \overline{b} = \emptyset$ ou $\overline{a} = \overline{b}$, para todo $a, b \in E$.*

Demonstração. Para (1), como R é reflexiva, se $a \in E$, então aRa, ou seja, $a \in \overline{a}$. Para (2), por definição $\overline{a} \subseteq E$, e assim, $\cup_{a \in E} \overline{a} \subseteq E$. Por outro lado, se $a \in E$, então $a \in \overline{a}$, ou seja, $a \in \cup_{a \in E} \overline{a}$. Portanto, $E = \cup_{a \in E} \overline{a}$. Para (3), se $\overline{a} \cap \overline{b} \neq \emptyset$, então existe $x \in E$ tal que $x \in \overline{a} \cap \overline{b}$. Assim, $x \in \overline{a}$ e $x \in \overline{B}$, ou seja, xRa e xRb. Como R é simétrica e transitiva, segue que aRb. Agora, se $x \in \overline{a}$, então xRa. Como R é transitiva, segue que xRb, ou seja, $x \in \overline{b}$. Assim, $\overline{a} \subseteq \overline{b}$. De modo análogo, segue que $\overline{b} \subseteq \overline{a}$. Portanto, $\overline{a} = \overline{b}$. □

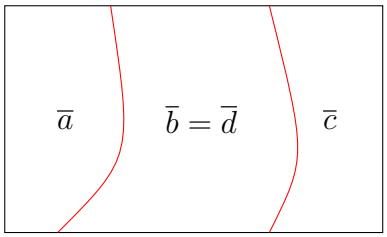
Observação 8.1.1. *As classes de equivalências determinam uma partição em E. Reciprocamente, se existe uma partição em E, então existe uma relação de equivalência R sobre E, de modo que, se aRb, então a e b pertencem ao mesmo conjunto.*

8.1.5 Conjunto quociente

Seja R uma relação de equivalência sobre um conjunto não vazio E.

Definição 8.1.6. *O conjunto quociente de E por R, indicado por E/R, é o conjunto de todas as classes de equivalências segundo a relação R, ou seja, $E/R = \{\overline{a} : a \in E\}$.*

Exemplo 8.1.10. *Seja R uma relação de equivalência sobre $E = \{a, b, c, d\}$ dada por $R = \{(a, a), (b, b), (c, c), (d, d), (b, d), (d, b)\}$. Neste caso, $\overline{a} = \{a\}$, $\overline{b} = \{b, d\}$, $\overline{c} = \{c\}$ e $\overline{d} = \{b, d\}$. Assim, $E/R = \{\{a\}, \{b, d\}, \{c\}\}$, ou seja, o conjunto quociente E/R é dado por*



8.1.6 Partição de um conjunto

Seja E um conjunto não vazio.

Definição 8.1.7. *Uma família $\mathcal{F}$ de subconjuntos não vazios de E é uma partição de E se:*

1. *$A, B \in \mathcal{F}$, então $A = B$ ou $A \cap B = \emptyset$, e*
2. *$\cup_{A \in \mathcal{F}} A = E$.*

Exemplo 8.1.11. *A família $\mathcal{F} = \{\{a\}, \{b, c\}, \{d\}\}$ é uma partição do conjunto $E = \{a, b, c, d\}$, uma vez que $E = \{a\} \cup \{b, c\} \cup \{d\}$ e $\{a\} \cap \{b, c\} = \{a\} \cap \{d\} = \{b, c\} \cap \{d\} = \emptyset$.*

Exemplo 8.1.12. *Se $P = \{x \in \mathbb{Z} : x \text{ é par}\}$ e $I = \{x \in \mathbb{Z} : x \text{ é impar}\}$, então $\mathcal{F} = \{P, I\}$ é uma partição de $\mathbb{Z}$, uma vez que $\mathbb{Z} = P \cup I$ e $P \cap I = \emptyset$.*

Exemplo 8.1.13. *A família $\mathcal{F} = \{]-\infty, -20],]-20, -5[, [-5, 23],]23, \infty[\}$ é uma partição de $\mathbb{R}$, uma vez que*

1. *$\mathbb{R} =]-\infty, -20] \cup]-20, -5[\cup [-5, 23] \cup]23, \infty[$ e*
2. *$]-\infty, -20] \cap]-20, -5[=]-\infty, -20] \cap [-5, 23] =]-\infty, -20] \cap]23, \infty[=]-20, -5[\cap [-5, 23] =]-20, -5[\cup]23, \infty[= [-5, 23] \cap]23, \infty[= \emptyset$.*

Veremos, a seguir, que via uma relação de equivalência sobre um conjunto não vazio E, fica determinada uma partição de E e vice-versa.

Proposição 8.1.2. *Se R é uma relação de equivalência sobre um conjunto E, então E/R é uma partição sobre E.*

Demonstração. Seja $\overline{a} \in E/R$. Como $a \in \overline{a}$, segue que $\overline{a} \neq \emptyset$, para todo $a \in E$. Se $\overline{a}, \overline{b} \in E/R$, então $\overline{a} \cap \overline{b} = \emptyset$ ou $\overline{a} = \overline{b}$. Finalmente, $\cap_{a \in E} \overline{a} = E$. Portanto, E/R é uma partição de E. □

Proposição 8.1.3. *Se $\mathcal{F}$ é uma partição de E, então existe uma relação de equivalência R sobre E tal que $E/R = \mathcal{F}$.*

Demonstração. Seja R uma relação sobre E definida como

$$xRy \text{ se, e somente se, existe } A \in \mathcal{F} : x, y \in A.$$

Mostramos que R é uma relação de equivalência sobre E. Assim, se $x \in E$, então existe $A \in \mathcal{F}$ tal que $x \in A$, ou seja, xRx. Agora, se $x, y \in E$ com xRy, então existe $A \in \mathcal{F}$ tal que $x, y \in A$. Logo, $y, x \in A$, ou seja, yRx. Finalmente, se $x, y, z \in E$ com xRy e yRz, então existem $A, B \in \mathcal{F}$ tal que $x, y \in A$ e $y, z \in B$. Como $A \cap B \neq \emptyset$, segue que $A = B$. Portanto, xRz, ou seja, R é uma relação de equivalência sobre E. □

8.1.7 Exercícios

1. Determine todas as relações sobre o conjunto:
   (a) $A = \{a, b\}$, com $a \neq b$.
   (b) $A = \{a, b, c\}$, com $a \neq b$, $a \neq c$ e $b \neq c$.
2. Sejam A um conjunto de 5 elementos e $R = \{(0, 1), (1, 2), (2, 3), (3, 4)\}$ uma relação sobre A. Determine:
   (a) Os elementos de A.
   (b) Domínio e imagem de R.
   (c) Os elementos, domínio e imagem de R^{-1}.
   (d) Os gráficos de R e R^{-1}.
3. Seja A o conjunto das retas definidas pelos vértices de um paralelogramo. Seja a relação R sobre A definida por $xRy \iff x$ é paralelo a y.
   (a) Determine os elementos de R.
   (b) Quais as propriedades que R satisfaz?
4. Sejam os conjuntos $A = \{0, 2, 4, 6, 8\}$ e $B = \{1, 3, 5, 7, 9\}$.
   (a) Determine os elementos de $R = \{(x, y) \in A \times B : y = x + 1\}$.
   (b) Determine os elementos de $S = \{(x, y) \in A \times B : x \leq y\}$.
   (c) Determine R^{-1} e S^{-1}.
5. Esboce o gráfico das seguintes relações sobre $\mathbb{R}$.

(a) $R = \{(x, y) \in \mathbb{R}^2 : x + y \leq 2\}$.

(b) $R = \{(x, y) \in \mathbb{R}^2 : y^2 = x\}$.

(c) $R = \{(x, y) \in \mathbb{R}^2 : 9x^2 + 4y^2 = 36\}$.

6. Esboce o gráfico e determine $D(R)$, $Im(r)$ e R^{-1} das seguintes relações sobre $\mathbb{R}$.

(a) $R = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 4\}$.

(b) $R = \{(x, y) \in \mathbb{R} : x^2 + y^2 \geq 16\}$.

(c) $R = \{(x, y) \in \mathbb{R}^2 : x^2 + 2 = y^2\}$.

7. Seja A um conjunto com n elementos.

(a) Quantas relações reflexivas existem sobre A?

(b) Quantas relações simétricas existem sobre A?

(c) Quantas relações transitivas existem sobre A?

8. Determine $Dom(R)$, $Im(R)$ e R^{-1}.

(a) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : 4x^2 + 9y^2 = 36\}$.

(b) $R = \{(x, y) \in \mathbb{R}^2 : x - 3 = 7\}$.

9. Sejam $a, b, m \in \mathbb{Z}$ tal que $m > 1$. Defina a relação aRb se, e somente se, $a - b = mk$, para algum $k \in \mathbb{Z}$.

(a) Mostre que R é uma relação de equivalência.

(b) Determine o conjunto quociente $\mathbb{Z}/R$.

10. Sejam A e B conjuntos com m e n elementos, respectivamente. Determine o número de elementos de $A \times B$ e o número de relações de A em B.

11. Seja R uma relação sobre $A = \{1, 2, 3, 4, 5\}$ definida por $xRy \iff x - y = 2k$, para algum $k \in \mathbb{Z}$. Determine os elementos de R e quais propriedades que R satisfaz.

12. Seja R uma relação sobre $\mathbb{N} - \{0\}$ definida por $R = \{(x, y) : x, y \in \mathbb{N} - \{0\} \text{ e } 2x + y = 10\}$. Determine:

(a) Domínio e imagem de R.

(b) R^{-1} e domínio e imagem de R^{-1}.

13. Seja $E = \{x \in \mathbb{Z} :| x |\leq 5\}$ e R uma relação sobre E definida por $xRy \iff x^2 + 2x = y^2 + 2y$. Mostre que R é uma relação de equivalência e encontre E/R.

14. Mostre que $R = \{(x, y) \in \mathbb{R}^2 : x - y \in \mathbb{Q}\}$ é uma relação de equivalência sobre $\mathbb{R}$ e determine as classes de equivalências de $1/2$ e $\sqrt{2}$.

15. Seja R uma relação sobre $\mathbb{C}$ definida por $(x + yi)R(z + wi) \iff x^2 + y^2 = z^2 + w^2$.

(a) Mostre que R é uma relação de equivalência.

(b) Determine a classe $\overline{1+i}$.

16. Construir sobre o conjunto $E = \{a, b, c, d\}$ relações binárias R_1, R_2 e R_3, onde R_1 seja apenas reflexiva, R_2 seja apenas simétrica e R_3 seja apenas transitiva.

17. Se R é uma relação de equivalência, mostre que R^{-1} é uma relação de equivalência.

18. Sejam R e S relações sobre um conjunto não vazio E.

(a) Mostre que $R^{-1} \cup S^{-1} = (R \cap S)^{-1}$.

(b) Mostre que $R^{-1} \cap S^{-1} = (R \cup S)^{-1}$.

(c) Mostre que $R \cup R^{-1}$ é simétrica.

19. Sejam R e S relações sobre um conjunto não vazio E.

(a) Se R e S são transitivas, mostre que $R \cap S$ é transitiva.

(b) Se R e S são simétricas, mostre que $R \cap S$ e $R \cup S$ são simétricas.

(c) Se R e S são reflexivas, mostre que $R \cap S$ e $R \cup S$ são reflexivas.

(d) Se R é anti-simétrica, mostre que R^{-1} também é.

20. Seja R uma relação sobre $\mathbb{C}$ definida por $(a+bi)R(c+di) \iff b = d$.

(a) Mostre que R é uma relação de equivalência.

(b) Determine o conjunto quociente $\mathbb{C}/R$.

21. Sejam $E = \mathbb{N}$ e R definida por $(a, b)R(c, d)$ se, e somente se, $a + b = c + d$. Mostre que R é uma relação de equivalência.

22. Seja S uma relação sobre $\mathbb{Z} \times \mathbb{Z}^*$ definida por $(a, b)S(c, d)$ se, e somente se, $ad = bc$. Mostre que S é uma relação de equivalência.

23. Sejam $E = \mathbb{C}$ e R definida por $(a+bi)R(c+di)$ se, e somente se, $a \leq c$ e $b \leq d$. Verifique se R é reflexiva, simétrica, anti-simétrica e transitiva.

24. Seja R uma relação sobre $\mathbb{N} - \{0\}$ definida por $(a, b)R(c, b)$ se, e somente se, c é um múltiplo de a e $b \leq d$. Mostre que R é uma relação de equivalência.

25. Seja R uma relação sobr $A = \{x \in \mathbb{Z} : 0 \leq x \leq 10\}$ definida por $xRy \iff x - y = 4x$.

(a) Mostre que R é uma relação de equivalência.

(b) Determine o conjunto quociente A/R.

26. Sejam $E = \{-3, -2, -1, 0, 1, 2, 3\}$ e $R = \{(x, y) \in E^2 : x+ \mid x \mid = y+ \mid y \mid\}$. Mostre que R é uma relação de equivalência e determine E/R.

27. Seja R uma relação sobre $\mathbb{Q}$ definida por $xRy \longleftrightarrow x - y \in \mathbb{Z}$. Mostre que R é uma relação de equivalência e determine $\overline{1}$ e $\overline{1/2}$.

28. Mostre que $R = \{(a + bi, c + di) \in \mathbb{C}^2 : a \leq c \text{ e } b = d\}$ é uma relação de equivalência e descreva $\mathbb{C}/R$.

29. Sejam E um conjunto não vazio e $A \subseteq E$.

    (a) Mostre que $xRy \leftrightarrow x \cap A = y \cap A$ é uma relação de equivalência sobre $\mathcal{P}(E)$.

    (b) Mostre que $xSy \leftrightarrow x \cup A = y \cup A$ é uma relação de equivalência sobre $\mathcal{P}(E)$.

30. Sejam $p(x_1, y_1)$ e $q(x_2, y_2)$ pontos de $\mathbb{R}^2$. Mostre que são relações de equivalências:

    (a) $pRq \Longleftrightarrow x_1y_1 = x_2y_2$.

    (b) $pSq \Longleftrightarrow y_2 - y_1 = x_2 - x_1$.

    (c) $pTq \Longleftrightarrow x_1^2 + y_1^2 = x_2^2 + y_2^2$.

31. Verifique se as relações R abaixo sobre $\mathbb{Z}$ é reflexiva, simétrica, anti-simétrica e transitiva.

    (a) aRb se, e somente se, $a + b = 7$.

    (b) aRb se, e somente se, b é um mútiplo de $(a - b)$.

    (c) aRb se, e somente se, $a - b$ é mútiplo de $m > 1$.

32. Seja E o conjunto de todas as retas do plano. Seja R uma relação sobre E definida por xRy se, e somente se, $x = y$ ou $x \cap y = \emptyset$.

    (a) Mostre que R é uma relação de equivalência.

    (b) Determine a classe de equivalência. $\overline{x}$.

8.2 Relação de ordem

O conceito de relação de ordem é bastante intuitivo. Podemos ver diariamente muitos exemplos de relações de ordem, como por exemplo: uma fila em uma sorveteria, a ordem de prioridades de execução das nossas tarefas diárias, a ordenação léxica de nomes em uma lista de presença, a ordenação numérica de itens a serem comprados ordenados pelos respectivos preços e outros.

Seja R uma relação binária sobre um conjunto não vazio E. Neste caso, é muito comum usar a notação $a \preceq b$, e $a \prec b$ quando $a \neq b$ e $a \preceq b$.

Definição 8.2.1. *A relação R é chamada uma relação de ordem (parcial) sobre E se:*

1. *aRa, para todo $a \in E$, ou seja, R é reflexiva.*

2. *Se aRb e bRa, então $a = b$, onde $a, b \in E$, ou seja, R é anti-simétrica.*

3. Se aRb e bRc, então aRc, para todo $a, b, c \in E$, ou seja, R é transitiva.

Neste caso, quando $a, b \in E$ e aRb, o elemento a é dito que precede b.

Em outras palavras, uma relação R sobre um conjunto E é uma relação de ordem se R for: reflexiva, antisimétrica e transitiva. A relação de ordem como acima definida é conhecida também como relação de ordem parcial.

Definição 8.2.2. *Uma relação binária R é chamada uma relação de quasi-ordem se é reflexiva e transitiva.*

Exemplo 8.2.1. *O conjunto dos inteiros $\mathbb{Z}$ com a relação R definida por aRb se, e somente se, b é um múltiplo de a, é uma quase-ordem.*

Um conjunto E com uma ordem parcial R é chamado um conjunto parcialmente ordenado mediante a ordem R. Uma ordem parcial R sobre E é chamada uma ordem total se para todo $x, y \in E$ tem-se que xRy ou yRx, ou seja, quaisquer dois elementos $x, y \in E$ são comparáveis mediante a relação de ordem R. Um conjunto E com uma ordem total é chamado conjunto totalmente ordenado mediante a ordem R.

Exemplo 8.2.2. *A relação R definida por aRb se, e somente se, b é um mútiplo de a é uma relação de ordem parcial sobre $\mathbb{N}$. De fato, como $a = a.1$, para todo $a \in \mathbb{N}$, segue que aRa. Agora, se aRb e bRa, então b é um múltiplo de a e a é um múltiplo de b, onde $a, b \in \mathbb{N}$. Assim, $b = ac_1$ e $a = bc_2$, onde $c_1, c_2 \in \mathbb{N}$, e portanto, $a = bc_2 = a(c_1c_2)$. Como $c_1c_2 \neq 0$, segue que $a = b$. Finalmente, se aRb e bRc, com $a, b, c \in \mathbb{N}$, então $b = ac_1$ e $c = bc_2$, onde $c_1, c_2 \in \mathbb{N}$, e portanto, $c = bc_2 = a(c_1c_2)$. Como $c_1c_2 \neq 0$, segue que c é um mt́iplo de a, ou seja, aRc. Portanto, R é uma ordem parcial. A ordem não é total, uma vez que $3 \neq 4$, 4 não é múltiplo de 3 e 3 não é múltiplo de 4.*

Exemplo 8.2.3. *A relação R definida por $xRy \iff x \leq y$ é uma relação de ordem total sobre $\mathbb{R}$. De fato, como $a \leq a$, para todo $a \in \mathbb{R}$, segue que aRa. Agora, se aRb e bRa, onde $a, b \in \mathbb{R}$, então $a \leq b$ e $b \leq a$, e portanto, $a = b$. Agora, se aRb e bRc, com $a, b, c \in \mathbb{R}$, então $a \leq b$ e $b \leq c$, e portanto, $a \leq c$, ou seja, aRc. Finalmente, dados $a, b \in \mathbb{R}$, segue que $a \leq b$ ou $b \leq a$. Portanto, R é uma ordem total.*

Exemplo 8.2.4. *Sejam A um conjunto não vazio e $\mathcal{P}(A)$ o conjunto das partes de A. A relação R sobre $\mathcal{P}(A)$ definida por $xRy \iff x \subset y$ é uma relação de ordem parcial. De fato, como $a \subset a$, para todo $a \in \mathcal{P}(A)$, segue que aRa. Agora, se aRb e bRa, onde $a, b \in \mathcal{P}(A)$, então $a \subset b$ e $b \subset a$, ou seja, $a = b$. Finalmente, se aRb e bRc, com $a, b, c \in \mathcal{P}(A)$, então $a \subset b$ e $b \subset c$, e portanto, $a \subset c$, ou seja, aRc. Portanto, R é uma ordem parcial. A ordem não é total pois em $\mathcal{P}(A)$ existem conjuntos $\{a\}$ e $\{b\}$, com $a \neq b$, tal que $a \not\subset b$ e $b \not\subset a$.*

8.2.1 Ordem lexicográfica

As palavras de um dicionário são listadas em ordem alfabética ou ordem lexicográfica, que é baseada na ordem das letras do alfabeto.

Sejam E_1 e E_2 conjuntos com ordens dadas por $\preceq^1$ e $\preceq^2$, respectivamente. Uma ordem lexicográfica $\preceq$ em $E_1 \times E_2$ é definida por

$$(a_1, a_2) \preceq (b_1, b_2) \longleftrightarrow a_1 \preceq^1 b_1 \text{ ou } a_1 = b_1 \text{ e } a_2 \preceq^2 b_2.$$

Em geral, se $(E_1, \preceq^1)$, $(E_2, \preceq^2)$, ..., $(E_n, \preceq^n)$. Uma ordem parcial em $E_1 \times E_2 \times \cdots \times E_n$ é definida por

$$(a_1, a_2, \ldots, a_n) \preceq (b_1, b_2, \ldots, b_n)$$

se, e somente se,

$$a_1 \preceq^1 b_1 \text{ ou existe um inteiro } m \geq 1 \text{ tal que } a_1 = b_1, \ldots, a_m = b_m \text{ e } a_{m+1} \preceq^{m+1} b_{m+1}.$$

8.2.2 Limites superiores de um conjunto

Seja R uma relação de ordem sobre um conjunto não vazio E.

Definição 8.2.3. *Seja $A \subseteq E$ um subconjunto. Um elemento $a \in E$ é chamado um limite superior de A se todo elemento de A precede a, ou seja, xRa para todo $x \in A$.*

Exemplo 8.2.5. *Sejam a relação de ordem R sobre $\mathbb{Z}$ definida por $xRy \iff x \leq y$ e $A = \{0, 1, 2, 3\}$. Os limites superiores de A são todos os $a \in \mathbb{Z}$ tal que xRa, para todo $x \in A$, ou seja, $a = 3, 4, 5, 6, \cdots$*

Exemplo 8.2.6. *Sejam $E = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$ e R a relação de ordem sobre E definida por $xRy \iff x \subset y$. Se $A = \{\{1\}, \{1, 3\}\}$, então os limites superiores de A são os subconjuntos a de E tal que xRa, para todo $x \in A$. Assim, $\{1, 3\}$ e $\{1, 2, 3\}$.*

8.2.3 Máximo de um conjunto

Sejam R uma relação de ordem sobre um conjunto não vazio E e $A \subseteq E$, onde $A \neq \emptyset$.

