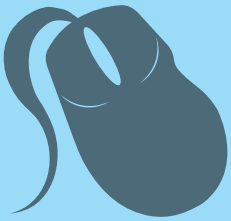


Computação

Matemática Discreta

Raquel Montezuma Pinheiro Cabral

Ed UECE

Geografia

História

Educação Física

Química

Ciências Biológicas

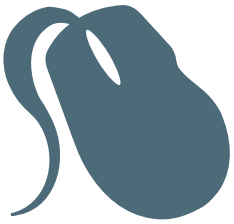
Artes Plásticas

Computação

Física

Matemática

Pedagogia



Computação

Matemática Discreta

Raquel Montezuma Pinheiro Cabral

1ª edição
Fortaleza - Ceará

Ed UECE

2017

Geografia

História

Educação Física

Química | Ciências Biológicas | Artes Plásticas | Computação | Física | Matemática | Pedagogia

Editora Filiada à

ASSOCIAÇÃO BRASILEIRA DAS EDITORAS UNIVERSITÁRIAS

Dados Internacionais de Catalogação na Publicação
Sistema de Bibliotecas
Biblioteca Central Prof. Antônio Martins Filho
Meirilane Santos de Morais Bastos – CRB-3 / 785
Bibliotecária

C117m Cabral, Raquel Montezuma Pinheiro.
Matemática discreta / Raquel Montezuma Pinheiro Cabral. – Fortaleza, Ce: EDUECE, 2017.
81 p. : il; 20,0 x 25,5cm – (Computação)

Inclui referências.

ISBN: 978-85-7826-570-0

1. Computação – Matemática. 2. Modelos matemáticos. 3. Computação – Matemática discreta. I. Título.

CDD : 004.0151

Editora da Universidade Estadual do Ceará – EdUECE
Av. Dr. Silas Munguba, 1700 – Campus do Itaperi – Reitoria – Fortaleza – Ceará
CEP: 60714-903 – Fone: (85) 3101-9893
Internet: www.uece.br – E-mail: eduece@uece.br

Secretaria de Apoio às Tecnologias Educacionais
Fone: (85) 3101-9962

Sumário

Apresentação

Este material foi produzido para a Disciplina de Matemática Discreta, do Curso de Licenciatura em Computação, ofertado a distância pela Universidade Aberta do Brasil/UECE e tem como objetivo oferecer subsídios para orientar os estudos dos alunos e facilitar sua aprendizagem.

A Matemática discreta provê uma série de técnicas para a modelagem de problemas da Ciência da Computação, estudando, principalmente, conjuntos contáveis, finitos ou infinitos, como Naturais, Inteiros e Racionais. Compreendemos que as demonstrações de teoremas são de grande importância na Matemática, oferecendo melhor compreensão e comprovação do que foi afirmado. Apresentaremos neste material os principais conceitos e resultados da Matemática Discreta, utilizando uma linguagem simples e acessível, objetivando que o estudante possa desenvolver o raciocínio abstrato e aplicar os conceitos básicos de Matemática Discreta na solução de problemas.

Os conceitos aqui apresentados são úteis para estudantes do Curso de Licenciatura em Computação e indicamos uma bibliografia complementar para aqueles que desejarem aprofundar seus estudos.

Este material foi elaborado com muito cuidado, para que possa ajudar ao estudante a construir conhecimentos e utilizá-los sempre que necessitar.

A autora

Capítulo 1

Teoria dos Conjuntos

Objetivos

- Conhecer a noção e a representação de conjuntos;
- Reconhecer os símbolos que permitem relacionar elementos a conjuntos e conjuntos a conjuntos;
- Operar com conjuntos e conhecer as principais propriedades das operações.

É de fundamental importância conhecer a linguagem dos conjuntos e suas operações, pois praticamente todos os conceitos desenvolvidos em computação e informática são baseados em conjuntos e suas construções.

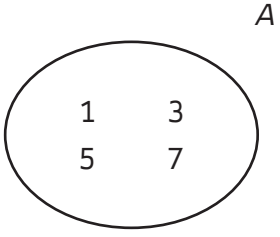
1. Noções de conjuntos

Definição: Um conjunto é uma coleção de objetos distintos. Os objetos que fazem parte do conjunto são chamados de elementos, não importando a ordem em que se apresentam.

Podemos representar um conjunto utilizando chaves ou diagrama de Venn.

Exemplo 1: Representamos os elementos do conjunto entre chaves e no diagrama de Venn:

$A = \{1,3,5,7\}$



O conjunto que não possui elementos é chamado de conjunto vazio e representado por { } ou ∅. O conjunto que possui apenas um elemento é chamado de conjunto unitário. Denominamos de conjunto universo ao conjunto que possui todos os elementos com uma determinada propriedade.

Exemplo 2: Seja $M = \{x \mid x$ é mês do ano que começa com a letra $z\}$, o conjunto M é vazio, ou seja, $M = \{\ \}$ ou ∅.

Quando não deixar dúvidas, podemos escrever os conjuntos utilizando reticências ou uma condição.

Exemplo 3: $P = \{x \mid x$ é um número primo$\}$ e lemos: conjunto de elementos x tal que x é um número primo, ou seja, $P = \{2, 3, 5, 7, 11, ...\}$.

A