Definição 8.2.4. *O máximo de A, se existir, é um limite superior de A que pertence a A e denotado por $max(A)$.*

Exemplo 8.2.7. *O máximo de $A = \{0, 1, 2, 3\}$ com a relação de ordem R sobre $\mathbb{Z}$ definida por $xRy \leftrightarrow x \leq y$ é o elemento 3, pois é um limite superior que pertence a A.*

Exemplo 8.2.8. *O máximo do conjunto $A = \{\{1\}, \{1, 3\}\}$ com a relação de ordem R sobre o cojunto $E = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$ definida por $xRy \iff x \subset y$ é o elemento $\{1, 3\}$, pois é um limite superior que pertence a A.*

Exemplo 8.2.9. *Os limites superiores do conjunto $A = \{\{1\}, \{2\}\}$ com a relação de ordem R sobre o conjunto $E = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$ definida por $xRy \iff x \subset y$ são os elementos $\{1, 2\}$ e $\{1, 2, 3\}$. Como não pertencem a A, segue que A não tem máximo.*

8.2.4 Limites inferiores de um conjunto

Seja R uma relação de ordem sobre um conjunto não vazio E.

Definição 8.2.5. *Seja $A \subseteq E$ um subconjunto. Um elemento $a \in E$ é chamado um limite inferior de A se a precede todo elemento de A, ou seja, aRx para todo $x \in A$.*

Exemplo 8.2.10. *Sejam a relação de ordem R sobre $\mathbb{Z}$ definida por $xRy \iff x \leq y$ e $A = \{5, 10, 100\}$. Os limites inferiores de A são os elementos $a \in \mathbb{Z}$ tal que $a \leq 5$.*

Exemplo 8.2.11. *Sejam o conjunto $E = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$ e R uma relação de ordem sobre E definida por $xRy \iff x \subset y$. Se $A = \{\{1,2\}, \{1,3\}\}$, então os limites inferiores de A são $\emptyset$ e $\{1\}$.*

8.2.5 Mínimo de um conjunto

Sejam R uma relação de ordem sobre um conjunto não vazio E e $A \subseteq E$, onde $A \neq \emptyset$.

Definição 8.2.6. *O mínimo de A, se existir, é um limite inferior de A que pertence a A e denotado por $min(A)$.*

Exemplo 8.2.12. *O mínimo do conjunto $A = \{5, 10, 100\}$ com a relação de ordem R sobre $\mathbb{Z}$ definida por $xRy \iff x \leq y$ é o elemento 5, pois é um limite inferior que pertence a A.*

Exemplo 8.2.13. *O mínimo do conjunto $A = \{\{1\}, \{1,3\}\}$ com a relação de ordem R, definida por $xRy \iff x \subset y$, sobre $E = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$ é o elemento $\{1\}$, pois é um limite inferior que pertence a A.*

Exemplo 8.2.14. *O conjunto $A = \{\{1,2\}, \{1,3\}\}$ com a relação de ordem R, definida por $xRy \iff x \subset y$, sobre $E = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$ não possui mínimo.*

Proposição 8.2.1. *Se A é um subconjunto de um conjunto parcialmente ordenado E e existe máximo (mínimo) de A, então o máximo (mínimo) é único.*

Demonstração. Para o máximo, sejam M_1 e M_2 máximos de A. Assim, como M_1 é máximo de A e $M_2 \in A$, segue que M_2RM_1. De modo análogo, como M_2 é máximo de A e $M_1 \in A$, segue que M_1RM_2. Logo, $M_1 = M_2$. Para o mínimo, sejam m_1 e $_2$ mínimos de A. Assim, como m_1 é mínimo de A e $m_2 \in A$, segue que m_1Rm_2. De modo análogo, como m_2 é mínimo de A e $m_1 \in A$, segue que m_2Rm_1. Logo, $m_1 = m_2$. □

8.2.6 Supremo e ínfimo de um conjunto

Sejam R uma relação de ordem sobre um conjunto não vazio E e $A \subseteq E$, onde $A \neq \emptyset$.

Definição 8.2.7. *O supremo do conjunto A, denotado por $m = sup(A)$, é o mínimo do conjunto dos limites superiores de A, ou seja,*

1. *xRm, para todo $x \in A$, e*

2. *se $a \in E$ e xRa, para todo $x \in A$, então mRa.*

Exemplo 8.2.15. *O supremo do conjunto $A = \{\{1\}, \{1,3\}\}$ com a relação de ordem R sobre o conjunto $E = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$ definida por $xRy \iff x \subset y$ é o elemento $\{1,3\}$. Agora, se $A = \{\{2\}, \{3\}\}$, então os limites superiores de A são $\{2,3\}$ e $\{1,2,3\}$. O $sup(A) = \{2,3\}$ e A não possui máximo.*

Exemplo 8.2.16. *Seja a relação de ordem $xRy \iff x \leq y$ sobre $\mathbb{R}$. Os limites superiores do conjunto $A = \{1/2, 2/3, 3/4, \cdots\}$ são $\{x \in \mathbb{R} : x \geq 1\}$. O supremo de A é o elemento 1 e não tem máximo.*

Definição 8.2.8. *O ínfimo de A, denotado por $m = inf(A)$, é o máximo do conjunto dos limites inferiores de A, ou seja,*

1. *mRx, para todo $x \in A$, e*

2. *se $a \in E$ e aRx, para todo $x \in A$, então aRm.*

Exemplo 8.2.17. *O ínfimo do conjunto $A = \{\{1\}, \{1,3\}\}$ com a relação de ordem R sobre o conjunto $E = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$ definida por $xRy \iff x \subset y$ é o elemento $\{1\}$. Agora, se $A = \{\{2\}, \{3\}\}$, então limites superiores de A são $\{2,3\}$ e $\{1,2,3\}$. O $sup(A) = \{2,3\}$ e A não possui máximo.*

Exemplo 8.2.18. *Seja a relação de ordem R sobre $\mathbb{R}$ definida por $xRy \iff x \leq y$. Os limites inferiores de $A =]0,2[$ são $\{x \in \mathbb{R} : x \leq 0\}$. O ínfimo é o elemento 0 e não possui mínimo.*

8.2.7 Elementos maximais e minimais de um conjunto

Os elementos maximais e minimais de um subconjunto não vazio de um conjunto parcialmente ordenado são definidos da seguinte maneira.

Definição 8.2.9. *Seja A um subconjunto não vazio de um conjunto parcialmente ordenado E.*

1. *Um elemento $m_1 \in A$ é um elemento maximal de A se não existe $x \in A$ tal que m_1Rx, ou seja, quando o único elemento de A precedido por m_1 é ele próprio.*

2. *Um elemento $m_o \in A$ é um elemento minimal de A se não existe $x \in A$ tal que xRm_o, ou seja, quando o único elemento de A que precede m_o é ele próprio.*

Exemplo 8.2.19. *Em $\mathbb{R}$ não existem elementos maximais ou minimais com respeito a ordem usual.*

Exemplo 8.2.20. *Em $D(36)$ (divisores de 36), considere o subconjunto $A = \{2,3,6,12,18\}$. Os números 2 e 3 são elementos minimais, e os números 12 e 18 são elementos maximais em A, mas A não possui máximo e nem mínimo.*

8.2.8 Exercícios

1. Seja R um relação sobre $\mathbb{N} - \{0\}$ definida por xRy se, e somente se y é um múltiplo de x.

   (a) Mostre que R é uma relação de ordem parcial.

   (b) Se $A = \{3, 4\}$, determine os limites superiores, limites inferiores, máximo, mínimo, supremo e ínfimo de A.

2. Seja a relação R sobre $\mathbb{C}$ definida por $(a + bi)R(c + di)$ se, e somente se, $a \leq c$ e $b \leq d$.

   (a) Mostre que R é uma ordem parcial sobre $\mathbb{C}$.

   (b) Determine os limites superiores, limites superiores, ínfimo, supremo, máximo, mínimo de $A = \{2 + i; 1 + 2i\}$.

3. Seja R é uma relação de ordem parcial sobre um conjunto não vazio E.

   (a) Mostre que R^{-1} também é uma relação de ordem parcial.

   (b) Verifique se $R \cup R^{-1}$ é uma relação de ordem parcial.

4. Seja a relação R sobre $\mathbb{N} \times \mathbb{N} - \{(0, 0)\}$ definida por $(a, b)R(c, d)$ se, e somente se, c é um múltiplo de a e $b \leq d$.

   (a) Mostre que R é uma relaçao de ordem parcial.

   (b) Determine os limites inferiores, limites superiores, ínfimo, supremo, máximo, mínimo de $A = \{(2, 1); (1, 2)\}$.

5. Seja a relação R sobre $\mathbb{N} \times \mathbb{N} - \{(0, 0)\}$ definida por $(a, b)R(c, d)$ se, e somente se, $a \leq c$ e d é um múltiplo de b.

   (a) Mostre que R é uma relação de ordem parcial.

   (b) Determine os limites inferiores, limites superiores, ínfimo, supremo, máximo e mínimo do conjunto $A = \{(3, 1); (1, 3)\}$.

6. Seja o conjunto $E = \{\{a\}; \{b\}; \{a, b, c\}; \{a, b, d\}; \{a, b, c, d\}; \{a, b, c, d, e\}\}$.

   (a) Mostre que E com a relação de inclusão é uma relação de ordem parcial.

   (b) Determine os limites inferiores, limites superiores, ínfimo, supremo, máximo e mínimo do conjunto A, onde $A = \{\{a, b, c\}; \{a, b, d\}; \{a, b, c, d\}\}$.

7. Seja a relação sobre $\mathbb{N} - \{0\}$ definida por aRb se, e somente se, b é um múltiplo de a.

   (a) Mostre que a relação R é uma relação de ordem parcial.

   (b) Quais dos seguintes conjuntos são totalmente ordenados $A = \{24, 2, 6\}$, $B = \{3, 15, 5\}$, $C = \{15, 5, 30\}$ e $D = \mathbb{N}$.

8. Seja a relação sobre $\mathbb{Q}$ definida por xRy se, e somente se, $x \leq y$.

(a) Mostre que R é uma relação de ordem total.

(b) Determine os limites inferiores, limites superiores, ínfimo, supremo, máximo e mínimo do conjuto $A = \{x \in \mathbb{Q} : 0 \leq x^2 \leq 2\}$.

9. Sejam $E = \{a, b, c, d\}$ e $\mathcal{P}(E)$ o conjunto das partes de E.

(a) Mostre que a relação de inclusão é uma relação de ordem parcial em $\mathcal{P}(E)$.

(b) Determine os limites superiores, limites superiores, ínfimo, supremo, máximo, mínimo de $A = \{\emptyset, \{a, d\}, \{c\}\}$.

10. Determine infimo, supremo, mínimo e máximo (se existirem) dos seguintes conjuntos:

(a) $A = \left\{ \dfrac{(-1)^n + n}{n^2} : n \in \mathbb{N} \right\}$.

(b) $B = \left\{ x \in \mathbb{R} : -1 \leq \dfrac{x-2}{x+3} \leq 0 \right\}$.

11. Seja R uma relação sobre $\mathbb{N}$ definida por aRb se, e somente se, b é um múltiplo de a.

(a) Mostre que R é uma relação de ordem parcial sobre $\mathbb{N}$.

(b) R é simétrica? Porque?

12. Seja R uma relação sobre $\mathbb{Z}$ definida por aRb se, e somente se, b é um múltiplo de a.

(a) Mostre que R não é uma relação de ordem parcial sobre $\mathbb{Z}$.

(b) R é simétrica? Porque?

13. Seja R uma relação sobre $\mathbb{Z}$ definida por aRb se, e somente se, $a - b$ é um múltiplo de m, onde $m > 1$ é um inteiro.

(a) Verifique se R é uma relação de ordem parcila sobre $\mathbb{Z}$.

(b) R é simétrica? Porque?

14. Seja E um conjunto formado por subconjuntos. Seja a relação R definida sobre E por $\mathcal{A}R\mathcal{B}$ se, e somente se, $\mathcal{A} \cap \mathcal{B} = \mathcal{A}$.

(a) Mostre que R é uma relação de ordem ordem parcial.

(b) É ordem total? Porque?

15. Seja a relação sobre $\mathbb{C}$ definida por $(a + bi)R(c + di)$ se, e somente se, $a < c$ ou ($a = c$ e $b \leq d$).

(a) Mostre que R é uma relação de ordem parcial. É total?

(b) Determine o infimo, supremo, mínimo e máximo (se existirem) do conjunto $A = \{1 + 2i, 3 - 2i, -1 + 3i\}$.

16. Sejam A e B conjuntos parcialmente ordenados com ordens $\preceq^A$ e $\preceq^B$, respectivamente, onde $a \prec b$ significa que $a \preceq b$ e $a \neq b$. Seja a relação $(a, b)R(c, d)$ se, e somente se, $a \prec^A c$ ou ($a = c$ e $b \preceq^B d$).

    (a) Mostre R é uma relação de ordem parcial.

    (b) Se os conjuntos são totalmente ordenados, mostre R é uma ordem total.

17. Sejam A_1, A_2, ... A_n conjuntos totalmente ordenados com ordens totais dadas por $<_1, <_2$ $, \ldots, <_n$, respectivamente. Seja a relação R sobre $A = A_1 \times A_2 \times \cdots \times A_n$ definida por

$$(a_1, a_2, \ldots, a_n)R(b_1, b_2, \ldots, b_n) \longleftrightarrow (\exists m > 0)(\forall i < m)(a_i = b_i \text{ e } a_m <_m b_m).$$

    Mostre que R é uma ordem total sobre A.

Capítulo

9

Funções ou aplicações

O conceito de função é um dos mais importantes da matemática de modo que toda vez que temos dois conjuntos e algum tipo de associação entre eles, que faça corresponder a todo elemento do primeiro conjunto um único elemento do segundo, obtemos uma função. O uso de funções pode ser encontrado em diversos fatos do nosso dia a dia. Por exemplo, na tabela de preços de uma fábrica, onde a cada produto corresponde um determinado preço; o valor pago numa conta da mensalidade escolar, que depende do valor associado a cada mês, enfim, existem diversos exemplos.

Deste modo, neste capítulo, apresentamos o conceito de uma função (também conhecida com uma aplicação), funções injetoras, sobrejetoras e bijetoras, imagem direta e imagem inversa, aplicações monótonas, e finalmente, apresentamos as noções e propriedades dos conjuntos equipotentes e dos conjuntos enumeráveis.

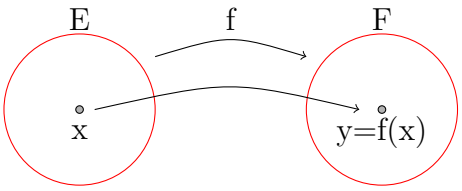
9.1 Aplicações - funções

O conceito de função, assim como o de conjuntos, é essecial para todas as áreas da Matemática, onde esses dois conceitos são sempre a parte central para desenvolvimento de estudos nas áreas da Matemática. Assim, consideramos E e F dois conjuntos não vazios.

Definição 9.1.1. *Uma relação f de E em F é uma aplicação (ou função) de E em F se para todo $x \in E$, existe $!y \in F$ tal que xfy, ou seja, $xfy \iff (x,y) \in f$, para um único $y \in F$. Neste caso, indica-se tal fato por $f : E \to F$, e se xfy, então escreve-se $y = f(x)$ e lê-se y é a imagem de x por f.*

A função f também pode ser representada pelo conjunto $\{(x, f(x)) : x \in E\}$. O diagrama

de Veen de uma função $f : E \to F$ é representado por:



Exemplo 9.1.1. *Se $E = \{a, b, c, d\}$ e $F = \{r, s, t, u, v\}$ e $f(c) = r$, $f(b) = s$, $f(a) = t$ e $f(d) = t$, então f é uma aplicação.*

Exemplo 9.1.2. *Se $E = \{a, b, c, \}$ e $F = \{r, s, t, u\}$ e $f(a) = r$ e $f(b) = s$, então f não é uma aplicação.*

Exemplo 9.1.3. *Se $E = \{a, b, c\}$ e $F = \{r, s, t, u, v\}$ e $f(a) = r$, $f(b) = s$, $f(a) = t$ e $f(d) = u$, então f não é uma aplicação.*

Definição 9.1.2. *Sejam $f : E \to F$ e $g : E \to F$ duas funções.*

1. *A função f é igual a função g, ou seja, as funções f e g são iguais, se $f(x) = g(x)$, para todo $x \in E$, ou seja, $f = g \iff f(x) = g(x)$, para todo $x \in E$.*
2. *O conjunto $D(f) = \{x \in E : \text{ existe } y \in F \text{ tal que } f(x) = y\}$ é definido como o domínio de uma função f.*
3. *O conjunto $Im(f) = \{y \in F : \text{ existe } x \in E \text{ tal que } f(x) = y\}$ é definido como a imagem de uma função f.*
4. *O contra-domínio de f é definido por $Cd(f) = F$.*

Exemplo 9.1.4. *Sejam $E = \{a, b, c, d\}$, $F = \{r, s, t, u, v\}$ e $f : E \to F$ uma aplicação definida por $f(c) = r$, $f(b) = s$, $f(a) = t$ e $f(d) = t$. Assim, $D(f) = \{a, b, c, d\}$, $Im(f) = \{r, s, t\}$ e $Cd(f) = \{r, s, t, u, v\}$.*

Exemplo 9.1.5. *Se $f : \mathbb{R} \to \mathbb{R}$ é uma função definida por $f(x) = x^2$, para todo $x \in \mathbb{R}$, então $D(f) = \mathbb{R}$, $Im(f) = \mathbb{R}_+$ e $Cd(f) = \mathbb{R}$.*

Definição 9.1.3. *Seja $X \subset E$, com $X \neq \emptyset$. A aplicação $i : X \to E$ tal que $f(x) = x$, para todo $x \in X$, é chamada aplicação inclusão de X em E. No caso de $X = E$, tem-se uma aplicação de E em E que é chamada aplicação idêntica de E.*

Exemplo 9.1.6. *Sejam $E = \{a, b, c, d, e\}$ e $X = \{b, c, d\}$. Neste caso, a aplicação inclusão $i : X \to E$ é dada por $i(b) = b$, $i(c) = c$ e $i(d) = d$. Agora, a aplicação idêntica de E é dada por $i(a) = a$, $i(b) = b$, $i(c) = c$, $i(d) = d$ e $i(e) = e$.*

Definição 9.1.4. *Sejam $f : E \to F$ uma aplicação e $A \subset E$, com $A \neq \emptyset$. A restrição de f ao conjunto A é a aplicação $f_A : A \to F$ definida por $(f_A)(x) = f(x)$, para todo $x \in A$.*

Exemplo 9.1.7. *Sejam $E = \{a, b, c, d, e\}$, $F = \{r, s, t, u, v\}$ e $f : E \to F$ definida por $f(a) = s$, $f(b) = u$, $f(c) = t$ e $f(d) = u$. Se $A = \{c, d\}$, então $f_A : A \to F$ é dada por $f(c) = t$ e $f(d) = u$.*

Exemplo 9.1.8. *Seja $f : \mathbb{Z} \to \mathbb{Z}$, onde $f = \{(x, x^2) : x \in \mathbb{Z}\}$. Se $A = \mathbb{N}$, então a restrição de f a $\mathbb{N}$ é dada por $f_{\mathbb{N}} = \{(x, x^2) : x \in \mathbb{N}\}$.*

9.1.1 Funções bijetoras

Sejam E, F, G e H conjuntos não vazios.

Definição 9.1.5. *Seja $f : E \to F$ uma aplicação. A aplicação f é chamada injetora sempre que $x_1 \neq x_2$ implicar que $f(x_1) \neq f(x_2)$, para todo $x_1, x_2 \in E$, ou seja, sempre que $f(x_1) = f(x_2)$ implicar que $x_1 = x_2$, para todo $x_1, x_2 \in E$.*

Exemplo 9.1.9. *Sejam $E = \{a, b, c\}$ e $F = \{r, s, t, u\}$. A função $f : E \to F$ definida por $f(a) = s$, $f(b) = t$ e $f(c) = u$ é injetora. Agora, se $f : E \to F$ é definida por $f(a) = r$, $f(b) = u$ e $f(c) = r$, então f não é injetora.*

Exemplo 9.1.10. *A função $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = 2x + 5$, para todo $x \in \mathbb{R}$ é injetora, uma vez que se $f(x_1) = f(x_2)$, então $x_1 = x_2$. De modo análogo, a função $f : \mathbb{R} - \{0\} \to \mathbb{R}$ definida por $f(x) = \frac{x+1}{x}$, para todo $x \in \mathbb{R} - \{0\}$, é injetora.*

Definição 9.1.6. *Seja $f : E \to F$ uma função. Dizem que f é uma função sobrejetora se $Im(f) = F$, ou seja, para todo $y \in F$, existe $x \in E$ tal que $f(x) = y$.*

Exemplo 9.1.11. *Sejam $E = \{a, b, c, d\}$ e $F = \{r, s, t\}$. A função $f : E \to F$ definida por $f(a) = s$, $f(b) = t$, $f(c) = r$ e $f(d) = s$ é sobrejetora. Agora, se $f : E \to F$ é definida por $f(a) = r$, $f(b) = r$ e $f(c) = t$, então f não é sobrejetora.*

Definição 9.1.7. *Uma função $f : E \to F$ chamada de função bijetora se f é injetora e sobrejetora. Se f é bijetora, os conjuntos E e F são chamados equipotentes, ou seja, possuem a mesma cardinalidade.*

Exemplo 9.1.12. *A função $f : E \to F$, onde $E = \{a, b, c\}$ e $F = \{r, s, t\}$, definida por $f(a) = s$, $f(b) = r$ e $f(c) = t$, é bijetora, e neste caso, os conjuntos E e F são equipotentes.*

Exemplo 9.1.13. *Os conjuntos $\mathbb{N}$ e $\mathbb{N} - \{0\}$ são equipotentes, uma vez que a função $f : \mathbb{N} \to \mathbb{N} - \{0\}$ definida por $f(n) = n + 1$, para todo $n \in \mathbb{N}$, é bijetora. Também, os conjuntos $\mathbb{N}$ e $A = \{20, 21, 22, \cdots\}$ são equipotentes, uma vez que a função $f : \mathbb{N} \to A$ definida por $f(n) = n + 20$, para todo $n \in \mathbb{N}$, é bijetora.*

Definição 9.1.8. *Sejam E, F e G conjuntos não vazios, e sejam $f : E \to F$ e $g : F \to G$ funções. A composta de f e g é a aplicação $g \circ f : E \to G$ definida por $(g \circ f)(x) = g(f(x))$, para todo $x \in E$.*

Observe que para que exista a composta $g \circ f$, devemos ter que $Im(f) \subseteq D(g)$.

Exemplo 9.1.14. *Sejam $f : \mathbb{R} \to \mathbb{R}$ uma função, onde $f(x) = x + 1$, para todo $x \in \mathbb{R}$, e $g : \mathbb{R} \to \mathbb{R}_+$ uma função, onde $g(x) = x^2 + 1$, para todo $x \in \mathbb{R}$. Assim, $g \circ f : \mathbb{R} \to \mathbb{R}_+$ é dada por $(g \circ f)(x) = g(f(x)) = g(x + 1) = (x + 1)^2 + 1 = x^2 + 2x + 2$, para todo $x \in \mathbb{R}$. Também, $f \circ g : \mathbb{R}_+ \to \mathbb{R}$ e é definida por $(f \circ g)(x) = f(g(x)) = f(x^2 + 1) = (x^2 + 2) + 1 = x^2 + 2$, para todo $x \in \mathbb{R}_+$.*

Exemplo 9.1.15. *Sejam $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ uma função definida por $f(x, y) = (2x, x - y)$, para todo $(x, y) \in \mathbb{R} \times \mathbb{R}$, e $g : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ uma função definida por $f(x, y) = x + y$, para todo $(x, y) \in \mathbb{R} \times \mathbb{R}$. Assim, $g \circ f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ é definida por $(g \circ f)(x, y) = g(f(x, y)) = g(2x, x - y) = 2x + x - y = 3x - y$, para todo $(x, y) \in \mathbb{R} \times \mathbb{R}$. Neste caso, como $Im(g) \nsubseteq D(f)$, segue que não existe a $f \circ g$.*

Proposição 9.1.1. *Sejam E, F e G conjuntos não vazios, $f : E \to F$ e $g : F \to G$ funções.*

1. *Se f e g são injetoras, então $g \circ f$ é injetora.*
2. *Se f e g são sobrejetoras, então $g \circ f$ sobrejetora.*

Demonstração. Para (1), se $(g \circ f)(x_1) = (g \circ f)(x_2)$, com $x_1, x_2 \in E$, então $g(f(x_1)) = g(f(x_2))$. Como g é injetora, segue que $f(x_1) = f(x_2)$. Finalmente, como f é injetora, segue que $x_1 = x_2$, ou seja, $g \circ f$ é injetora. Para (2), seja $z \in G$. Como g é sobrejetora, segue que existe $y \in F$ tal que $g(y) = z$. Agora, como f é sobrejetora, segue que existe $x \in E$ tal que $f(x) = y$. Assim, $(g \circ f)(x) = g(f(x)) = f(y) = z$, e portanto, $g \circ f$ é sobrejetora. □

Corolário 9.1.1. *Se f e g são bijetoras, então $g \circ f$ é bijetora.*

Proposição 9.1.2. *Sejam E, F, G e H conjuntos não vazios. Se $f : E \to F$, $g : F \to G$ e $h : G \to H$ são funções, então $h \circ (g \circ f) = (h \circ g) \circ f$.*

Demonstração. Se $x \in E$, então $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x)$. □

Exemplo 9.1.16. *Sejam $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x^2$, para todo $x \in \mathbb{R}$, $g : \mathbb{R} \to \mathbb{R}_+$ definida por $g(x) = sen(x)$, para todo $x \in \mathbb{R}$, e $h : \mathbb{R} \to \mathbb{R}_+$ definida por $h(x) = 2^x$, para todo $x \in \mathbb{R}$. Assim, $h \circ g \circ f : \mathbb{R} \to \mathbb{R}_+$ e é definida por $(h \circ g \circ h)(x) = h(g(f(x))) = h(g(x^2)) = h(sen(x^2)) = 2^{sen(x^2)}$, para todo $x \in \mathbb{R}$.*

Teorema 9.1.1. *Seja $f : E \to F$ uma função, onde E e F são conjuntos não vazios. A relação f^{-1} de F em E é uma função se, e somente se, f é bijetora.*

Demonstração. Suponhamos que f^{-1} é uma função. Se $f(x_1) = f(x_2) = y$, com $x_1, x_2 \in E$, então $x_1 f y$ e $x_2 f y$. Assim, $y f^{-1} x_1$ e $y f^{-1} x_2$. Como f^{-1} é uma função, segue que $x_1 = x_2$, ou seja, f é injetora. Para a sobrejetora, se $b \in F$, então $f^{-1}(b) = a \in E$. Assim, $b f^{-1} a$. Portanto, $a f b$ e $f(a) = b$, ou seja, f é sobrejetora. Portanto, f é bijetora. Reciprocamente, seja $y \in F$. Como f é sobrejetora, segue que existe $x \in E$ tal que $f(x) = y$. Assim, $y f^{-1} x$. Agora, se $x_1, x_2 \in E$ são tais que $y f^{-1} x_1$ e $y f^{-1} x_2$, então, $x_1 f y$ e $x_2 f y$, ou seja, $f(x_1) = f(x_2) = y$. Com f é injetora, segue que $x_1 = x_2$. Portanto, f^{-1} é uma função. □

Corolário 9.1.2. *Se f é bijetora, então $f^{-1} \circ f = id_E$ e $f \circ f^{-1} = id_F$.*

Demonstração. Se $x \in E$, então $f(x) = y \in F$. Assim, $(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(y) = x = id_E(x)$. Portanto, $f^{-1} \circ f = id_E$. Agora, se $y \in F$, então $f^{-1}(y) = x \in E$. Assim, $(f \circ f^{-1})(y) = f(f^{-1}(y)) = f(x) = y = id_F(y)$. Portanto, $f \circ f^{-1} = id_F$. □

Corolário 9.1.3. *Se f é bijetora, então f^{-1} é bijetora.*

Demonstração. Se $f^{-1}(y_1) = f^{-1}(y_2)$, com $y_1, y_2 \in F$, então $f(f^{-1}(y_1)) = f(f^{-1}(y_2))$, ou seja, $(f \circ f^{-1})(y_1) = (f \circ f^{-1})(y_2)$. Assim, $id_F(y_1) = id_F(y_2)$, ou seja, $y_1 = y_2$. Portanto, f^{-1} é injetora. Para a sobrejetora, se $x \in E$, então $id_E(x) = x$, ou seja, $(f^{-1} \circ f)(x) = x$. Assim, $f^{-1}(f(x)) = x$, ou seja, f^{-1} é sobrejetora. Portanto, f^{-1} é bijetora. □

Teorema 9.1.2. *Se existe $g : F \to E$ tal que $g \circ f = id_E$ e $f \circ g = id_F$, então f e g são bijetoras, $g = f^{-1}$ e $f = g^{-1}$.*

Demonstração. Primeiro, vamos provar que f é bijetora. Para a injetora, se $f(x_1) = f(x_2)$, com $x_1, x_2 \in E$, então $g(f(x_1)) = g(f(x_2))$, ou seja, $(g \circ f)(x_1) = (g \circ f)(x_2)$. Como $g \circ f = id_E$ e $f \circ g = id_F$, segue que $x_1 = x_2$, ou seja, f é injetora. Para a sobrejetora, se $b \in F$, então $id_F(b) = b$. Assim, $(f \circ g)(b) = b$, isto é, $f(g(b)) = b$. Como $g(b) \in E$, segue que f é sobrejetora. Portanto, f é bijetora. Agora, vamos provar que g é bijetora. Para a injetora, se $g(y_1) = g(y_2)$, com $y_1, y_2 \in F$, então $f(g(y_1)) = f(g(y_2))$, ou seja, $y_1 = (f \circ g)(y_1) = (f \circ g)(y_2) = y_2$. Portanto, g é injetora. Agora, se $a \in E$, então $id_E(a) = a$. Assim, $(g \circ f)(a) = g(f(a)) = a$. Como $f(a) \in F$, segue que g é sobrejetora. Portanto, g é bijetora. Agora, vamos mostrar que $g = f^{-1}$. Se $(y, x) \in g$, então $g(y) = x$. Aplicando f, segue que $f(g(y)) = f(x)$. Como $f \circ g = id_F$, segue que $f(x) = y$. Assim, $(x, y) \in f$, e desse modo, $(y, x) \in f^{-1}$. Portanto, $g \subseteq f^{-1}$. Para a outra inclusão, se $(y, x) \in f^{-1}$, então $(x, y) \in f$, ou seja, $f(x) = y$. Aplicando g, segue que $g(y) = g(f(x)) = (g \circ f)(x) = id_E(x) = x$. Assim, $(y, x) \in g$, e desse modo, $f^{-1} \subseteq g$. Portanto, $g = f^{-1}$. Agora, mostramos que $f = g^{-1}$. Assim, se $(x, y) \in f$, então $y = f(x)$. Aplicando g, segue que $g(y) = g(f(x)) = (g \circ f)(x) = id_E(x) = x$. Assim, $(y, x) \in g$, e desse modo, $(x, y) \in g^{-1}$. Portanto, $f \subseteq g^{-1}$. Agora, se $(y, x) \in g^{-1}$, então $(x, y) \in g$, ou seja, $g(x) = y$. Aplicando f, segue que $f(y) = f(g(x)) = (f \circ g)(x) = id_F(x) = x$. Assim, $(y, x) \in f$, e deste modo, $g^{-1} \subseteq f$. Portanto, $f = g^{-1}$. □

9.1.2 Imagem direta e imagem inversa

Sejam E e F conjuntos não vazios e $f : E \to F$ uma função.

Definição 9.1.9. *A imagem direta de um subconjunto $A \subseteq E$ através da função f, indicada por $f(A)$, é definida por $f(A) = \{f(x) : x \in A\}$. Se $A = E$, então $f(E) = Im(f)$.*

Exemplo 9.1.17. *Sejam $E = \{a, b, c, d, e\}$, $F = \{r, s, u, v\}$ e $f : E \to F$ uma função definida por $f(a) = r$, $f(b) = s$, $f(c) = s$, $f(d) = u$ e $f(e) = v$. Se $A = \{b, c, d\}$, então $f(A) = \{s, u\}$.*

Exemplo 9.1.18. *Seja $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = -1$, para todo $x < 1$, e $f(x) = x + 1$, para todo $x \geq 1$. Se $A = [-2, 1[$, então $f(A) = \{-1, 2\}$.*

Definição 9.1.10. *A imagem inversa de um subconjunto $B \subseteq F$ através da função f, indicada por $f^{-1}(B)$, é definida por $f^{-1}(B) = \{x \in E : f(x) \in B\}$. Se $B = F$, então $f^{-1}(F) = E$.*

Exemplo 9.1.19. *Sejam $E = \{a, b, c, d, e\}$, $F = \{r, s, u, v\}$ e $f : E \to F$ uma função definida por $f(a) = s$, $f(b) = r$, $f(c) = u$, $f(d) = r$ e $f(e) = r$. Se $B = \{r, s, u\}$, então $f^{-1}(B) = \{a, b, c, d, e\}$.*

9.1.3 Aplicações monótonas

Sejam E e F conjuntos não vazios e $f : E \to F$ uma função, onde E e F são conjuntos parcialmente ordenados com uma relação de ordem que indicamos por R.

Definição 9.1.11. *Seja $f : E \to F$ uma função.*

1. *A função f é chamada uma função crescente se xRy implicar que $f(x)Rf(y)$.*
2. *A função f é chamada uma função decrescente se xRy implicar que $f(y)Rf(x)$.*
3. *A função f é uma função monótona se f é uma função crescente ou decrescente.*
4. *A função f é chamada uma função estritamente crescente se xRy, com $x \neq y$, implicar que $f(x)Rf(y)$, com $f(x) \neq f(y)$.*
5. *A função f é chamada uma função estritamente decrescente se xRy, com $x \neq y$, implicar que $f(y)Rf(x)$, com $f(x) \neq f(y)$.*

Exemplo 9.1.20. *A função $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x$ é estritamente crescente.*

Exemplo 9.1.21. *A função $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = -x$ é estritamente decrescente.*

9.1.4 Exercícios

1. Determine todas as funções de $E = \{0, 1, 2\}$ em $F = \{3, 4\}$.
2. Determine todas as funções injetoras de $E = \{1, 2\}$ em $F = \{3, 4, 5\}$.
3. Determine todas as funções sobrejetoras de $E = \{1, 2, 3\}$ em $F = \{4, 5\}$.
4. Verifique se as funções $f : \mathbb{R} \to \mathbb{R}$ definidas por $f(x) = x^3$, $f(x) = x^2 - 5x + 6$, $f(x) = 2^x$, $f(x) =\mid sen(x) \mid$, $f(x) = x+ \mid x \mid$ e $f(x) = x + 3$, onde $x \in \mathbb{R}$, são bijetoras.
5. Determine uma função $f : A \to B$, onde
   (a) $A = \mathbb{R}$, $B \subseteq \mathbb{R}$, f é injetora e não é sobrejetora.
   (b) $A \subseteq \mathbb{R}$, $B = \mathbb{R}$, f é injetora e não é sobrejetora.
   (c) $A = \mathbb{R}$, $B \subseteq \mathbb{R}$, f é sobrejetora e não é injetora.

(d) $A \subseteq \mathbb{R}$, $B = \mathbb{R}$, f é sobrejetora e não é injetora.

6. Sejam $A = \{1, 2, 3\}$, $B = \{4, 5, 6, 7\}$ e $C = \{8, 9, 0\}$. Sejam as funções $f : A \to B$ e $g : B \to C$ definidas por $f() = 4$, $f(2) = 5$, $f(3) = 6$, $g(4) = 8$, $g(5) = 8$, $g(6) = 9$ e $g(7) = 0$. Verifique se existem $f \circ g$ e $g \circ f$ e se são injetoras e sobrejetoras.

7. Mostre que a equipotência é uma relação de equivalência.

8. Mostre que a função $f : \mathbb{Z} \to \mathbb{N}$ definida por $f(n) = \begin{cases} 2n \text{ se } n \geq 0 \\ -2n - 1 \text{ se } n < 0 \end{cases}$ é uma bijeção.

9. Mostre que a função $f : [a, b] \to [0, 1]$ definida por $f(x) = \frac{x-a}{b-a}$ é uma bijeção.

10. Mostre que a função $f : (-1, 1) \to \mathbb{R}$ definida por $f(x) = \frac{x}{1+|x|}$ é uma bijeção e que $f^{-1} : \mathbb{R} \to (-1, 1)$ e definida por $f(x) = \frac{x}{1-|x|}$.

11. Sejam $f, g, h : \mathbb{R} \to \mathbb{R}$ definidas por $f(x) = x - 1$, $g(x) = x^2 + 2$ e $h(x) = x + 1$, onde $x \in \mathbb{R}$. Determine $f \circ g$, $f \circ h$, $g \circ h$, $g \circ f$, $h \circ f$, $h \circ g$, $(f \circ g) \circ h$ e $f \circ (g \circ h)$.

12. Sejam as funções $f, g : \mathbb{R} \to \mathbb{R}$ definidas por $f(x) = x^3 + 1$ e $g(x) = x^2 + 1$, onde $x \in \mathbb{R}$. Determine $f \circ f$, $g \circ g$, $f \circ g$ e $g \circ f$.

13. Determine $f \circ f$, $g \circ g$, $f \circ g$ e $g \circ f$, onde $f, g : \mathbb{R} \to \mathbb{R}$ são definidas por $f(x) = \begin{cases} x^2 \text{ se } x < 0 \\ 3x \text{ se } x \geq 0 \end{cases}$ e $g(x) = \begin{cases} 1 - x \text{ se } x < 1 \\ 1 + x \text{ se} x \geq 1. \end{cases}$

14. Determine $f \circ f$, $g \circ g$, $f \circ g$ e $g \circ f$, onde $f, g : \mathbb{R} \to \mathbb{R}$ são definidas por $f(x) = \begin{cases} x^2 + 1 \text{ se } x < 0 \\ 2x + 1 \text{ se } x \geq 0 \end{cases}$ e $g(x) = \begin{cases} 3x \text{ se } x < 1 \\ 7x + 1 \text{ se } 1 \leq x \leq 5 \\ 2 + x \text{ se } x > 5. \end{cases}$

15. Seja a função $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = \begin{cases} 2x + 5 \text{ se } x < -1 \\ x^2 - 1 \text{ se } -1 \leq x \leq 1 \\ 5x \text{ se } x > 1. \end{cases}$
Esboce o gráfico e verifique se f é injetora e sobrejetora.

16. Seja a função $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = cos(x)$, onde $x \in \mathbb{R}$. Determine $f([0, \pi/2])$, $f([0, \pi])$, $f(\mathbb{R})$, $f^{-1}(1/2)$, $f^{-1}([1/2, 1])$ e $f^{-1}(\mathbb{R})$.

17. Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definida por$f(x, y) = mdc(2, y)$. Verifique se f é injetora e sobrejetora.

18. Quais das funções abaixo são iguais.

(a) $f(x) = \frac{x^2-4x+3}{x-3}$ e $g(x) = x - 1$, com $x \in \mathbb{R} - \{3\}$.

(b) $f(x) = 1$ e $g(x) = x^4$, onde $x \in \{1, -1, i, -i\}$.

(c) $f(x) = x^3$, onde $x \in \mathbb{R}$, e $g(y) = y^3$, onde $y \in \mathbb{R}$.

19. Seja $f : \mathbb{R} \to \mathbb{R}$ uma função definida por $f(x) = \begin{cases} x + 1 \text{ se } x \leq 0 \\ 1 - 2x \text{ se } x > 0. \end{cases}$ Determine $f \circ f$.

20. Sejam f e g duas funções definidas por $f(x) = \begin{cases} x+1, \text{ se } x \geq 0 \\ -x+1, \text{ se } x < 0 \end{cases}$ e $g(x) = 3x - 2$.

    (a) Faça o gráfico da f e g.

    (b) Determine $D(f)$, $Im(f)$, $D(g)$ e $Im(g)$.

    (c) Verifique se f e g são injetoras e sobrejetoras.

    (d) Determine f^{-1} e g^{-1}.

    (e) Determine $f \circ g$, $g \circ f$, $D(f \circ g)$, $D(g \circ f)$, $Im(f \circ g)$ e $Im(g \circ f)$.

    (f) Faça o gráfico de $f \circ g$ e $g \circ f$.

    (g) Determine $f \circ f$, $D(f \circ f)$, $Im(f \circ f)$ e seu gráfico.

    (h) Determine $g \circ g$, $D(g \circ g)$, $Im(g \circ g)$ e seu gráfico.

21. Mostre que a função $f : \mathbb{Z}^2 \to \mathbb{Z}^2$ definida por $f(x, y) = (x+3, 2-y)$ é bijetora e determine f^{-1}.

22. Seja $f : \mathbb{R}^* \to \mathbb{R} - \{1\}$ definida por $f(x) = (x+2)/x$. Mostre que f é bijetora e determine f^{-1}.

23. Mostre que as funções $f :]-1, 1[\to \mathbb{R}$ e $g : \mathbb{R} \to]-1, 1[$ definidas por $f(x) = \frac{x}{1-|x|}$, onde $x \in]-1, 1[$, e $g(x) = \frac{x}{1+|x|}$, onde $x \in \mathbb{R}$, são bijetoras e determine $g \circ f$ e $f \circ g$.

24. Seja $f : \mathbb{R} \to \mathbb{R}$ uma função definida por $f(x) = ax^n$, onde $a \in \mathbb{R}$ e $n \in \mathbb{N}$. Determine a e n tal que $(f \circ f)(x) = 3x^4$.

25. Sejam as funções $f, g : \mathbb{R} \to \mathbb{R}$ definidas por $f(x) = \begin{cases} x^2 \text{ se } x \geq 0 \\ 1 + x \text{ se } x < 0 \end{cases}$ e $g(x) = 3x + 1$, onde $x \in \mathbb{R}$. Determine $g \circ f$ e $f \circ g$.

26. Sejam as funções $f : (-1, 1) \to \mathbb{R}$ definida por $f(x) = \frac{x}{1-|x|}$ e $g : \mathbb{R} \to (-1, 1)$ definida por $g(x) = \frac{x}{1+|x|}$. Mostre que f e g são bijetoras e calcule $f \circ g$ e $g \circ f$.

27. Sejam $f : E \to F$ uma função, $A \subseteq E$ e $B \subseteq F$. Mostre que:

    (a) $f(E) - f(A) \subseteq f(E - A)$.

    (b) $f^{-1}(F - B) = E - f^{-1}(B)$.

    (c) $f(A \cap f^{-1}(B)) = f(A) \cap B$.

28. Seja $f : E \to F$ uma função. Mostre que:

    (a) $A \neq \emptyset$ se, e somente se, $f(A) \neq \emptyset$.

    (b) Se $A \subseteq B \subseteq E$, então $f(A) \subseteq f(B)$.

    (c) $f(A \cup B) = f(A) \cup f(B)$.

    (d) $f(A \cap B) \subseteq f(A) \cap f(B)$.

(e) $A \subseteq f^{-1}(f(A))$ e $f(f^{-1}(B)) \subseteq B$.

(f) Mostre que f é injetora se, e somente se, $f(A \cap B) = f(A) \cap f(B)$.

(g) f é sobretora se, e somente se, $f(A^c) = (f(A))^c$.

29. Seja $f : E \to F$ uma função. Mostre que:

(a) Se $A \subseteq B \subseteq F$, mostre que $f^{-1}(A) \subseteq f^{-1}(B)$.

(b) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

(c) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$. Determine $f^{-1}(A^c) = (f^{-1}(A))^c$.

30. Mostre que a função $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = ax + b$, com $a \neq 0$, é bijetora e determine f^{-1}.

31. Seja $F : \mathbb{R}^2 \to \mathbb{R}$ uma função definida por $f(x, y) = xy$.

(a) Verifique se f é injetora e sobrejetora.

(b) Determine $f^{-1}(\{0\})$ e $f([0, 1] \times [0, 1])$.

32. Sejam f e g funções.

(a) Se f e g são injetoras, mostre que $f \circ g$ é injetora.

(b) Se f e g são sobrejetoras, mostre que $f \circ g$ é sobrejetora.

(c) Se $g \circ f$ é injetora, mostre que f é injetora.

(d) Se $f \circ g$ é sobrejetora, mostre que f é sobrejetora.

33. Verifique se a função $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ definida por $f(x, y) = (2x + 3, 4y + 5)$ é injetora e sobrejetora.

34. Mostre que a função $f : \mathbb{R} - \{d/c\} \to \mathbb{R} - \{a/c\}$ definida por $f(x) = \frac{ax-b}{cx-d}$, onde $a, b, c, d \in \mathbb{R}$, $c \neq 0$ e $ad - bc \neq 0$, é bijetora e determine f^{-1}.

35. Seja a função $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = \begin{cases} x^2 & \text{se } x \leq 0 \\ \sqrt[3]{x} & \text{se } x > 0 \end{cases}$. Determinar $f([-1, 8])$, $f(\mathbb{R}_+)$, $f(\mathbb{R}_-)$, $f^{-1}(\{1, 16\})$, $f^{-1}([-1, 16])$ e $f^{-1}(\mathbb{R}_+^*)$.

36. Das funções de $\mathbb{R}$ em $\mathbb{R}$ abaixo, quais são injetoras e sobrejetoras: $f(x) = x^3 - 1$, $f(x) = x^2 - 5x + 6$, $f(x) = 2^x$, $f(x) = |sen(x)|$ e $f(x) = x + |x|$.

37. Sejam as funções reais $f(x) = 2x + 7$ e $(f \circ g)(x) = 4x^2 - 2x + 3$. Determinar g.

38. Seja $f : \mathbb{R} \to \mathbb{R}$ uma função definida por $f(x) =\mid x \mid$. Determine $f(\mathbb{R})$, $f([-1, 2])$, $f^{-1}([2, 5])$ e $f^{-1}(\{-7\})$.

39. Determine $D(f)$, $Im(f)$ e faça os gráficos das funções:

(a) $f(x) = \begin{cases} 3x - 2 & \text{se } x < 1 \\ x^2 & \text{se } x \geq 1 \end{cases}$

(b) $g(x) = \dfrac{x^2 - 9}{x - 3}$.

40. Determine $f \circ f$, $g \circ g$, $f \circ g$ e $g \circ f$ das seguintes funções

$$f(x) = \sqrt{3x - 4} \quad \text{e} \quad g(x) = \begin{cases} x^2 - 4 & \text{se } x < 3 \\ 2x - 1 & \text{se } x \geq 3. \end{cases}$$

9.2 Conjuntos equipotentes e enumeráveis

O infinito sempre assombrou os matemáticos e filósofos, estando relacionada aos maiores paradoxos e crises nos fundamentos da matemática, como é o caso dos famosos paradoxos de Zeno e de Eléia, que se baseiam em interpretações tortuosas do conceito de infinitude para provar a não existêencia de movimento.

No desenvolvimento da teoria dos conjuntos, o conceito de infinito desepenha um papel fundamental, sendo responsável por uma dos maiores problemas filosóficas na história da matemática. Como efeito desse problema, tivemos matemáticos e filosóficos sendo destruídos, novos questionamentos surgindo, divergências na própria concepção de verdade matemática, novas propostas de formalização da disciplina. Enfim, como aconteceu com as grandezas incomensuráveis e a história do quinto postulado de Euclides (esses dois também estão diretamente relacionados ao conceito de infinitude) os paradoxos da teoria dos conjuntos contribuíram enormemente para o enriquecimento do pensamento matemático.

Definição 9.2.1. *Dois conjuntos A e B são chamados equipotentes se existe uma bijeção f entre A e B.*

Sejam A, B e C conjuntos. A relação de equipotência é uma relação de equivalência, ou seja,

1. A é equipotente a A.
2. Se A é equipotente a B, então B é equipotente a A.
3. Se A é equipotente a B e B é equipotente a C, então A é equipotente a C.

Exemplo 9.2.1. *Os intervalos $[0, 1]$ e $[a, b]$, com $a < b$, são equipotentes, uma vez que a aplicação $f : [0, 1] \to [a, b]$ definida por $f(x) = (b - a)x + a$ é uma bijeção.*

Definição 9.2.2. *Seja A um conjunto.*

1. *O conjunto A é dito finito se é vazio ou se existe $n \in \mathbb{N}$ tal que A é equipotente a $\{1, 2, , 3, \ldots, n\}$. Caso contrário, A é dito infinito.*
2. *A cardinalidade do conjunto A é o número de elementos do conjunto A que pode ser finito ou infinito.*

O conjunto dos números naturais, o conjunto dos pontos de uma reta, o conjunto das retas em um plano, o conjunto das fraçõe e o conjunto dos números reais são exemplos de conjuntos infinitos. Observe que todos esses conjuntos são fomados por conceitos abstratos, e não por objetos concretos. Portanto, a idéia de infinitude não era fácil de assimilar.

Pergunta: será que a ordem que utilizamos para contar as coisas não afeta o resultado? Ninguém havia pensado nessa questão em conjuntos infinitos? Afinal, um conjunto infinito é infinito e não tem como contar os elementos de um conjunto infinito. Porém, algumas mentes mais aguçadas ousaram aprofundar-se nas questões filosóficas da infinitude. O cientista italiano Galileu Galilei (1564-1642) decidiu usar a noção de funções bijetoras para comparar conjuntos infinitos, chegando em um resultado bem curioso. Ele considerou a função que associa, a cada número natural, o seu dobro, conforme o seguinte diagrama:

$$\begin{array}{ccc} 0 & \longleftrightarrow & 0 \\ 1 & \longleftrightarrow & 2 \\ 2 & \longleftrightarrow & 4 \\ & \cdots & \end{array}$$

Com isso, Galilei mostrou que o conjunto dos números naturais tem a mesma cardinalidade que o conjunto dos nḿeros pares. Na época, isso parecia contradizer o axioma de Euclides que dizia que "o todo é sempre maior que a parte". O conjunto dos números pares é apenas uma parte do conjunto de todos os números naturais, e ainda assim, ambos os conjuntos têm a mesma cardinalidade, se utilizarmos essa noção de bijeções. Observe, que isso somente acontece com conjuntos infinitos. Em um conjunto finito, se tirarmos um único elemento não conseguimos associar biunivocamente os elementos do conjunto reduzido com os do conjunto todo.

O hotel de Hilbert: O matemático alemão David Hilbert (1862-1943) apresentou um exemplo parecido. Se chegamos em um hotel e todos os quartos estão ocupados, então sabemos que não existe vaga nesse hotel, a menos que um quarto seja desocupado. Agora, imaginamos um hotel com infinitos quartos, sendo um quarto para cada número natural, e que todos os quartos estão ocupados. Chega um novo hóspede querendo se hospedar e o dono não quer desalojar nenhum hóspede, mas também não quer perde clientes. Como existem infinitos quartos, mesmo que todos estejam ocupados, é possível resolver o problema. Para isso, é suficiente passar cada hóspede para o próximo quarto. Assim, quem está hospedado no quarto 0 vai para o quarto 1, e do quarto 1 para o 2, e assim, por diante, sobrando o quarto 0 para o novo hóspedes.

O problema do dono do hotel parece se complicar quando chega um ônibus com uma infinidade de hóspedes, um hóspede para cada número natural. Neste caso, o dono passa cada hóspede de um quarto para outro cujo número é o dobro do primeiro. Sobra, assim, todos os números ímpares para colocar os novos hóspedes. E se chegarem infinitos ônibus, cada ônibus marcado por um número natural diferente e com infinitos passageiros cada um, onde cada passageiro também marcado por um número? Nesse caso, o dono do hotel poderá ainda hospedar todo mundo de forma que não fique nenhum quarto vazio. Para isso, é suficiente colocar o n-ésimo passageiro do m-ésimo ônibus no quarto $2n(m+1)$, onde supomos que o hotel esteja vazio.

Aparentemente o paradoxo criado por Galilei não causou tanto impacto na matemática e na filosofia, nem foi devidamente explorado durante alguns séculos. Foi somente no século XIX que o assunto foi novamente estudado pelo matemático alemão Georg Cantor (1845-1918). Dessa vez, o impacto transformou totalmente o rumo da matemática moderna e deu início á teoria dos conjuntos que é vista hoje.

Cantor não só criou um paradoxo ou uma discussão filosófica através dessa idéia de comparar tamanho de conjuntos infinitos: ele de fato resolveu um problema matemático usando esse conceito. Enquanto outros matemáticos tiveram uma grande dificuldade para provar que números π e e são transcendentes (isto é, não são raízes de equações polinomiais de coeficientes inteiros), Cantor provou, de maneira relativamente simples, que existem muitos números transcendentes, mesmo sem exibir um sequer.

Definição 9.2.3. *Um conjunto A é dito enumerável se A é equipotente a um subconjunto dos números naturais $\mathbb{N}$. Caso contrário, o conjunto A é chamado não enumerável.*

Pela Definição 9.2.3, segue que todo comjunto finito e todo subconjunto de $\mathbb{N}$ são enumeráveis, e portanto, $\mathbb{N}$ é um conjunto enumerável. Agora, se A é um conjunto enumerável e $f : A \to B$ é uma bijeção, então B é enumerável.

Exemplo 9.2.2. *O conjunto $2\mathbb{N}$ é enumerável, uma vez que a aplicação $f : \mathbb{N} \to 2\mathbb{N}$ definida por $f(n) = 2n$, onde $n \in \mathbb{N}$, é uma bijeção.*

Exemplo 9.2.3. *O conjunto dos numeros inteiros $\mathbb{Z}$ é enumerável, uma vez que a aplicação $f : \mathbb{N} \to \mathbb{Z}$ definida por*

$$f(n) = \begin{cases} \frac{n-1}{2} & \text{se } n \text{ é impar} \\ -\frac{n}{2} & \text{se } n \text{ é par} \end{cases}$$

é uma bijeção.

Proposição 9.2.1. *Se A é um conjunto infinito, então A possui um subconjunto infinito enumerável.*

Demonstração. Vamos definir uma função $f : \mathbb{N} \to A$. Como A é infinito, segue que existe um elemento $x_0 \in A$. Assim, definimos $f(0) = x_0$. Como A é infinito, segue que $A_1 = A - \{x_0\}$ é não vazio, ou seja, existe $x_1 \in A_1$. Assim, definimos $f(1) = x_1$. De modo análogo, se $A_2 = A - A_1$, definimos $f(2) = x_2$, onde $x_2 \in A_2$. Por recorrência, definimos $f(n) = x_n$, onde $x_n \in A - \{x_0, x_1, x_2, \ldots, x_{n-1}\}$. A função f é injetora, uma vez que se $m, n \in \mathbb{N}$, com $m \neq n$, então $f(m) \in \{f(1), f(2), \ldots, f(n-1)\}$ e $f(n) \notin \{f(1), f(2), \ldots, f(n-1)\}$, ou seja, $f(m) \neq f(n)$. Assim, $f : \mathbb{N} \to Im(f) \subseteq A$ é uma bijeção, e portanto, A possui um subconjunto infinito enumerável. □

Proposição 9.2.2. *Sejam $A \subseteq B$ conjuntos. Se B é enumerável, então A é enumerável.*

Demonstração. Como B é enumerável, segue que B é equipotente a um subconjunto de $\mathbb{N}$, ou seja, existe uma aplicação bijetora $f : B \to C$, onde $C \subseteq \mathbb{N}$. Assim, a restrição de f ao conjunto A é uma bijeção na imagem, ou seja, $f_A :\to Im(f_A)$ é uma bijeção. Como $Im(f_A) \subseteq C \subseteq \mathbb{N}$, segue que A é enumerável. □

Proposição 9.2.3. *Sejam A e B conjuntos e $f : A \to B$ uma aplicação.*

1. *Se f é injetiva e B for enumerável, então A é enumerável.*
2. *Se f é sobrejetiva e A for enumerável, então B é enumerável.*

Demonstração. Para (1), como $f : A \to Im(f) \subseteq B$ é uma bijeção, pela Proposição 9.2.2, segue que $Im(f)$ é enumerável, e portanto, A é enumerável. Para (2), como f é sobrejetora, segue que para cada $b \in B$ existe $a \in A$ tal que $f(a) = b$. Com isso, obtemos a aplicação $g : B \to A$ tal que $f(g(b)) = b$, para todo $b \in B$. Assim, g é injetora, e pelo item (1), segue que B é enumerável. □

Lema 9.2.1. *O conjunto $\mathbb{N} \times \mathbb{N}$ é enumerável.*

Demonstração. A função $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definida por $f(m, n) = 2^m 3^n$ é injetiva. Logo, $\mathbb{N} \times \mathbb{N} \to f(\mathbb{N} \times \mathbb{N}) \subseteq \mathbb{N}$ é uma bijeção. Portanto, $\mathbb{N} \times \mathbb{N}$ é enumerável. □

Proposição 9.2.4. *Sejam A e B conjuntos.*

1. *Se A e B são enumeráveis, então $A \times B$ é um conjunto enumerável.*
2. *Se $A \times B$ é enumerável, então A e B são enumeráveis.*

Demonstração. Para (1), como A e B são enumeráveis, segue que existem bijeções $f : A \to A_1$ e $g : B \to B_1$, onde A_1 e B_1 são subconjuntos de $\mathbb{N}$. Assim, aplicação $h : A \times B \to A_1 \times B_1$ definida por $h(a, b) = (f(a), g(b))$ é uma bijeção. Como $A_1 \times B_1 \subseteq \mathbb{N} \times \mathbb{N}$, segue que $A \times B$ é enumerável. Para (2), a aplicação $f : A \to A \times \{0\}$ definida por $f(a) = (a, 0)$, onde $a \in A$, ém bijeção e $A \times \{0\} \subset A \times B$. Como $A \times B$ é enumerável, pela Proposição 9.2.2, segue que A é enumerável. De modo análogo, B é enumerável. □

Pela Proposição 9.2.4, segue que para uma quantidade finita de conjuntos enumeráveis, o produto cartesiano ainda será enumerável, entretanto para o caso infinito isso não ocorre, ou seja, dados infinitos conjuntos enumeráveis, não necessariamente o produto cartesiano será enumerável.

Corolário 9.2.1. *O conjunto dos números racionais é enumerável.*

Demonstração. Seja $\mathbb{Z}^*$ o conjunto dos inteiros não nulos. Como $\mathbb{Z}^* \subseteq \mathbb{Z}$, segue que $\mathbb{Z}^*$ é enumerável. Assim, pela Proposição 9.2.4, segue que $\mathbb{Z}^* \times \mathbb{Z}$ é enumerável. Agora, a aplicação $f : \mathbb{Z}^* \times \mathbb{Z} \to \mathbb{Q}$ definida por $f(m, n) = \frac{m}{n}$ é sobrjetororа. Pela Proposição 9.2.3, segue que $\mathbb{Q}$ é enumerável. □

Corolário 9.2.2. *A união de uma família enumerável de conjuntos enumeráveis é enumerável.*

Demonstração. Sejam $A_1, A_2, \ldots$ uma família enumerável de conjuntos enumeráveis. Assim, existem funções sobrejetoras $f_i : \mathbb{N} \to A_i$, para todo i. Sejam $A = \cup_{i=1}^{\infty} A_i$ e $f : \mathbb{N} \times \mathbb{N} \to A$ definida por $f(m, n) = f_n(m)$. Como f é sobrejetora, segue que A é enumerável. □

Teorema 9.2.1. *O intervalo* $(0,1)$ *não é enumerável.*

Demonstração. Se $(0,1)$ for enumerável, então existe uma bijeção $f : \mathbb{N} \to (0,1)$. Assim, $f(i) = x_i$, para todo $i \in \mathbb{N}$, onde

$$\begin{aligned} x_1 &= 0, x_{11}x_{12}x_{13}\cdots \\ x_2 &= 0, x_{21}x_{22}x_{23}\cdots \\ x_3 &= 0, x_{31}x_{32}x_{33}\cdots \\ &\vdots \end{aligned}$$

Agora, seja $k \in (0,1)$ dado por $k = 0, k_1k_2k_3\ldots$, onde $k_i \neq x_{ii}$ para todo i. Desse modo, $k \in (0,1)$ e $k \neq x_i$, para todo i, o que é uma contradição. Portano, $(0,1)$ não é enumerável. □

Corolário 9.2.3. *O conjunto dos números reais* $\mathbb{R}$ *não é enumerável.*

Demonstração. Se $\mathbb{R}$ for enumumerável, então $(0,1)$ é enumerável, pois todo subconjunto de um conjunto enumerável é enumerável, o que é uma contradição. Portanto, $\mathbb{R}$ não é enumerável. □

Corolário 9.2.4. *O conjunto dos números irracionais não é enumerável.*

Demonstração. Se $\mathbb{R} - \mathbb{Q}$ for enumerável, segue que $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} - \mathbb{Q})$ é enumerável, o que é uma contradição. Portanto, o conjunto dos números irracionais não é enumerável. □

Definição 9.2.4. *Um número complexo* α *é chamado algébrico se existem inteiros* $a_o, a_1, \cdots, a_n$*, não todos nulos, tal que* $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$*. Caso, contrário,* α *é chamado transcendente.*

Lema 9.2.2. *O conjunto* $P_n(\mathbb{Z})$ *de todos os polinômios de coeficientes inteiros de grau máximo* n *é enumerável.*

Demonstração. A aplicação $f : \mathbb{Z}^{n+1} \to P_n(\mathbb{Z})$, definida por $f(a_o, a_1, \cdots, a_n) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, é bijetora. Portanto, $P_n(\mathbb{Z})$ é enumerável. □

Proposição 9.2.5. *O conjunto dos números algébricos é enumerável.*

Demonstração. Seja $P(\mathbb{Z})$ o conjunto dos polinômio de qualquer grau, ou seja, $P(\mathbb{Z}) = \cup_{n=1}^{\infty} P_n(\mathbb{Z})$. Como $P_n(\mathbb{Z})$ é enumerável, segue que $P(\mathbb{Z})$ é enumerável. Agora, seja R_p o conjunto das raízes de um polinômio $p(x) \in P(\mathbb{Z})$. A aplicação $f : P(\mathbb{Z}) \to \cup_{p\in P(\mathbb{Z})} R_p$ que associa cada polinômio $q \in P(\mathbb{Z})$ ao conjunto de suas raízes $R_q \in \cup R_p$ é sobrejetora. Portanto, $\cup_{p\in P(\mathbb{Z})} R_p$ é enumerável. □

Corolário 9.2.5. *O conjunto dos números transcendentes não é enumerável.*

Demonstração. Como $\mathbb{C}$ é a união dos números algébricos com os números transcendentes, segue que o conjunto dos números transcendentes não é enumerável. □

9.2.1 Exercícios

1. Mostre que a união e a interseção de dois conjuntos finitos é um conjunto finito.
2. Seja A um conjunto.
   (a) Mostre que A não é equipotente a $\mathcal{P}(A)$.
   (b) Mostre que A é finito se, e somente se, $\mathcal{P}(A)$ é finito.
3. Mostre que $\mathbb{Z}$ e $2\mathbb{Z}$ são equipotentes. Mostre que $\mathbb{Z}$ é equipotente a $n\mathbb{Z}$, onde $n > 1$.
4. Mostre que o conjunto dos naturais pares é equipotente ao conjunto dos naturais impares.
5. Mostre que os conjuntos $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$ são conjuntos enumeráveis e equipotentes.
6. Mostre que o intervalo aberto $]-1, 1[$ e $\mathbb{R}$ são equipotentes.
7. Sejam $a, b \in \mathbb{R}$, com $a < b$. Mostre que os intervalos $[-1, 1]$ e $[a, b]$ são equipotentes.
8. Mostre que $[0, 1]$ é equipotente a $]0, 2[$.
9. Mostre que $\mathbb{R}$ é equipotente a $[0, \infty[$.
10. Sejam A e B conjuntos enumeráveis. Mostre que $A \cup B$ e $\cap B$ são conjuntos enumeráveis.
11. Mostre que o conjunto $A = \{\frac{1}{n} : n \in \mathbb{Z} - \{0\}\}$ é enumerável.
12. Mostre que um conjunto A é enumerável se, e somente se, A é finito ou A é equipontente a $\mathbb{N}$.
13. Se A é enumerável, mostre que existe uma aplicação sobrejetora $f : \mathbb{N} \to A$.
14. Mostre que o conjunto $A = \{3^m 5^n : m, n \in \mathbb{N}\}$ é um conjunto enumerável.
15. Mostre que:
   (a) $\mathbb{N}^* \times \mathbb{N}$ é enumerável.
   (b) $\mathbb{Z}^* \times \mathbb{N}$ é enumerável.
   (c) $\mathbb{N}^* \times \mathbb{Q}$ é enumerável.
   (d) $\mathbb{Z}^* \times \mathbb{Q}^*$ é enumerável.

Capítulo

10

Operações binárias

Uma lei de composição interna é uma função que associa cada elemento do produto cartesiano de um conjunto a um elemento dese conjunto. A partir desse conceito obtemos várias propriedades, como veremos a seguir. Deste modo, no presente capítulo, apresentamos o conceito de operações sobre um conjunto (também conhecido como leis de composição interna), com a introdução das propriedades: associativa, comutativa, existência do elemento neutro, elementos simetrizáveis, elementos regulares e a operação distributiva.

10.1 Operações - leis de composição interna

Seja E um conjunto não vazio.

Definição 10.1.1. *Uma aplicação $f : E \times E \to E$ é chamada operação sobre E (ou lei de composição interna em E) e denotada por $f(x, y) = x * y$, onde $x, y \in E$.*

Seja $*$ uma operação sobre um conjunto E e A um subconjunto não vazio de E. O conjunto A é chamado fechado em relação a operação $*$ ou que a operação é fechada sobre A se $a * b \in A$, para todo $a, b \in A$.

Exemplo 10.1.1.

1. *A relação $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definida por $f(x, y) = x * y = mdc(x, y)$, onde $x, y \in \mathbb{N}$, é uma operação sobre $\mathbb{N}$.*

2. *O conjunto $m\mathbb{Z}$, onde $m \in \mathbb{Z}$, é fechado em relação a adição e a multiplicação.*

3. *O conjunto formado pelos números ímpares é fechado em relação a multiplicação, mas não é fechado em relação a adição.*

4. *A relação* $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *definida por* $f(x, y) = x - y$ *não define uma operação sobre* $\mathbb{N}$*, uma vez que* $(3, 5) \in \mathbb{N} \times \mathbb{N}e$ $f(3, 5) = 3 - 5 = -2$ *não pertence aos naturais.*

5. *A relação* $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ *definida por* $f(x, y) = \frac{x}{y}$ *não define uma operação sobre* $\mathbb{Z}$*, uma vez que* $(3, 6) \in \mathbb{Z} \times \mathbb{Z}$ *e* $(3, 6) = \frac{3}{6} = \frac{1}{2}$ *não pertence aos inteiros.*

6. *A relação* $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *definida por* $f(x, y) = xy$ *define uma operação sobre* $\mathbb{N}$*, uma vez que para quaisquer* $x, y \in \mathbb{N}$*, segue que* xy *é um número natural.*

7. *A adição sobre* $\mathbb{N}$*,* $\mathbb{Z}$*,* $\mathbb{Q}$*,* $\mathbb{R}$ *ou* $\mathbb{C}$ *é uma operação binária.*

8. *A subtração sobre* $\mathbb{Z}$*,* $\mathbb{Q}$*,* $\mathbb{R}$ *ou* $\mathbb{C}$ *é uma operação binária.*

9. *A multiplicação sobre* $\mathbb{N}$*,* $\mathbb{Z}$*,* $\mathbb{Q}$*,* $\mathbb{R}$ *ou* $\mathbb{C}$ *é uma operação binária.*

10. *A adição e multiplicação de matrizes sobre o conjunto das matrizes quadradas* $M_n(A)$ *com coeficientes em* A*, onde* $A = \mathbb{N}$*,* $\mathbb{Z}$*,* $\mathbb{Q}$*,* $\mathbb{R}$ *ou* $\mathbb{C}$ *é uma operação binária.*

10.1.1 Associativa

A operação $*$ sobre E é associativa se $a * (b * c) = (a * b) * c$, para todo $a, b, c \in E$.

Exemplo 10.1.2. *Em* $\mathbb{R}$ *as operações de adição e muliplicação são associativas, uma vez que* $a + (b + c) = (a + b) + c$ *e* $a(bc) = (ab)c$*, para todo* $a, b, c \in \mathbb{R}$*. Em* $\mathbb{R}$ *a divisão e a subtração não são associativas, uma vez que* $2 = (8 : 2) : 2 \neq 8 : (2 : 2) = 8$ *e* $-1 = (8 - 4) - 5 \neq 8 - (4 - 5) = 9$*. Também, em* $\mathbb{N} - \{0\}$*, a potenciação* $a * b = a^b$ *não é associativa, uma vez que* $(2 * 3) * 2 = 2^3 * 2 = (2^3)^2 = 2^6$ *e* $2 * (3 * 2) = 2 * 3^2 = 2 * 9 = 2^9$*.*

Exemplo 10.1.3. *Em* $\mathbb{R}$ *a operação* $x * y = x + y + xy$ *é associativa, uma vez que* $x * (y * z) = x * (y + z + yz) = x + y + z + yz + x(y + z + yz) = x + y + z + yz + xy + xz + xyz$ *e* $(x * y) * z = (x + y + xy) * z = x + y + xy + z + (x + y + xy)z = x + y + z + xy + xz + yz + xyz$*, para todo* $x, y, z \in \mathbb{R}$*.*

10.1.2 Comutativa

A operação $*$ sobre E é comutativa se $a * b = b * a$, para todo $a, b \in E$.

Exemplo 10.1.4. *Em* $\mathbb{R}$ *as operações de adição e muliplicação comutativas, uma vez que* $a+b = b+a$ *e* $ab = ba$*, para todo* $a, b \in \mathbb{R}$*. Em* $\mathbb{R}$ *a divisão e a subtração não são comutativas, uma vez que* $2 = (8 : 4) \neq (4 : 8) = 0.5$ *e* $3 = 8 - 4 \neq 4 - 8 = -4$*. Também, em* $\mathbb{N} - \{0\}$*, a potenciação* $a * b = a^b$ *não é associativa, uma vez que* $2 * 3 = 2^3 = 8 \neq 3 * 2 = 9$*.*

Exemplo 10.1.5. *Em* $\mathbb{N} - \{0\}$ *a operação* $x * y = mdc(x, y)$*, com* $x, y \in \mathbb{N} - \{0\}$*, é comutativa, uma vez que* $mdc(x, y) = mdc(y, x)$*, para todo* $x, y \in \mathbb{N} - \{0\}$*.*

Exemplo 10.1.6. *Em* $\mathbb{R}$ *a operação* $x * y = x + y + xy$ *é comutativa, uma vez que* $x * y = x + y + xy = y * x$*, para todo* $x, y \in \mathbb{R}$*. Agora, sobre* $\mathbb{R}$*, a operação* $x * y = x + xy$*, com* $x, y \in \mathbb{R}$ *não é comutativa, uma vez que* $3 = 1 * 2 = 1 + 1.2 \neq 2 * 1 = 2 + 2.1 = 4$*.*

10.1.3 Elemento neutro

Um elemento $e \in E$ é chamado elemento neutro em relação a operação $*$ se $x*e = e*x = x$, para todo $x \in E$.

Exemplo 10.1.7. *Em $\mathbb{R}$ o 0 é o elemento neutro da adição, uma vez que $x+0 = 0+x = x$, para todo $x \in \mathbb{R}$. Em $\mathbb{R} - \{0\}$, o 1 é o elemento neutro da multiplicação, uma vez que $x.1 = 1.x$, para todo $x \in \mathbb{R} - \{0\}$.*

Exemplo 10.1.8. *No conjunto $M_2(\mathbb{R})$, das matrizes 2×2, a matriz nula $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ é o elemento neutro em relação a adição e a matriz identidade $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ é o elemento neutro em relação ao produto.*

Exemplo 10.1.9. *Em $\mathbb{R}-\{-1\}$ a operação $x*y = x+y+xy$, com $x, y \in \mathbb{R}$, não possui elemento neutro, uma vez que se $x * e = x$, então $x + e + xe = x$, ou seja, $e(1 + x) = 0$. Como $x \neq -1$, segue que $e = 0$, e portanto, 0 é o elemento neutro.*

Proposição 10.1.1. *O elemento neutro de uma operação $*$ sobre E é único (caso exista).*

Demonstração. Se e_1 e e_2 são elementos neutros da operação $*$, então $e_1 * x = x = x * e_1$ e $e_2 * x = x = x * e_2$, para todo $x \in E$. Em particular, tomando $x = e_2$ na primeira igualdade e $x = e_1$ na segunda igualdade, segue que $e_1 = e_1 * e_2 = e_2$, ou seja, o elemento neutro (caso exista) é único. □

10.1.4 Elementos simetrizáveis

Seja $*$ uma operação sobre E que admite um elemento neutro $e \in E$. Um elemento $a \in E$ é chamado elemento simetrizável em relação a operação $*$ se existe um elemento $b \in E$ tal que $a * b = b * a = e$. Neste caso, o elemento b é denotado por a' e é chamado de simétrico de a. O elemento neutro é sempre simetrizável e é o próprio simétrico.

No caso da adição o simétrico aditivo de a é denotado por $-a$ e no caso da multiplicação o simétrico multiplicativo de a é denotado por a^{-1}, caso existam.

Exemplo 10.1.10. *Em $\mathbb{N}$ a operação de adição, $x*y = x+y$, com $x, y \in \mathbb{N}$, tem como elemento neutro o 0. Neste caso, o 0 é o único elemento simetrizável de $\mathbb{N}$.*

Exemplo 10.1.11. *Em $\mathbb{Z}$ com a operação de adição, todos os elementos são simetrizáveis.*

Exemplo 10.1.12. *Em $\mathbb{Z}$ com a operação de multiplicação, os únicos elementos simetrizáveis são ± 1.*

Exemplo 10.1.13. *Em $\mathbb{R}$ com a operação de adição, todos os elementos são simetrizáveis.*

Exemplo 10.1.14. *Em $\mathbb{R}$ com a operação de multiplicação, os elementos simetrizáveis são $\mathbb{R} - \{0\}$.*

Proposição 10.1.2. *Seja $*$ uma operação associativa sobre E que admite um elemento neutro $e \in E$. Se $a \in E$ é simetrizável, então o simétrico de a é único.*

Demonstração. Se a' e a' são simétricos de a em relação a operação $*$, então $a * a' = a' * a = e$ e $a'' * a = a * a'' = e$. Assim, $a' * e = a' = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''$, ou seja, o elemento simétrico de a é único. □

Proposição 10.1.3. *Seja $*$ uma operação associativa sobre E que admite um elemento neutro $e \in E$. Se $a, b \in E$ são simetrizáveis, então $a*b$ é simetrizável e seu simétrico é $(a*b)' = b'*a'$.*

Demonstração. Se a' e b' são os simétricos de a e b, respectivamente, em relação a operação $*$, então $(a * b) * (b' * a') = a * (b * b') * a' = a * a' = e$ e $(b' * a')(a * b) = b' * (a' * a) * b = b' * b = e$. Portanto, $b' * a'$ é o elemento simétrico de $a * b$. □

Corolário 10.1.1. *Seja $*$ uma operação associativa sobre E que admite um elemento neutro $e \in E$. Se $a \in E$ é simetrizável, então a' é simetrizável e $(a')' = a$.*

Demonstração. Se a é simetrizável, então existe o simétrico a' de a em E tal que $a*a' = a'*a = e$. Assim, por definição, a' é simetrizável, e desse modo, existe $(a')' \in E$ tal que $(a')' * a' = e$. Aplicando, a em ambos os lados, segue que $((a')') * a') * a = e * a$, ou seja, $(a')' * (a' * a) = a$. Assim, $(a')' * e = a$, e portanto, $(a')' = a$. □

Exemplo 10.1.15. *Todos os elementos de $\mathbb{R} - \{-1\}$ com a operação $x * y = x + y + xy$, onde $x, y \in \mathbb{R} - \{-1\}$, é simetrizável e o simétrico de $a \in \mathbb{R} - \{-1\}$ é dado por $a' = -\frac{a}{a+1}$, uma vez que se a' é o simétrico de a, então $a * a' = 0$. Assim, $a + a' + aa' = 0$, ou seja, $a' = -\frac{a}{a+1}$.*

10.1.5 Elementos regulares

Seja $*$ uma operação sobre E que é associativa. Um elemento $a \in E$ é chamado regular a esquerda se, para todo $x, y \in E$, $a * x = a * y$ e $x * a = y * a$ implicar que $x = y$, ou seja, vale a lei do cancelamento a esquerda. Um elemento $a \in E$ é chamado regular a direita se, para todo $x, y \in E$, $x * a = y * a$ implicar que $x = y$, ou seja, vale a lei do cancelamento a direita. Um elemento $a \in E$ é chamado regular se é regular a esquerda e regular a direita.

Exemplo 10.1.16. *Todos os elementos de $\mathbb{R}$, com relação a adição, são regulares e todos os elementos não nulos de $\mathbb{R}$, com relação ao produto, são regulares. Similarmente, todos os elementos de $\mathbb{Z}$, com relação a adição, são regulares e todos os elementos não nulos de $\mathbb{Z}$, com relação ao produto, são regulares.*

Exemplo 10.1.17. *Os elementos regulares de $\mathbb{R}$, com relação a operação $x * y = x + y + xy$, onde $x, y \in \mathbb{R}$, são os elementos $a \in \mathbb{R}$ tal que $a \neq -1$, uma vez que se $a * x = a * y$, então $a + x + ax = a + y + ay$, ou seja, $x + ax = y + ay$. Assim, $(x - y)(a + 1) = 0$, e $x = y$ sempre que $a \neq -1$.*

Exemplo 10.1.18. *Os elementos regulares de $\mathbb{R}-\{0, -1\}$, com relação a operação $x*y = x+xy$, onde $x, y \in \mathbb{R}$, são os elementos de $\mathbb{R}-\{0, -1\}$, uma vez que se $a*x = a*y$, então $a+ax = a+ay$, ou seja, $ax = ay$. Assim, $a(x-y) = 0$, e como $a \neq 0$, segue que $x = y$. Agora, se $x*a = y+a$, então $x + ax = y + ay$. Assim, $(x - y)(a + 1) = 0$. Como $a \neq -1$, segue que $x = y$.*

Proposição 10.1.4. *Seja $*$ uma operação sobre E que é associativa e tem elemento neutro. Se $a \in E$ é simetrizável, a é regular.*

Demonstração. Se $a \in E$ é simetrizável, então existe $a' \in E$ tal que $a' * a = a * a' = e$. Agora, sejam $x, y \in E$. Se $a * x = a * y$, então $a' * (a * x) = a' * (a * y)$. Assim, $(a' * a) * x = (a' * a) * y$, e portanto, $e * x = e * y$, ou seja, $x = y$. Similarmente, se $x * a = y * a$, então $(x * a) * a' = (y * a) * a'$. Assim, $x * (a * a') = y * (a * a')$, e portanto, $x * e = y * e$, ou seja, $x = y$. Portanto, a é regular. □

10.1.6 Operação distributiva

Sejam E um conjunto não vazio munido de duas operações $\star$ e $\triangle$.

Definição 10.1.2. *A operação $\star$ é chamada distributiva em relação a operação $\triangle$ se:*

1. $a \star (b \triangle c) = (a \star b) \triangle (a \star c \ e$
2. $(a \triangle b) \star c = (a \star c) \triangle (b \star c)$,

para todo $a, b, c \in E$.

Exemplo 10.1.19. *Seja $A = \mathbb{N}$ ou ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$). Neste caso, $a(b + c) = ab + ac$, para todo $a, b, c \in A$.*

10.1.7 Tábua de operações

Sejam $E = \{a_1, a_2, \ldots, a_n\}$ um conjunto de n elementos e $\star$ uma operação sobre E. Considerando que a operação de dois elementos de E é dada por $a_i \star a_j = a_{ij}$, podemos dispor os elementos através da seguinte tábua, chamada tábua de uma operação.

$\star$	a_1	a_2	$\ldots$	a_i	$\ldots$	a_j	$\ldots$	a_n
a_1	a_{11}	a_{12}	$\ldots$	a_{1i}	$\ldots$	a_{1j}	$\ldots$	a_{1n}
a_2	a_{21}	a_{22}	$\ldots$	a_{2i}	$\ldots$	a_{2j}	$\ldots$	a_{2n}
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
a_i	a_{i1}	a_{i2}	$\ldots$	a_{ii}	$\ldots$	a_{ij}	$\ldots$	a_{in}
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
a_j	a_{j1}	a_{j2}	$\ldots$	a_{ji}	$\ldots$	a_{jj}	$\ldots$	a_{jn}
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
a_n	a_{n1}	a_{n2}	$\ldots$	a_{ni}	$\ldots$	a_{nj}	$\ldots$	a_{nn}

Exemplo 10.1.20. *Sejam o conjunto $E = \{1, 3, 5, 9\}$ com a operação $a \star b = mdc(a, b)$. A tábua de operação é dada por*

$\star$	*1*	*3*	*5*	*9*
1	*1*	*1*	*1*	*1*
3	*1*	*3*	*1*	*3*
5	*1*	*1*	*5*	*1*
9	*1*	*3*	*1*	*9*

10.1.8 Exercícios

1. Em cada uma das operações abaixo verifique se é fechada, associativa, comutativa, tem elemento neutro, encontre os elementos simetrizáveis e os elementos regulares.

   (a) $E = \mathbb{R}_+$ e $x * y = \sqrt{x^2 + y^2}$.

   (b) $E = \mathbb{R}$ e $x * y = \sqrt[3]{x^3 + y^3}$.

   (c) $E = \mathbb{Z}$ e $x * y = xy + 2x$.

   (d) $E = \mathbb{Q}$ e $x * y = x + xy$.

   (e) $E = \mathbb{Z}$ e $x * y = x + xy$.

2. Verifique, em cada uma das operações abaixo verifique se é fechada, associativa, comutativa, tem elemento neutro, encontre os elementos simetrizáveis e os elementos regulares.

   (a) $E = \mathbb{Z} \times \mathbb{Z}$ e $(a, b) * (c, d) = (a + c, bd)$.

   (b) $E = \mathbb{R}$ e $x * y = x^2 + y^2 + xy$.

   (c) $E = \{a, b, c\}$ e $x * y = mdc(x, y)$.

   (d) $E = \mathcal{P}(\{a, b\})$ e $x * y = x \cup y$.

   (e) $E = \mathcal{P}(\{0, 1\})$ e $x * y = (x \cup y) - (x \cap y)$.

3. Em cada uma das operações abaixo verifique se é fechada, associativa, comutativa, tem elemento neutro, encontre os elementos simetrizáveis e os elementos regulares.

   (a) $E = \mathbb{R}$ e $x * y = \frac{x+y}{2}$.

   (b) $E = \mathbb{R}$ e $x * y = x$.

   (c) $E = \mathbb{R}^*$ e $x * y = x/y$.

   (d) $E = \mathbb{R}_+$ e $x * y = \frac{x+y}{1+xy}$.

4. Verifique, em cada uma das operações abaixo verifique se é fechada, associativa, comutativa, tem elemento neutro, encontre os elementos simetrizáveis e os elementos regulares.

   (a) $E = \mathbb{Z}$ e $x * y = x + y + xy$.

   (b) $E = \mathbb{R}$ e $x * y = x^2 + y^2 + 2xy$.

   (c) $E = \mathbb{N}$ e $x * y = min\{x, y\}$.

   (d) $E = \mathbb{Z}$ e $x * y = mdc(x, y)$.

   (e) $E = \mathbb{Z}$ e $x * y = mmc(x, y)$.

5. Em cada uma das operações abaixo sobre $\mathbb{Z} \times \mathbb{Z}$, verifique se é fechada, associativa, comutativa, tem elemento neutro, encontre os elementos simetrizáveis e os elementos regulares.

(a) $(a,b)*(c,d)=(ac,0)$.

(b) $(a,b)*(c,d)=(ac,ad+bc)$.

(c) $(a,b)*(c,d)=(a+c,bd)$.

(d) $(a,b)*(c,d)=(ac-bd,ad+bc)$.

(e) $(a,b)*(c,d)=(a+c,b+d)$.

6. Verifique se é fechada, associativa, comutativa, tem elemento neutro, encontre os elementos simetrizáveis e os elementos regulares da operação $(a,b,c)*(d,e,f)=(ad,be,cf)$ sobre $\mathbb{Z}^3$.

7. Em cada uma das operações abaixo verifique se é fechada, associativa, comutativa, tem elemento neutro, encontre os elementos simetrizáveis e os elementos regulares, com a operação de adição.

(a) $E=\{x\in\mathbb{Z}: x \text{ é par}\}\subseteq\mathbb{Z}$

(b) $E=\{x\in\mathbb{Z}: x \text{ é impar}\}\subseteq\mathbb{Z}$

(c) $E=m\mathbb{Z}=\{x\in\mathbb{Z}: m \text{ divide } x\}\subseteq\mathbb{Z}$

(d) $E=\{\begin{pmatrix} cos(a) & sen(a) \\ -sen(a) & cos(a)\end{pmatrix}: a\in\mathbb{R}\}\subseteq M_2(\mathbb{R})$.

(e) $A=\{z\in\mathbb{C}: z=cos(\theta)+isen(\theta)\}\subseteq\mathbb{C}$.

8. Em cada uma das operações abaixo verifique se é fechada, associativa, comutativa, tem elemento neutro, encontre os elementos simetrizáveis e os elementos regulares, com a operação de multiplicação.

(a) $E=\{x\in\mathbb{Z}: x \text{ é par}\}\subseteq\mathbb{Z}$

(b) $E=\{x\in\mathbb{Z}: x \text{ é impar}\}\subseteq\mathbb{Z}$

(c) $E=m\mathbb{Z}=\{x\in\mathbb{Z}: m \text{ divide } x\}\subseteq\mathbb{Z}$

(d) $E=\left\{\begin{pmatrix} cos(a) & sen(a) \\ -sen(a) & cos(a)\end{pmatrix}: a\in\mathbb{R}\right\}\subseteq M_2(\mathbb{R})$.

(e) $A=\{z\in\mathbb{C}: z=cos(\theta)+isen(\theta)\}\subseteq\mathbb{C}$.

9. Em cada uma das operações abaixo faça a tábua de operação e verifique se é fechada, associativa, comutativa, tem elemento neutro, encontre os elementos simetrizáveis e os elementos regulares, com a operação de multiplicação.

(a) $E=\{1,2,3,6\}$ e $x*y=mdc(x,y)$.

(b) $E=\{1,3,9,27\}$ e $x*y=mmc(x,y)$.

(c) $E=\mathcal{P}(\{a,b\})$ e $x*y=x\cup y$.

(d) $E=\mathcal{P}(\{a,b\})$ e $x*y=x\cap y$.

(e) $E=\mathcal{P}(\{a,b\})$ e $x*y=(x\cup y)-(x\cap y)$.

10. Determine, em cada uma das operações abaixo a tábua de operação e verifique se é fechada, associativa, comutativa, tem elemento neutro, encontre os elementos simetrizáveis e os elementos regulares, com a operação de multiplicação.

    (a) $E = \{\sqrt{3/2}, \sqrt[3]{5/2}, \sqrt[4]{7/2}\}$ e $x * y = min\{x, y\}$.

    (b) $E = \{3\sqrt{2}, \pi, 7/2\}$ e $x * y = max\{x, y\}$.

    (c) $E = \{1, -1, i, -i\}$ e $x * y = xy$.

    (d) $E = \{1, 4, 5, 20\}$ e $x * y = max\{x, y\}$.

    (e) E é o conjunto das permutações de $A = \{1, 2, 3\}$ com a operação de composição de funções.

11. Determine $m, n \in \mathbb{Z}$ para que a operação $x * y = mx + ny$, sobre $\mathbb{Z}$, seja:

    (a) Associativa.

    (b) Comutativa.

    (c) Admita elemento neutro.

12. Seja a operação $*$ sobre $\mathbb{R}$ definida por $x * y = ax + by + cxy$, onde $a, b, c \in \mathbb{R}$. Determine a, b e c tal que a operação $*$ seja associativa e tenha elemento neutro.

13. Determine os elementos neutros a esquerda no conjunto $E = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{R} \right\}$ com a operação de multiplicação.

14. Construir a tábua da operação de composição das funções $f_1 = \{(a, a); (b, b); (c, c)\}$, $f_2 = \{(a, b); (b, c); (c, a)\}$ e $f_3 = \{(a, c); (b, a); (c, b)\}$.

15. Verifique se a operação dada por $(a, b) * (c, d) = (ac, ad + bc)$ é distributiva em relação a operação $(a, b)\triangle(c, d) = (a + c, b + d)$ sobre $\mathbb{Z} \times \mathbb{Z}$.

16. Determine $m \in \mathbb{R}$ tal que a operação $a * b = a + mb$ seja distributiva em relação a operação $x \triangle y = x + y + xy$.

17. Sejam A, B, C três conjuntos não vazios. Mostre que a operção $\cap$ é distributiva em relação a operação $\cup$, ou seja,

    (a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

    (b) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

18. Sejam A, B, C três conjuntos não vazios. Mostre que a operção $\cup$ é distributiva em relação a operação $\cap$, ou seja,

    (a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

    (b) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

19. Seja $G = \{z \in \mathbb{C} : z = cos(\theta) + isen(\theta)\} \subseteq \mathbb{C}$ com relação ao produto.

(a) Verifique se é fechada, comutativa e associativa.

(b) Determine o elemento neutro e os elementos simetrizáveis.

20. Determinar todas as operações sobre:

(a) O conjunto $E = \{a, b\}$, com $a \neq b$.

(b) O conjunto $E = \{a, b, c\}$, com $a \neq b$, $a \neq c$ e $b \neq c$.

21. Seja A um conjunto não vazio e $\mathbb{R}^A$ o conjunto de todas as aplicações de A em $\mathbb{R}$. Seja as seguintes operações sobre $\mathbb{R}^A$, para todo $f, g \in \mathbb{R}^A$: $(f + g)(x) = f(x) + g(x)$, para todo $x \in A$, e $(fg)(x) = f(x)g(x)$, para todo $x \in A$.

(a) Verifique que se $(\mathbb{R}^A, +)$ é fechada, comutativa e associativa. Determine o elemento neutro e os elementos simetrizáveis.

(b) Verifique que se $(\mathbb{R}^A, \cdot)$ é fechada, associativa e comutativa. Determine o elemento neutro e os elementos simetrizáveis.

22. Se $(G, \star)$ é fechada, associativa, possui elemento neutro e todo elemento é simetrizável, para todo $x, y, z \in G$, mostre que $(x * y * z)^{-1} = z^{-1} * y^{-1} * x^{-1}$.

23. Seja $G = \mathbb{Z}_m$, onde $m \in \mathbb{N}$. Mostre que $g \in G$ é simetrizável em relação ao produto se, e somente se, $mdc(g, m) = 1$.

24. Determine uma operação sobre um conjunto E tal que todo elemento é regular, possui elemento neutro e e e é o único elemento simetrizável.

25. Encontro uma operação sobre um conjunto E que possui elemento neutro e todos os elementos de E, com excessão do elemento neutro, tem dois simétricos.

26. Determine uma operação sobre E tal que o composto de dois elementos simetrizáveis não é simetrizável.

27. Determine uma operação sobre um conjunto E que não é associativa, mas possui elemento regular.

28. Seja E um conjunto com uma operação $*$ que é associativa.

(a) Mostre que $a \in E$ é regular se, e somente se, as aplicações $f : E \to E$ e $g : E \to E$ definidas por $g(x) = a * x$ e $g(x) = x * a$, onde $x \in E$, são injetoras.

(b) Se $a, b \in E$ são regulares, mostre que $a * b$ é regular.

(c) Se $a \in E$ é regular, mostre que o conjunto $a * E = \{a * x : x \in E\} = E$, quando E for finito.

29. Verifique se as operações abaixo é fechada, associativa, comutativa, elemento neutro, elementos simetrizáveis e elementos regulares.

(a) $E = \mathbb{N}$ e $x \star y = x - y$.

(b) $E = \mathbb{Q}$ e $x \star y = x/y$.

(c) $E = \mathbb{Z}$ e $x \star y = xy + x + x^2$.

(d) $E = \mathbb{Z}$ e $x \star y = x^2 + y^2$

10.2 Adição e multiplicação modular

Sejam $a, b, m \in \mathbb{Z}$ com $m > 1$. A relação

$$a \equiv b(mod\ m) \text{ se, e somente se, } m|(a-b)$$

é uma relação de equivalência sobre $\mathbb{Z}$. A classe de equivalência de um elemento $a \in \mathbb{Z}$ é dada por

$$\overline{a} = \{x \in \mathbb{Z} : x \equiv a(mod\ m)\}.$$

Pelo algoritmo da divisão, segue que existem $q, r \in \mathbb{Z}$ únicos tal que $a = mq + r$, onde $0 \leq r \leq m-1$. Assim,

$$\overline{a} = \overline{r},$$

e portanto, o conjunto quociente é dado por

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}.$$

Neste caso, podemos usar a notação $\mathbb{Z}_m = \{0, 1, 2, \cdots, m-1\}$, onde $m \in \mathbb{Z}$, com $m > 1$ e $r = 0, 1, \cdots, m-1$ é o resto da divisão de $a \in \mathbb{Z}$ por m.

Definição 10.2.1. *(Adição módulo m) Sejam $a, b \in \mathbb{Z}_m$. A adição de a e b módulo m é definida por $a +_m b = r$, onde r é o resto da divisão euclidiana de $a + b$ por m.*

Exemplo 10.2.1. *Em $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, segue que $2 +_4 2 = 0$ e $1 +_4 3 = 0$.*

Propriedades 10.2.1. *Sejam $a, b, c \in \mathbb{Z}_m$. Em relação a operação de adição módulo m, segue as seguintes propriedades.*

1. *Associativa: $a +_m (b +_m c) = (a +_m b) +_m c$. De fato, se $b +_m c = r_1$, então $b + c = mq + r_1$, onde $q, r_1 \in \mathbb{Z}$ e $0 \leq r_1 < m$. Se $a +_m r_1 = r$, então $a + r_1 = mq_1 + r$, onde $q_1, r \in \mathbb{Z}$ e $0 \leq r < m$. Assim, $b + c = mq + r_1 = mq + mq_1 + r - a$, ou seja, $a + b + c = m(q + q_1) + r$, com $0 \leq r < m$. Logo, r é o resto da divisão de $a+(b+c)$ por m, ou seja, $r = a +_m (b +_m c)$. Analogamente, $(a +_m b) +_m c$ é o resto da divisão euclidiana de $(a+b)+c$ por m. Portanto, $a +_m (b +_m c) = (a +_m b) +_m c$.*

2. *Comutativa: $a +_m b = b +_m a$. De fato, se $r = a +_m b$, então $a + b = mq + r$, onde $q, r \in \mathbb{Z}$ e $0 \leq r < m$. Assim, r também é o resto da divisão de $b + a$ por m, ou seja, $b +_m a = r$. Portanto, $a +_m b = b +_m a$.*

3. *Elemento neutro: $a +_m 0 = a$, para todo $a \in \mathbb{Z}_m$, ou seja, 0 é o elemento neutro. De fato, segue diretamente do fato que a é o resto da divisão de $a + 0 = a$ por m.*

4. *Elementos simetrizáveis: Todo elemento $a \in \mathbb{Z}_m$ é simetrizável, ou seja, se $a \in \mathbb{Z}_m$, então existe $m - a \in \mathbb{Z}_m$ tal que $a +_m (m - a) = 0$. De fato, segue diretamente do fato que 0 é o resto da divisão de $a + (m - a) = m$ por m.*

Definição 10.2.2. *(Multiplicação módulo m) Sejam $a, b \in \mathbb{Z}_m$. A multiplicação de a e b módulo m é definida por $a._m b = r$, onde r é o resto da divisão de ab por m.*

Exemplo 10.2.2. *Em $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, segue que $2._6 2 = 4$ e $2._6 3 = 0$.*

Propriedades 10.2.2. *Sejam $a, b, c \in \mathbb{Z}_m$. Em relação a operação de multiplicação módulo m, segue as seguintes propriedades.*

1. *Associativa: $a._m(b._m c) = (a._m b)._m c$. De fato, se $b._m c = r_1$, então $bc = mq + r_1$, onde $q, r_1 \in \mathbb{Z}$ e $0 \leq r_1 < m$. Se $a._m r_1 = r$, então $ar_1 = mq_1 + r$, onde $q_1, r \in \mathbb{Z}$ e $0 \leq r < m$. Assim, $abc = amq + ar_1 = amq + mq_1 + r$, ou seja, $abc = m(aq + q_1) + r$, com $0 \leq r < m$. Logo, r é o resto da divisão de $a(bc)$ por m, ou seja, $r = a._m(b._m c)$. Analogamente, $(a._m b)._m c$ é o resto da divisão euclidiana de $(ab)c$ por m. Portanto, $a._m(b._m c) = (a._m b)._m c$.*

2. *Comutativa: $a._m b = b._m a$. De fato, se $r = a._m b$, então $ab = mq + r$, onde $q, r \in \mathbb{Z}$ e $0 \leq r < m$. Assim, r também é o resto da divisão de ba por m, ou seja, $b._m a = r$. Portanto, $a._m b = b._m a$.*

3. *Elemento neutro: $a._m 1 = a$, para todo $a \in \mathbb{Z}_m$, ou seja, 1 é o elemento neutro. De fato, segue diretamente do fato que a é o resto da divisão de $a.1 = a$ por m.*

4. *Elementos simetrizáveis: $a \in \mathbb{Z}_m$ é simetrizável, se e somente se, $mdc(a, m) = 1$. De fato, se $a \in \mathbb{Z}_m$ é simetrizável, então existe $b \in \mathbb{Z}_m$ tal que $a._m b = 1$. Assim, $ab = mq + 1$, onde $q \in \mathbb{Z}$. Desse modo, $ab + m(-q) = 1$, ou seja, $mdc(a, m) = 1$. Reciprocamente, se $mdc(a, m) = 1$, então existem $x_0, y_0 \in \mathbb{Z}$ tal que $ax_0 + my_0 = 1$. Assim, $ax_0 = m(-y_0) + 1$, ou seja, 1 é o resto da divisão de ax_0 por m. Portanto, $a._m x_0 = 1$, ou seja, x_0 é o simétrico de a.*

Exemplo 10.2.3. *Se n não for um primo, então existem elementos em $\mathbb{Z}_n - \{0\} = \{1, 2, \cdots, n - 1\}$ que não não inversíveis sob a operação de multiplicação módulo n. Por exemplo, para $n = 4$, segue que $\mathbb{Z}_4 - \{0\} = \{1, 2, 3\}$ e $2 \times 2 = 0$.*

Exemplo 10.2.4. *Em relação a multiplicação, os elementos simetrizáveis de $\mathbb{Z}_6$ são $\{1, 5\}$ e os elementos simetrizávies de $\mathbb{Z}_5$ são $\{1, 2, 3, 4\}$.*

10.2.1 Exercícios

1. Em cada uma das operações abaixo faça a tábua da operação e verifique se é fechada, associativa, comutativa, tem elemento neutro, determine os elementos simetrizáveis e os elementos regulares.

   (a) $E = \{0, 1, 2, 3\}$ e $x * y$ é o resto da divisão em $\mathbb{Z}$ de $x + y$ por 4.

   (b) $E = \{1, 2, 3, 4\}$ e $x * y$ é o resto da divisão em $\mathbb{Z}$ de xy por 5.

(c) $E = \mathbb{Z}_{24}$, onde $x * y$ é o resto da divisão de xy por 24.

2. Determine:

   (a) Os elementos simetrizáveis e regulares de $\mathbb{Z}_6$ em relação ao produto.

   (b) Os elementos simetrizáveis e regulares de $\mathbb{Z}_{12}$ em relação ao produto.

3. Determine a ordem dos elementos de:

   (a) $(\mathbb{Z}_{12}, +_{12})$.

   (b) $(\mathbb{Z}_7^*, .7)$.

   (c) $\mathbb{Z}_2 \times \mathbb{Z}_4$.

4. Construir a tábua de operação do conjunto:

   (a) $E = \{0, 1\}$ com a operação da soma módulo 2.

   (b) $E = \{1, -1\}$ com a operação de multiplicação.

   (c) $E = \{0, 1, 2\}$ a operação de multiplicação módulo 3.

5. Determine a tábua das seguintes operações:

   (a) $E = \{0, 1, 2, 3\}$ com a operação de adição módulo 4.

   (b) $E = \{0, 1, 2, 3\}$ com a operação de multiplicação módulo 4.

   (c) $E = \{0, 1, 2, 3, 4\}$ com a operação de adição módulo 5.

   (d) $E = \{0, 1, 2, 3, 4\}$ com a operação de multiplicação módulo 5.

6. Determine os elementos simetrizáveis:

   (a) $E = \{0, 1, 2, 3\}$ com a operação de adição módulo 4.

   (b) $E = \{0, 1, 2, 3\}$ com a operação de multiplicação módulo 4.

   (c) $E = \{0, 1, 2, 3, 4\}$ com a operação de adição módulo 5.

   (d) $E = \{0, 1, 2, 3, 4\}$ com a operação de multiplicação módulo 5.

7. Determine os elementos simetrizáveis, em relação a adição, dos seguintes conjuntos:

   (a) $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$.

   (b) $\mathbb{R}$, $\mathbb{C}$ e $M_n(\mathbb{N})$.

8. Determine os elementos simetrizáveis, em relação ao produto, dos seguintes conjuntos:

   (a) $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$.

   (b) $\mathbb{R}$, $\mathbb{C}$ e $M_n(\mathbb{N})$.

9. Verifique quais dos conjuntos abaixo são grupos.

(a) O conjunto $M_n(\mathbb{N})$ com o produto.

(b) O conjunto $M_n(\mathbb{N})$ com a soma.

(c) O conjunto $M_n(\mathbb{Z})$ com o produto.

(d) O conjunto $M_n(\mathbb{Z})$ com a soma.

10. Verifique quais dos conjuntos abaixo são grupos.

(a) O conjunto $M_n(\mathbb{Z}_2)$ com o produto.

(b) O conjunto $M_n(\mathbb{Z}_2)$ com a soma.

(c) O conjunto $M_n(\mathbb{Z}_3)$ com o produto.

(d) O conjunto $M_n(\mathbb{Z}_3)$ com a soma.

Capítulo

11

Álgebra de Boole

George Boole nasceu em Lincoln - Inglaterra em 2 de Novembro de 1815, filho de um sapateiro pobre. A sua formação base na escola primária da National Society foi muito rudimentar. Autodidata, fundou aos 20 anos de idade a sua própria escola e dedicou-se ao estudo da Matemática.

Em 1840 publicou o seu primeiro trabalho original e em 1844 foi condecorado com a medalha de ouro da Royal Society pelo seu trabalho sobre cálculo de operadores. Em 1847 publica um volume sob o título The Mathematical Analysis of Logic em que introduz os conceitos de lógica simbólica demonstrando que a lógica podia ser representada por equações algébricas. Este trabalho é fundamental para a construção e programação dos computadores eletrônicos iniciada cerca de 100 anos mais tarde.

Na álgebra de Boole existem apenas três operadores E, OU e NÃO (AND, OR e NOT). Estas três funções são as únicas operações necessárias para efetuar comparações ou as quatro operações aritméticas base. Em 1937, cerca de 75 anos após a morte de Boole, Claude Shannon, então estudante no MIT - Boston, USA - estabeleceu a relação entre a álgebra de Boole e os circuitos eletrônicos transferindo os dois estados lógicos (SIM e NÃO) para diferentes diferenças de potencial no circuito.

Atualmente todos os computadores usam a álgebra de Boole materializada em microchips que contêm milhares de interruptores miniaturizados combinados em portas (gates) lógicos que produzem os resultados das operações utilizando uma linguagem binária.

Para descrever os circuitos que podem ser construídos pela combinação de portas lógicas, um novo tipo de álgebra é necessário, uma vez que as variáveis e funções podem ter apenas valores 0 e 1. Tal álgebra é denominada álgebra booleana, devido ao seu descobridor, o matemático

inglês George Boole (1815 - 1864).

Do mesmo modo que existem funções em álgebra "comum", também existem funções na álgebra booleana. Uma função booleana tem uma ou mais variáveis de entrada e fornece somente um resultado que depende apenas dos valores destas variáveis.

Como uma função de n variáveis possui apenas 2n conjuntos possíveis de valores de entrada, a função pode ser descrita completamente através de uma tabela de 2n linhas, cada linha mostrando o valor da função para uma combinação diferente dos valores de entrada. Tal tabela é denominada tabela verdade.

Neste capítulo, apresentamos inicialmente alguns fatos e propriedades da teoria de grupos e anéis, anel de Boole, álgebra de Boole, ordem de Boole e o Teorema de Stoné.

11.1 Grupos e anéis

A presente seção, tem como objetivo uma recapitulação de alguns conceitos básicos de álgebra. Ao mesmo tempo, fixamos a terminologia e a notação adotadas nas demais seções, onde apresentamos estruturas algébricas que são muito útil para a álgebra abstrata, chamadas grupo e anel.

Definição 11.1.1. *Um conjunto não vazio G é chamado um semi-grupo em relação a uma operação $*$ se a operação $*$ é associativa, ou seja, $a*(b*c) = (a*b)*c$, para todo $a, b, c \in G$. Neste caso, também é dito que a operação $*$ define uma estrutura de semi-grupo sobre G.*

Se a operação $*$ também for comutativa, ou seja, $a*b = b*a$, para todo $a, b \in G$, o semi-grupo é chamado um semi-grupo comutativo.

Definição 11.1.2. *Um conjunto G é chamado um monóide em relação a operação $*$ se:*

1. *a operação $*$ é associativa, ou seja, $a*(b*c) = (a*b)*c$, para todo $a, b, c \in G$, e*
2. *a operação $*$ possui elemento neutro, ou seja, existe $e \in G$ tal que $a*e = e*a = a$, para todo $a \in G$.*

Neste caso, também é dito que a operação $*$ define uma estrutura de monóide sobre G.

Portanto, um monóide é um semi-grupo que possui elemento neutro. Se a operação também for comutativa, o monóide G é chamado um monóide comutativo.

Exemplo 11.1.1. *As operações de soma e de multiplicação sobre o conjunto dos naturais $\mathbb{N}$ são associativas, comutativas e possuem elementos neutros. Portanto, o conjunto dos naturais é um monóide comutativo em relação a adição, e também, em relação a multiplicação.*

Exemplo 11.1.2. *O mesmo vale para o conjunto dos números inteiros, para o conjunto dos números racionais e para o conjunto dos números reais.*

Exemplo 11.1.3. *O conjunto $2\mathbb{N}$ com a operação de adição é um monóide aditivo.*

Exemplo 11.1.4. *O conjunto* $2\mathbb{N}$ *com a operação de multiplicação é apenas um semi-grupo multiplicativo, uma vez que não possui elemento neutro. O mesmo vale para* $2\mathbb{Z}$*.*

Exemplo 11.1.5. *O conjunto* $\mathbb{N} - \{0\}$ *dos naturais sem o zero é apenas um semi-grupo.*

Exemplo 11.1.6. *O conjunto* $\mathbb{N} - \{0\}$ *com a operação* $*$ *definida por* $a * b = a^b$ *não é um semi-grupo, pois não é associativa.*

Proposição 11.1.1. *Todo elemento simetrizável de um monóide* $(G, *)$ *é regular.*

Demonstração. Sejam $a \in G$ um elemento simetrizável e $x, y \in G$ tal que $a * x = a * y$. Assim, existe $a' \in G$ tal que $a * a' = a' * a = e$, e desse modo, $x = e * x = (a' * a) * x = a' * (a * x) = a' * (a * y) = (a' * a) * y = e * y = y$. Portanto, a é regular a esquerda. De modo análogo, a é regular a direita. □

Exemplo 11.1.7. *Seja o monóide multiplicativo* $\mathbb{Z}$*. O número* 0 *não é regular, pois* $0 \cdot 1 = 0 \cdot 2$ *e* $1 \neq 2$*. Mas, todo inteiro não nulo é regular. Assim, existem elementos regulares que não são simetrizáveis.*

Observação 11.1.1. *Seja* G *um conjunto não vazio munido de uma operação* $*$ *e que possua elemento neutro* e*. O conjunto dos elementos simetrizáveis de* G*, em relação a operação* $*$*, é denotado por* G^**, ou seja,* $G^* = \{a \in G : \text{existe } a' \in G \text{ tal que } a * a' = a' * a = e\}$*.*

Definição 11.1.3. *Seja* G *um conjunto não vazio munido de uma operação* $\star$ *sobre* G*. O conjunto* G *é chamado um grupo em relação a essa operação se as seguintes propriedades são satisfeitas:*

1. *associativa, isto é,* $a \star (b \star c) = (a \star b) \star c$*, para todo* $a, b, c \in G$*,*
2. *existe um elemento identidade ou neutro* $e \in G$ *tal que* $a \star e = e \star a = a$*, para todo* $a \in G$*, e*
3. *para todo* $a \in G$ *existe um elemento* $a' \in G$ *tal que* $a \star a' = a' \star a = e$*. O elemento* a' *(ou* a^{-1}*) é chamado elemento simétrico ou inverso do elemento* a*. Neste caso, O elemento* a *é chamado simetrizável.*

Se, além disso, $a \star b = b \star a$ *para todo* $a, b \in G$*, o grupo* G *é chamado um grupo comutativo ou abeliano.*

Seja G um grupo.

1. O elemento neutro $e \in G$ é único. De fato, se $e_1, e_2 \in G$ são elementos neutros de G, então $e_1 = e_1 \star e_2 = e_2$. Assim, $e_1 = e_2$, e portanto, o elemento neutro de G é único.
2. O simétrico de um elemento $a \in G$ é único. De fato, se a', a'' são simétricos de um elemento $a \in G$ e é o elemento neutro de G, então $a' = a' \star e = a' \star (a \star a'') = (a' \star a) \star a'' = e \star a'' = a''$. Assim, $a' = a''$, e portanto, o simétrico de a é único.

Definição 11.1.4. *Seja* G *um grupo.*

1. *O grupo G é um chamado um grupo finito se G for um conjunto finito. Caso contrário, G é chamado um grupo infinito.*

2. *Se G for um grupo finito, o número de elementos de G é chamado de ordem de G e denotado por $\circ(G)$.*

Exemplo 11.1.8. *O conjunto dos números reais sob a operação de adição, o conjunto dos números reais não nulos sob a operação de multiplicação, o conjunto dos números inteiros sob a operação de adição, o conjunto dos números racionais sob a operação de adição, o conjunto dos números racionais não nulos sob a operação de multiplicação são exemplos de grupos infinitos.*

Exemplo 11.1.9. *O conjunto dos inteiros não nulos com a operação de multiplicação não é um grupo. Mas, considerando os números inteiros munido da operação subtração não é um grupo, uma vez que não existe um elemento neutro e tal que $e - x = x$, para todo $x \in \mathbb{Z}$.*

Definição 11.1.5. *Seja A um conjunto diferente do vazio munido das leis de composição de adição $(x, y) \to x + y$ e de multiplicação $(x, y) \to xy$. O conjunto A é chamado um anel se:*

1. *$(A, +)$ é um grupo abeliano, ou seja:*

   (a) *Se $a, b, c \in A$ então $a + (b + c) = (a + b) + c$ (associativa);*

   (b) *Se $a, b \in A$ então $a + b = b + a$ (comutativa);*

   (c) *Existe o elemento neutro $0 \in A$ tal que, qualquer que seja $a \in A$, segue que, $a+0 = a$ (elemento neutro);*

   (d) *Qualquer que seja $a \in A$ existe um elemento em A, indicado genericamente por $-a$, tal que $a + (-a) = 0$ (simétrico);*

2. *A multiplicação é distributiva em relação à adição, ou seja, se $a, b, c \in A$, então $a(b+c) = ab + ac$.*

3. *A multiplicação goza da propriedade associativa, ou seja, se $a, b, c \in A$, então $a(bc) = (ab)c$.*

Um anel não precisa ter elemento neutro da multiplicação, e também, os elementos não nulos de um anel não precisam ter inversos multiplicativos.

Observação 11.1.2. *Seja A um anel.*

1. *O elemento neutro é único.*

2. *O oposto $-a$ de um elemento A do anel é único.*

3. *Se $a_1, a_2, \ldots, a_n \in A$, então $-(a_1 + a_2 + \cdots + a_n) = (-a_1) + (-a_2) + \cdots + (-a_n)$.*

4. *Se $a \in A$, então $-(-a) = a$.*

5. *Se $a + x = a + y$, então $x = y$,* lei do cancelamento*, ou seja, todo elemento de A é regular em relação a adição.*

6. *A equação $a + x = b$ tem somente a solução $b + (-a)$.*

7. *Se $a \in A$, então $a0 = 0a = 0$.*

8. *Se $a, b \in A$, então $a(-b) = (-a)b = -(ab)$.*

9. *Se $a, b \in A$, então $(-a)(-b) = ab$.*

Definição 11.1.6. *Seja A um anel.*

1. *O anel A é chamado um anel comutativo se a sua multiplicação é comutativa, isto é, se $ab = ba$ para todo $a, b \in A$.*

2. *O anel A é chamado um anel com unidade se A possui o elemento neutro para a multiplicação. Esse elemento será indicado por 1_A ou apenas 1, se não houver possibilidade de confusão. Além disso, supomos sempre que $1 \neq 0$ (o elemento neutro aditivo de A). O elemento neutro da multiplicação do anel A é chamado unidade do anel.*

3. *O anel A é chamado um anel comutativo com unidade se a multiplicação é comutativa e para a qual existe o elemento neutro da multiplicação.*

Exemplo 11.1.10. *O conjunto dos números inteiros, o conjunto do números racionais, o conjunto dos números reais e o conjunto dos números complexos sob a adição e a multiplicação usuais são anéis comutativos com unidade.*

Exemplo 11.1.11. *O conjunto $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$ sob as operações de soma e de produto módulo n são anéis comutativos com unidade, neste caso, o elemento 1 é o elemento unidade.*

Exemplo 11.1.12. *Os anéis $n\mathbb{Z}$ não admitem unidade, salvo quando $n = 1$, caso que se trata do próprio $\mathbb{Z}$.*

Exemplo 11.1.13. *O anel das matrizes $M_n(\mathbb{K})$, onde $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, não é comutativo, mas possui unidade.*

Exemplo 11.1.14. *Se A e B são anéis, então o produto direto $A \times B = \{(a, b) : a \in A \text{ e } b \in B\}$, onde as operações de soma e produto são definidas componente a componente, é um anel. Em geral, o produto direto de n anéis é um anel.*

Definição 11.1.7. *Seja A um anel.*

1. *Um elemento a não nulo de A é chamado divisor de zero se existe um elemento não nulo $b \in A$ tal que $ab = 0$ ou $ba = 0$.*

2. *Se A for um anel com unidade, um elemento a de A é denominado inversível (ou unidade) em A se existir $b \in A$ tal que $ab = ba = 1$, onde o elemento b será denotado por a^{-1}.*

O conjunto dos elementos inversíveis de A será denotado por A^* e é um grupo abeliano em relação a multiplicação. Além disso, é comum usarmos o termo unidade de A para um elemento inversível de A.

Definição 11.1.8. *Seja A um anel.*

1. *O anel A é chamado um anel com divisão, ou um quase corpo, se $(A-\{0\},\cdot)$ é um grupo.*
2. *Um elemento $a \in A$, $a \neq 0$, é chamado um divisor de zero à esquerda de A se existe $b \neq 0$ em A tal que $ab = 0$. Analogamente, $a \neq 0$ é um divisor próprio de zero à direita se existe $b \neq 0$ tal que $ba = 0$.*
3. *Um anel comutativo com unidade A é chamado um anel de integridade (ou domínio) se para $a, b \in A$ tal que $ab = 0$ implicar que $a = 0$ ou $b = 0$, ou seja, A não possui divisores de zeros não nulos.*

A frase $ab = 0$ implica que $a = 0$ ou $b = 0$, onde $a, b \in A$, recebe o nome de *lei do anulamento do produto*. Assim, um anel de integridade é um anel comutativo com unidade em que vale a lei do anulamento do produto. Em outras palavras podemos dizer que A é um anel de integridade se o mesmo não contiver divisores de zero.

Exemplo 11.1.15. *Os anéis $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são domínios.*

Exemplo 11.1.16. *No anel $\mathbb{Z}_6$ os elementos $\overline{2}$ e $\overline{3}$ são divisores de zero uma vez que são não nulos, e no entanto, $\overline{2}.\overline{3} = \overline{0}$. Assim, o anel $\mathbb{Z}_6$ não é um anel de integridade.*

Exemplo 11.1.17. *O anel $\mathbb{Z}_m$ é um domínio se, e somente se, m é primo. De fato, se m não for primo, então existem $r, s \in \mathbb{Z}$, de tal forma que $1 < r, s < m$ e $rs = m$. Assim, $\overline{0} = \overline{m} = \overline{rs}$. Desse modo, existem divisores de zero em $\mathbb{Z}_m$, o que é contra à hipótese. Reciprocamente, se existem $\overline{a}, \overline{b} \in \mathbb{Z}_m$ tal que $\overline{a}\overline{b} = \overline{0}$, então $m \mid ab$. Como m é primo, segue que $m \mid a$ ou $m \mid b$. Isto significa que $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$, ou seja, que $\mathbb{Z}_m$ é um domínio. Assim, $\mathbb{Z}_n$, com $n \neq p$, onde p é um primo, não é um anel de integridade.*

11.1.1 Exercícios

1. Seja $\mathbb{N}$ o conjunto dos números naturais.
   (a) Mostre que as operações de soma e de multiplicação sobre $\mathbb{N}$ são associativas, comutativas e possuem elementos neutros.
   (b) Mostre que $\mathbb{N}$ é um monóide comutativo em relação a adição.
   (c) Mostre que $\mathbb{N}$ é um monóide em relação à multiplicação.
2. Seja $G = 2\mathbb{N}$ com a operação de adição.
   (a) Mostre que G é um semi-grupo.
   (b) Mostre que G não é monóide.
3. Seja o conjunto $G = 2\mathbb{N} = \{2n : n \in \mathbb{N}\}$ com a operação de multiplicação.
   (a) Mostre que G é um semi-grupo.

(b) Mostre que G não é um monóide.

4. Seja $G = \mathbb{N} - \{0\}$ com a operação de adição.

   (a) Mostre que G é um semi-grupo.

   (b) Mostre que G não é um monóide.

5. Mostre que $\mathbb{N} - \{0\}$ com a operação $*$ definida por $a * b = a^b$ não é um semi-grupo.

6. Mostre que o conjunto $\mathbb{Z}^*$ (respectivamente, $\mathbb{Q}^*$, $\mathbb{R}^*$ e $\mathbb{C}^*$) é um grupo com a operação de multiplicação usual.

7. Mostre que o conjunto $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ forma um grupo com a multiplicação.

8. Mostre que a operação de subtração sobre $\mathbb{N}$ não é fechada.

9. Mostre que a operação de subtração sobre $\mathbb{Z}$ é fechada, mas não é associativa, não é comutativa e não tem elemento neutro.

10. Mostre que a operação de divisão sobre $\mathbb{Q}^*$ é fechada, mas não é associativa, não é comutativa e não tem elemento neutro.

11. Mostre que o conjunto $G = \{-1, 1\}$ é um grupo com a operação de multiplicação.

12. Mostre que o conjunto $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ com a operação multiplicação definida por $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $kj = -i$, $ik = -j$ e $ji = -k$ (ou $i^2 = j^2 = k^2 = ijk = -1$), é um grupo, chamado grupo dos quatérnios .

13. Mostre que o conjunto $D_3 = \{e, \rho, \rho^2, \phi, \rho\phi, \rho^2\phi\}$, onde $\rho^3 = e$, $\phi^2 = e$ e $\phi\rho = \rho^2\phi$, é um grupo, chamado grupo diedral de ordem 6.

14. Mostre que o conjunto $D_4 = \{e, \rho, \rho^2, \rho^3, \phi, \rho\phi, \rho^2\phi, \rho^3\phi\}$, onde $\rho^4 = e$, $\phi^2 = e$ e $\phi\rho = \rho^3\phi$, é um grupo chamado grupo diedral de ordem 8.

15. Seja S um conjunto não vazio. Uma *permutação* de S é uma bijeção de S em S. Mostre que o conjunto $B(S)$ das bijeções de S em S munido da operação composição de funções é um grupo, chamado *grupo das permutações* de S.

16. Seja $S = \{1, 2, \cdots, n\}$.

   (a) Mostre que $B(S) = S_n$ é um grupo (chamado *grupo simétrico de grau n* (ou grupo de permutações de n elementos) cuja ordem é $n!$).

   (b) Determine os elementos de S_2.

   (c) Determine os elementos de S_3.

17. Seja o conjunto $G = M_n(\mathbb{A})$, onde $\mathbb{A} = \mathbb{Q}$ ou $\mathbb{R}$, das matrizes quadradas de ordem n.

   (a) Mostre que G munido com a operação de adição usual de matrizes é um grupo abeliano.

(b) Mostre que G munido com a operação de multiplicação usual de matrizes não é um grupo.

18. Seja $A = \{f : [0,1] \to \mathbb{R} : f \text{ é bijetora}\}$ com as operações de soma e produto definidas por $(f+g)(x) = f(x) + g(x)$ e $(fg)(x) = f(x)g(x)$, para todo $x \in [0,1]$. Verifique se A é um anel.

19. Seja A um anel. Se $a^2 = a$, para todo $a \in A$, mostre que $a = -a$, para todo $a \in A$, e que A é comutativo.

20. Seja E um conjunto não vazio. Considere no conjunto das partes $\mathcal{P}(E)$ as seguintes operações $x \triangle y = (x \cup y) - (x \cap y)$ e $x * y = x \cap y$. Mostre que $(\mathcal{P}(E), \triangle, *)$ é um anel comutativo com unidade.

21. Mostre que os números racionais $\mathbb{Q}$ com as operações $a \oplus b = a + b - 1$ e $a \odot b = a + b - ab$, onde $a, b \in \mathbb{Q}$, é um anel.

22. Sejam A um anel de integridade e $a \in A$. Se $a^2 = 1$, mostre que $a = 1$ ou $a = -1$.

23. Sejam A um anel de integridade e $a \in A$. Se $a^2 = a$, mostre que $x = 0$ ou $x = 1$.

24. Seja A um anel com unidade tal que $a^2 = a$ para todo $a \in A$. Mostre que A é um anel de integridade se, e somente se, $A = \{0, 1\}$.

25. Mostre que todo elemento não nulo de $\mathbb{Z}_n$ é uma unidade ou um divisor de zero.

11.2 Anel de Boole

O termo anel booleana é uma homenagem a George Boole, um matemático inglês autodidata. Boole introduziu o sistema algébrico, inicialmente, em um pequeno panfleto, o The Mathematical Analysis of Logic, publicado em 1847, em resposta a uma controvérsia em curso entre Augustus De Morgan e William Hamilton, e mais tarde como um livro mais substancial, The Laws of Thought, publicado em 1854. A formulação de Boole difere das descritas acima em alguns aspectos importantes. Por exemplo, a conjunção e a disjunção em Boole não era um duplo par de operações.

Definição 11.2.1. *Um anel A com as operações de adição e multiplicação é chamado um anel de Boole (ou anel booleano) se é unitário e idempontente, isto é, existe $1 \in A$ e $a^2 = a$, para todo $a \in A$.*

Exemplo 11.2.1. *O anel $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ é um anel booleano com as operações de soma e produto módulo 2.*

Exemplo 11.2.2. *O anel $A^n = \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ com as operações $(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$ e $(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n)$, onde $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in A^n$, é um anel booleano. Os elementos neutros da adição e da multiplicação são dados, respectivamente, por $0 = (0, 0, \ldots, 0)$ e $1 = (1, 1, \ldots, 1)$. O inverso de $a = (a_1, a_2, \ldots, a_n)$ é dado por $-a = (-a_1, -a_2, \ldots, -a_n)$.*

Exemplo 11.2.3. *Seja E um conjunto não vazio. O conjunto das partes de E, $\mathcal{P}(E)$, com as operações $a+b=(a\cup b)-(a\cap b)$ e $ab=a\cap b$, para todo $a,b\in\mathcal{P}(E)$, onde $\cup$ e $\cap$ são a união e a interseção de conjuntos, respectivamente, é um anel booleano.*

Proposição 11.2.1. *Um anel booleano A é comutativo e $-a=a$, para todo $a\in A$.*

Demonstração. Sejam $a,b\in A$. Por hipótese, segue que $a+b=(a+b)^2=(a+b)(a+b)=a^2+ab+ba+b^2=a+ab+ba+b$, ou seja, $a+b=a+ab+ba+b$. Agora, cancelando a e b de ambos os lados, segue que $ab+ba=0$. Somando $-ba$ em amos os lados, segue que $ab=-ba$. Fazendo $b=1$, segue que $a=-a$, para todo $a\in A$. Fianlmente, $ab=-(ba)=(-b)a=ba$, ou seja, $ab=ba$ para todo $a,b\in A$. □

Definição 11.2.2. *Seja A um anel booleano.*

1. *O complemento de um elemento $a\in A$ é definido por $\overline{a}=a+1$.*
2. *A união de $a,b\in A$ é definida por $a\oplus b=a+b+ab$.*

Observação 11.2.1. *Seja A um anel booleano. Assim, $a=-a$ e $a^2=a$, para todo $a\in A$. Para todo $a,b,c\in A$ vale às seguintes propriedades:*

1. $0\oplus 0=0$, *uma vez que*
$$0\oplus 0=0+0+0.0=0.$$
2. $0\oplus 1=1\oplus 0=1$, *uma vez que*
$$0\oplus 1=0+1+0.1=1+0+1.0=1.$$
3. $1\oplus 1=1$, *uma vez que* $1=-1$ *e*
$$1\oplus 1=1+1+1.1=1+(-1)+1=0+1=1.$$
4. $a\oplus b=b\oplus a$, *uma vez que*
$$a\oplus b=a+b+ab=b+a+ba=b\oplus a.$$
5. $a\oplus(b\oplus c)=(a\oplus b)\oplus c$, *uma vez que*
$$\begin{aligned} a\oplus(b\oplus c) &= a\oplus(b+c+bc)=a+b+c+bc+a(b+c+bc)\\ &= a+b+c+bc+ab+ac+abc \end{aligned}$$
e
$$\begin{aligned} (a\oplus b)\oplus c &= (a+b+ab)\oplus c=a+b+ab+c+(a+b+ab)c\\ &= a+b+ab+c+ac+bc+abc. \end{aligned}$$

6. $a(b \oplus c) = ab \oplus ac$, *uma vez que* $a^2 = 2$, *para todo* $a \in A$,

$$a(b \oplus c) = a(b + c + bc) = ab + ac + abc$$
$$ab \oplus ac = ab + ac + (ab)(ac) = ab + ac + a^2bc = ab + ac + abc.$$

7. $a \oplus (bc) = (a \oplus b)(a \oplus c)$, *uma vez que* $a^2 = a$ *e* $a = -a$, *para todo* $a \in A$, $a \oplus bc = a + bc + abc$ *e*

$$\begin{aligned}(a \oplus b)(a \oplus c) &= (a + b + ac)(a + c + ac) \\ &= a^2 + ac + a^2c + ba + bc + abc + a^2c + ac^2 + a^2c^2 \\ &= a + ac + ac + ab + bc + abc + ac + ac + ac = a + bc + abc.\end{aligned}$$

8. $a \oplus a = a$, *uma vez que*

$$a \oplus a = a + a + a^2 = a.$$

9. $a \oplus 0 = a$, *uma vez que*

$$a \oplus 0 = a + 0 + a.0 = a.$$

10. $a \oplus 1 = 1$, *uma vez que*

$$a \oplus 1 = a + 1 + a.1 = a + 1 + a = 1.$$

11. $a \oplus \overline{a} = 1$, *uma vez que*

$$a \oplus \overline{a} = a \oplus (a + 1) == a + a + 1 + a(a + 1) = 1 + a^2 + a = 1 + a + a = 1.$$

12. $a\overline{a} = 0$, *uma vez que*

$$a\overline{a} = a(a + 1) = a^2 + a = a + a = 0.$$

13. $\overline{a \oplus b} = \overline{a}\overline{b}$, *uma vez que*

$$\overline{a \oplus b} = (a \oplus b) + 1 = (a + b + ab) + 1$$

e

$$\overline{a}\overline{b} = (a + 1)(b + 1) = a + b + ab + 1.$$

14. $\overline{ab} = \overline{a} \oplus \overline{b}$, *uma vez que* $\overline{ab} = ab + 1$ *e*

$$\begin{aligned}\overline{a} \oplus \overline{b} &= (a + 1) \oplus (b + 1) = a + 1 + b + 1 + (a + 1)(b + 1) \\ &= a + b + ab + a + b + 1 = ab + 1.\end{aligned}$$

15. $\overline{\overline{a}} = a$, *uma vez que*

$$\overline{\overline{a}} = \overline{a + 1} = (a + 1) + 1 = a.$$

16. $a \oplus b = a\overline{b} \oplus \overline{a}b$, *uma vez que* $a \oplus b = a + b + ab$ *e*

$$\begin{aligned} a\overline{b} \oplus \overline{a}b &= a(b+1) \oplus (a+1)b = a(b+1) + (a+1)b + a(b+1)(a+1)b \\ &= ab + a + ab + b + ab(ab + a + b + 1) \\ &= a + b + a^2b^2 + a^2b + ab^2 + ab = a + b + ab + ab + ab = a + b + ab. \end{aligned}$$

11.2.1 Exercícios

1.

11.3 Álgebra de Boole

A álgebra de Boole surgiu na década de 1860, em artigos escritos por William Jevons e Charles Sanders Peirce. A primeira apresentação sistemática de álgebra booleana e reticulados foi dada por Vorlesungen de Ernst Schröder em 1890. O primeiro tratamento extensivo de álgebra de Boole foi dado em 1898 na Universal Algebra de Whitehead. A próxima definição é em homenagem a Huntington dada em 1904.

Definição 11.3.1. *Um conjunto não vazio* A *com as operações binárias de adição e multiplicação é uma álgebra de Boole (ou álgebra booleana) se*

A_1 *:* $ab = ba$*, para todo* $a, b \in A$*, ou seja, é comutativa.*

A_2 *:* A *possui elemento neutro em relação a adição e a multiplicação, denotado por* 0 *e* 1*, respectivamente. Assim,* $a + 0 = a$ *e* $a.1 = a$*, para todo* $a \in A$*.*

A_3 *:* $(a+b)c = ac+bc$ *e* $a+bc = (a+b)(a+c)$*, para todo* $a, b, c \in A$*, ou seja, vale a distributiva. Neste caso,* $a(b + c) = ab + ac$*, uma vez que* $a(b + c) \overset{A_1}{=} (b + c)a = ba + ca \overset{A_1}{=} ab + ac$*.*

A_4 *: Para todo* $a \in A$ *existe um elemento* $\overline{a} \in A$ *tal que* $a + \overline{a} = 1$ *e* $a\overline{a} = 0$*, ou seja, existe o complemento de* a*, denotado por* $\overline{a}$*.*

Exemplo 11.3.1. *Seja* E *um conjunto não vazio. O conjunto* $\mathcal{P}(E)$ *com as operações de união e interse cão é uma álgebra booleana, onde* $0 = \emptyset$*,* $1 = E$ *e* $\overline{a} = E - a$*.*

Definição 11.3.2. *Seja* p *uma proposição. A proposição dual de* p *é uma proposição* q *obtida de* p *da segunte maneira:*

1. *trocando* $+$ *por* $\cdot$ *e vice-versa,*
2. *e trocando* 0 *por* 1 *e vice-versa.*

Exemplo 11.3.2. *O dual de* $a + ab = a$ *é* $a(a + b) = a$*. O dual de* $0 + a = a$ *é* $1.a = a$*. O dual de* $1.a = a$ *é* $0 + a = a$*.*

Sejam A uma álgebra booleana e $a, b, c \in A$. Assim, por A_4, segue que existe $\overline{a}$ tal que $a + \overline{a} = 1$ e $a\overline{a} = 0$. Neste caso, vale às seguintes propriedades.

1. P_1: (Idempotência da soma): $a + a = a$, uma vez que

$$a \overset{A_2}{=} a + 0 \overset{A_4}{=} a + a\overline{a} \overset{A_3}{=} (a + a)(a + \overline{a}) \overset{A_4}{=} (a + a).1 \overset{A_2}{=} a + a.$$

2. P_2: (Idempotência do produto): $aa = a$, uma vez que

$$a \overset{A_1}{=} a.1 \overset{A_4}{=} a(a + \overline{a}) \overset{A_3}{=} aa + a\overline{a} \overset{A_4}{=} aa + 0 \overset{A_2}{=} aa.$$

3. P_3: $a + 1 = 1$, uma vez que

$$a + 1 \overset{A_2}{=} (a + 1).1 \overset{A_4}{=} (a + 1)(a + \overline{a}) \overset{A_3}{=} a + 1.\overline{a} \overset{A_2}{=} a + \overline{a} \overset{A_4}{=} 1.$$

4. P_4: (Absorção) $a + ab = a$, uma vez que

$$a + ab \overset{A_2}{=} a.1 + ab \overset{A_3}{=} a(1 + b) \overset{P_3}{=} a.1 \overset{A_2}{=} a.$$

5. P_5: (Absorção) $a(a + b) = a$, uma vez que

$$a(a + b) \overset{A_3}{=} aa + ab \overset{P_2}{=} a + ab \overset{P_4}{=} a.$$

Lema 11.3.1. *Se $a, b, c \in A$, então $a + a(bc) = a + (ab)c$.*

Demonstração. Se $a, b, c \in A$, então

$$\begin{aligned} a + a(bc) &\overset{P_4}{=} a \overset{P_5}{=} a(a + c) \overset{P_4}{=} (a + ab)(a + c) \\ &\overset{A_3}{=} a + (ab)c, \end{aligned}$$

o que prova o lema. □

Lema 11.3.2. *Se $a, b, c \in A$, então $\overline{a} + a(bc) = \overline{a} + (ab)c$.*

Demonstração. Se $a, b, c \in A$, então

$$\begin{aligned} \overline{a} + a(bc) &\overset{A_3}{=} (\overline{a} + a)(\overline{a} + bc) \overset{A_4}{=} 1.(\overline{a} + bc) \overset{A_2}{=} \overline{a} + bc \overset{A_3}{=} (\overline{a} + b)(\overline{a} + c) \\ &\overset{A_2}{=} [(\overline{a} + b).1](\overline{a} + c) \overset{A_4}{=} [(\overline{a} + b)(\overline{a} + a)](\overline{a} + c) \\ &\overset{A_3}{=} (\overline{a} + ba)(\overline{a} + c) \overset{A_1}{=} (\overline{a} + ab)(\overline{a} + c) \overset{A_3}{=} \overline{a} + (ab)c, \end{aligned}$$

o que prova o lema. □

Proposição 11.3.1. *Se $a, b, c \in A$, então $a(bc) = (ab)c$.*

Demonstração. Pelos Lemas 11.3.1 e 11.3.2, segue que

$$a + a(bc) = a + (ab)c \quad \text{e} \quad \overline{a} + a(bc) = \overline{a} + (ab)c.$$

Agora, multiplicando, membro a membro essas igualdades, segue que

$$[a + a(bc)][\overline{a} + a(bc)] = [a + (ab)c][\overline{a} + (ab)c].$$

Por A_3, segue que

$$a\overline{a} + (ab)c = a\overline{a} + (ab)c.$$

Por A_4, segue que

$$0 + a(bc) = 0 + (ab)c.$$

Por A_2, segue que

$$a(bc) = (ab)c,$$

o que prova a proposição. □

Proposição 11.3.2. *Se $a, b, c \in A$, então $a + (b + c) = (a + b) + c$.*

Demonstração. Pela Proposição 11.3.1, segue que $a(bc) = (ab)c$. Agora, aplicando o processo da dualidade, Definição 11.3.2, segue que $a + (b + c) = (a + b) + c$. □

Corolário 11.3.1. *Se $a \in A$, então $a.0 = 0$.*

Demonstração. Se $a \in A$, então

$$a.0 \overset{A_4}{=} a(a\overline{a}) \overset{\text{Proposição } 11.3.1}{=} (aa)\overline{a} \overset{P_2}{=} a\overline{a} \overset{A_4}{=} 0,$$

o que prova o corolário. □

Proposição 11.3.3. *Seja A uma álgebra booleana. Se $a \in A$, então o elemento $\overline{a}$ é único.*

Demonstração. Pela Definição 11.3.1, seque que existe $\overline{a} \in A$ tal que $a + \overline{a} = 1$ e $a\overline{a} = 0$. Suponhamos que existem $b, c \in A$ tal que $a + b = 1$, $ab = 0$, $a + c = 1$ e $ac = 0$. Assim,

$$b \overset{A_2}{=} b.1 = b(a + c) \overset{A_3}{=} ba + bc \overset{A_1}{=} ab + bc = 0 + bc = ac + bc \overset{A_3}{=} (a + b)c = 1.c \overset{A_2}{=} c.$$

Portanto, $b = c$, o que prova a unicidade. □

Corolário 11.3.2. *Seja A uma álgebra booleana. Se $a \in A$, então $\overline{(\overline{a})} = a$.*

Demonstração. Pela Definição 11.3.1, seque que existem $\overline{a}, \overline{(\overline{a})} \in A$ tal que $a + \overline{a} = \overline{a} + \overline{(\overline{a})} = 1$. Pela Proposição 11.3.3, unicidade do complemento de $\overline{a}$, segue que $a = \overline{(\overline{a})}$. □

Corolário 11.3.3. *Se A é uma álgebra booleana, então $\overline{0} = 1$ e $\overline{1} = 0$.*

Demonstração. Pela Definição 11.3.1, seque que $a+0=a$ e $a+\overline{a}=1$, para todo $a\in A$. Assim, $\overline{0}=0+\overline{0}=1$. Agora, como $\overline{0}=1$, pelo Corolário 11.3.2, segue que $0=\overline{(\overline{0})}=\overline{1}=1$. □

Proposição 11.3.4. *Seja A uma álgebra booleana. Se $a,b\in A$, então $\overline{ab}=\overline{a}+\overline{b}$.*

Demonstração. Se $a,b\in A$, então

$$ab+\overline{a}+\overline{b}\overset{A_3}{=}(a+\overline{a}+\overline{b})(b+\overline{a}+\overline{b})\overset{A_4}{=}(1+\overline{b})(1+\overline{a})\overset{P_2}{=}1.1\overset{A_2}{=}1$$
$$ab(\overline{a}+\overline{b})\overset{A_3}{=}ab.\overline{a}+ab.\overline{b}\overset{A_1}{=}a\overline{a}.b+a.b\overline{b}\overset{A_4}{=}0.b+a.0\overset{Prop.\ 11.3.1}{=}0+0\overset{A_2}{=}0.$$

Pela Definição 11.3.1 e Proposição 11.3.3, segue que $\overline{ab}=\overline{a}+\overline{b}$. □

Proposição 11.3.5. *Seja A uma álgebra booleana. Se $a,b\in A$, então $\overline{a+b}=\overline{a}\overline{b}$.*

Demonstração. Se $a,b\in A$, então

$$(a+b)\overline{a}\overline{b}\overset{A_3}{=}a(\overline{a}\overline{b})+b(\overline{a}\overline{b})\overset{A_1}{=}(a\overline{a})\overline{b}+\overline{a}(b\overline{b})\overset{A_4}{=}a.0+b.0\overset{Prop.\ 11.3.1}{=}0+0\overset{A_2}{=}0\quad\text{e}$$

$$\begin{aligned}(a+b)+(\overline{a}\overline{b})&\overset{A_3}{=}(a+b+\overline{a})(a+b+\overline{b})\overset{A_4}{=}(1+b)(1+a)\\&\overset{A_3}{=}1+ab\overset{A_4}{=}a+\overline{a}+ab\overset{A_3}{=}a(1+b)+\overline{a}\overset{P_3}{=}a+\overline{a}\overset{A_4}{=}1.\end{aligned}$$

Pela Definição 11.3.1 e Proposição 11.3.3, segue que $\overline{a+b}=\overline{a}\overline{b}$. □

11.3.1 Exercícios

1.

11.4 Ordem de Boole

Sejam A uma álgebra de Boole e $a,b\in A$. A relação

$$aRb \text{ se, e somente se, } a+b=b$$

é uma relação de ordem.

1. Reflexiva: aRa, para todo $a\in A$, uma vez que $a+a=a$, para todo $a\in A$, pela Propriedade P_1.
2. Anti-simétrica: Se aRb e bRa, então $a+b=b$ e $b+a=a$. Assim, $a=b+a=a+b=b$, ou seja, R é anti-simétrica.
3. Transitiva: Se aRb e bRc, então $a+b=b$ e $b+c=c$. Logo, $a+c=a+(b+c)=(a+b)+c=b+c=c$, ou seja, aRc.

Portanto, R é uma relação de ordem.

Proposição 11.4.1. *Sejam $a, b \in A$. São equivalentes.*

1. $ab = a$.
2. $a + b = b$.
3. $\overline{a} + b = 1$.
4. $a\overline{b} = 0$.

Demonstração. Para (1) implica (2), $a + b \overset{(1)}{=} ab + b \overset{A_3}{=} (a + 1)b \overset{P_3}{=} 1.b \overset{A_2}{=} b$. Para (2) implica (3), $\overline{a} + b \overset{(2)}{=} \overline{a} + (a + b) \overset{Prop.11.3.2}{=} (\overline{a} + a) + b \overset{A_4}{=} 1 + b \overset{P_3}{=} 1$. Para (3) implica (4), $a\overline{b} \overset{Prop.11.3.2}{=} \overline{\overline{a\overline{b}}} \overset{Prop.11.3.4}{=} \overline{\overline{a} + \overline{\overline{b}}} \overset{Prop.11.3.2}{=} \overline{\overline{a + b}} \overset{hip.}{=} \overline{1} \overset{Prop.11.3.3}{=} 0$. Para (4) implica (1), $ab \overset{A_2}{=} ab + 0 \overset{(4)}{=} ab + a\overline{b} \overset{A_3}{=} a(b + \overline{b}) \overset{A_4}{=} a.1 \overset{A_2}{=} a$. □

Corolário 11.4.1. *Se aRb e bRa, então $a = b$.*

Demonstração. Pela Proposição 11.4.1, segue que $ab = a$ e $ba = b$. Por A_1, segue que $a = ab = ba = b$. □

Observação 11.4.1. *Pela definição da relação de ordem R e a Proposição 11.4.1, segue que R é ua relação de ordem se satisfaz uma das condições da Proposição 11.4.1.*

Exemplo 11.4.1. *Sejam E um conjunto não vazio e a álgebra booleana $(\mathcal{P}(E), \cup, \cap)$. Pela Definição da relação de ordem R e da Proposição 11.4.1, segue que aRb se, e somente se, $a \cap b = a$ se, e somente se, $a \subseteq b$.*

Exemplo 11.4.2. *O anel $A^n = \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ com as operações $(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$ e $(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n)$, onde $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in A^n$, é um anel booleano. Pela Definição da relação de ordem R e da Proposição 11.4.1, segue que aRb se, e somente se, $ab = a$ se, e somente se, $(a_1b_1, a_2b_2, \ldots, a_nb_n) = (a_1, a_2, \ldots, a_n)a$ se, e somente se, $a_ib_i = a_i$, para todo $i = 1, 2, \ldots, n$. Portanto, aRb se, e somente se, a_iRb_i, para todo $i = 1, 2, \ldots, n$. Como $a_ib_i = 1$ se, e somente se, $a_i = b_i = 1$ se, e somente se, $a_i = b_i = 1$, para $i = 1, 2, \ldots, n$, segue que aRb se, e somente se, $a_i \leq b_i$, para todo $i = 1, 2, \ldots, n$.*

Proposição 11.4.2. *Sejam $a, b, c \in A$. Se aRb e aRc, então $aRbc$.*

Demonstração. Por definição de R e pela Proposição 11.4.1, segue que $ab = a$ e $ac = a$. Pela Proposição 11.3.1, segue que $a(bc) = (ab)c$. Assim, $a(bc) = ac = a$. Por definição de R e pela Proposição 11.4.1, segue que $aRbc$ □

Proposição 11.4.3. *Sejam $a, b, c \in A$. Se aRb e cRb, então $(a + c)Rb$.*

Demonstração. Por definição de R e pela Proposição 11.4.1, segue que $ab = a$ e $cb = c$. Por A_3, segue que $(a + c)b = ab + cb$. Assim, $(a + c)b = a + c$. Por definição de R e pela Proposição 11.4.1, segue que $(a + c)Rb$. □

Proposição 11.4.4. *Sejam $a, b, c \in A$. Se aRb, então $aR(b + c)$.*

Demonstração. Por definição de R e pela Proposição 11.4.1, segue que $ab = a$. Por A_3, segue que $a(b + c) = ab + ac$. Assim, $a(b + c) = a + ac \overset{A_3}{=} a(1 + c) \overset{P_3}{=} a.1 \overset{A_2}{=} a$. Por definição de R e pela Proposição 11.4.1, segue que $aR(b + c)$. □

Proposição 11.4.5. *Sejam $a, b, c \in A$. Se aRb, então $acRb$.*

Demonstração. Por definição de R e pela Proposição 11.4.1, segue que $ab = a$. Assim, $(ac)b \overset{A_1}{=} (ca)b \overset{Prop.11.3.1}{=} c(ab) = ca \overset{A_1}{=} ac$, ou seja, $(ac)b = ac$. Por definição de R e pela Proposição 11.4.1, segue que $acRb$. □

Proposição 11.4.6. *Sejam $a, b \in A$. Assim, aRb, se e somente se, $\overline{b}R\overline{a}$.*

Demonstração. Por definição de R e pela Proposição 11.4.1, segue que aRb se, e somente se, $\overline{a} + b = 1$. Assim, $0 \overset{Cor.11.3.3}{=} \overline{1} = \overline{\overline{a} + b} \overset{Prop.11.3.5}{=} \overline{(\overline{a})}\overline{b} \overset{A_1}{=} \overline{b}\overline{(\overline{a})}$. Por definição de R e pela Proposição 11.4.1, segue que $\overline{b}R\overline{a}$. □

Proposição 11.4.7. *Se $a \in A$, então $0Ra$ e $aR1$.*

Demonstração. Pelo Corolário 11.3.1 e A_1, segue que $a.0 = 0.a = 0$. Por definição de R e pela Proposição 11.4.1, segue que $0Ra$. Seja $a \in A$. Por A_2, segue que $a.1 = a$. Por definição de R e pela Proposição 11.4.1, segue que $aR1$. □

Proposição 11.4.8. *Se $a, b \in A$, então existe $sup\{a, b\}$ e $sup\{a, b\} = a + b$.*

Demonstração. Como aRa, pela Proposição 11.4.4, segue que $aR(a + b)$. De modo análogo, $bR(a + b)$. Portanto, $a + b$ é um limite superior de $\{a, b\}$. Agora, se m é um outro limite superior de $\{a, b\}$, ou seja, aRm e bRm, pela Proposição 11.4.3, segue que $(a+b)Rm$. Portanto, $a + b = sup\{a, b\}$. □

Proposição 11.4.9. *Se $a, b \in A$, então exist $inf\{a, b\}$ e $inf\{a, b\} = ab$.*

Demonstração. Como aRa e bRb, pela Proposição 11.4.5, segue que $abRa$ e $abRc$. Portanto, ab é um limite inferior de $\{a, b\}$. Agora, se m é um limite inferior de $\{a, b\}$, ou seja, mRa e mRb, pela Proposição 11.4.2, segue que $mRab$. Portanto, $ab = inf\{a, b\}$. □

Observação 11.4.2. *Sejam $x_1, x_2, \ldots, x_n \in A$, para $n \geq 1$, por indução sobre n, segue que*

$$\sum_{i=1}^{n} x_i = sup\{x_1, x_2, \ldots, x_n\} \quad e \quad \prod_{i=1}^{n} x_i = in\{x_1, x_2, \ldots, x_n\}.$$

11.4.1 Exercícios

1.

11.5 Teorema de Stone

Duas álgebras A e B são isomorfas se existe uma bijeção entre A e B que preserva as estruturas algébricas envolvidas, ou seja, adição, multiplicação e complementação.

Definição 11.5.1. *Um átomo em uma álgebra booleana A é um elemento $a \neq 0$ tal que se $0Rb$ e bRa, para todo $b \in A$, implicar que $b = 0$ ou $b = a$, ou seja, para todo $b \in A - \{0\}$, tem-se que $ab = 0$ ou $ab = a$.*

Em outras palavras, mediante a relação de ordem R, a Definição 11.5.1, significa que entre 0 e a não existe elemento.

Exemplo 11.5.1. *Seja E um conjunto não vazio. Os átomos da álgebra $(\mathcal{P}(E), \cup, \cap)$ são os conjuntos unitários, ou seja, $\{a\} \subseteq E$.*

Exemplo 11.5.2. *Os átomos de $(\mathbb{Z}_2^n, +, \cdot)$ são as n-uplas $(a_1, a_2, \ldots, a_n) \in \mathbb{Z}_2^n$ com exatamente um dos a_i igual a 1.*

Proposição 11.5.1. *Se a é um átomo e $aR(x_1 + x_2 + \cdots + x_n)$, então aRx_i, para algum i.*

Demonstração. Por definição de R e pela Proposição 11.4.1, segue que $a(x_1+x_2+\cdots+x_n) = a$. Pela Proposição 11.4.9, segue que $ax_i = inf\{a, x_i\}$, para todo $i = 1, 2, \ldots, n$. Assim, ax_iRa, para todo $i = 1, 2, \ldots, n$. Pela Proposição 11.4.7, segue que $0Rax_i$, para todo $i = 1, 2, \ldots, n$. Assim, $0Rax_i$ e ax_iRa, para todo $i = 1, 2, \ldots, n$. Como a é um átomo, segue que $ax_i = 0$ ou $ax_i = a$, para todo $i = 1, 2, \ldots, n$. Se $a \not R x_i$, ou seja, $ax_i \neq a$, para todo $i = 1, 2, \ldots, n$, segue que $ax_i = 0$, para todo $i = 1, 2, \ldots, n$. Como $a = a(x_1 + x_2 + \cdots + x_n) \overset{A_3}{=} ax_1 + ax_2 + \cdots + ax_n$ e $ax_i = 0$, para todo $i = 1, 2, \ldots, n$, segue que $a = 0$, o que não ocorre. Portanto, aRx_i, para algum i. □

Proposição 11.5.2. *Se a é um átomo, então aRb ou $aR\overline{b}$ (exclusivo), para todo $b \in A$.*

Demonstração. Suponha que $a \not R b$, ou seja, $ab \neq a$. Como a é um átomo, segue que $ab = 0$. Pela Proposição 11.3.2, segue que $b = \overline{\overline{b}}$. Assim, $a(\overline{b}) = 0$. Pela Proposição 11.4.1, segue que $aR\overline{b}$. □

Definição 11.5.2. *Uma álgebra booleana A é chamada atômica se para todo elemento não $b \in A$, existe um átomo $a \in A$ tal que aRb.*

Proposição 11.5.3. *Se A é uma álgebra booleana finita, então A é atômica.*

Demonstração. Seja $b \in A$, com $b \neq 0$. Se b não é um átomo, então existe $b_1 \in A$ tal que $b \neq b_1$, $0Rb_1$ e b_1Rb, e portanto, $bb_1 = b_1$. Se b_1 é um átomo, segue que A é atômica. Se b_1 não é um átomo, então existe $b_2 \in A$ tal que $b_1 \neq b_2$, $0Rb_2Rb_1Rb$. Assim, $b_2 = b_2b_1 = b_2b_1b$. Se b_2 é um átomo, segue que A é atômica. Se b_2 não é um átomo, então continuando com o mesmo raciocínio, segue que existe uma cadeia finita $0Rb_nRb_{n-1}R \ldots Rb_1Rb_0 = b$, onde $n \geq 1$ e $b_k = b_kb_{k-1} \ldots b_1b_0$, para $k = 1, 2, \ldots, n$. Como A é finita, segue que existe um b_n que seja um átomo. □

Sejam A uma álgebra booleana atômica e $S = \{a_i : i \in I\}$ o conjunto de todos os átomos de A.

Proposição 11.5.4. *Se $x \in A$ e $T_x = \{t \in A : t \in S \text{ e } tRx\}$, então*

1. $x = \sum_{t \in T_x} t$, *e*
2. *nenhuma outra soma de átomos é igual a x.*

Demonstração. Para (1), por definição de T_x, segue que x é um limite superior de T_x. Pela Observação 11.4.2, segue que $sup(T_x) = \sum_{t \in T_x} t$ e $sup(T_x)Rx$. Suponha que $sup(T_x) \neq x$. Pelo Corolário 11.4.1, segue que $x \not R sup(T_x)$. Pela Proposição 11.4.1, segue que $x\overline{sup(T_x)} \neq 0$. Como A é atômica, segue que existe um átomo $a \in A$ tal que $aRx\overline{sup(T_x)}$. Pela Proposição 11.4.9, segue que $x\overline{sup(T_x)} = inf\{x, \overline{sup(T_x)}\}$, e deste modo, aRx e $a R\overline{sup(T_x)}$. Pela Proposição 11.5.2, segue que aRx e $a \not R sup(T_x)$, ou seja, $a \in T_x$ e a não está incluído na soma $\sum_{t \in T_x} t$, o que é um absurdo. Portanto, $x = sup(T_x) = \sum_{t \in T_x} t$. Para (2), se existe uma outra soma de átomos dada por $x = \sum_{u \in U} u$, onde $U \subseteq S$, então existe $t_0 \in T_x - U$ ou $u_0 \in U - T_x$, ou seja, $t_0 Rx$ ou $u_0 Rx$. Assim, $t_0 = t_0 x = t_0(\sum_{t \in T_x} t) = t_0(\sum_{u \in U} u) = \sum_{u \in U} t_0 u = 0 + 0 + \cdots + 0 = 0$, pois 0 é o ínfimo de dois átomos distintos, ou $u_0 = u_0 x = u_0(\sum_{u \in U} u) = \sum_{t \in T_x} t) = \sum_{u \in U} t_0 t = 0 + 0 + \cdots + 0 = 0$. Em ambos os casos é uma contradição. □

Corolário 11.5.1. *Se $x \in A$, então $x = \sum_{i \in I} \alpha_i a_i$, onde $\alpha_i \in \{0, 1\}$. Além disso, $\alpha_i = 1$ se, e somente se, $a_i Rx$. Em particular, $\sum_{i \in I} a_i = 1$. Finalmente, essa estrutura como soma de átomos de A é única.*

11.5.1 Exercícios

1.

Referências Bibliográficas

[1] Alencar Filho, E.; *Teoria elementar dos números*, Editora Nobel, São Paulo - SP, 1985.

[2] Andrade, A. A.; *Uma introdução às estruturas algébricas*, amazon.com, São José do Rio Preto - SP, 2002.

[3] Andrade, A. A.; *Uma introdução à teoria elementar dos números*, amazon.com, São José do Rio Preto - SP, 2022.

[4] Coutinho, S.C.; *Números inteiros e criptografia RSA*, Série Computação e Matemática, IMPA, Rio de Janeiro - RJ, 2001.

[5] Domingues, H. H.; *Fundamentos da Aritmética*, Atual Editora, São Paulo - SP, 1991.

[6] Hefez, A.; *Elementos de aritmética*, Sociedade Brasileira de Matemática, IMPA, Rio de Janeiro - RJ, 2005.

[7] Lemos, M.; *Criptografia, números primos e algoritmos*, 17^o Colóquio Brasileiro de Matemática, IMPA, Rio de Janeiro - RJ, 1989.

[8] Masuda, A. M., Panario, D.; *Tópicos de corpos finitos com aplicações em criptografia e teoria de códigos*, 26^o Colóquio Brasileiro de Matemática, IMPA, Rio de Janeiro - RJ, 2007.

[9] Silva, A. F e Santos, C. M.; *Aspectos formais da computação*, Cultura Acadêmica Editora, Unesp, São Paulo - SP, 2009.

Índice Remissivo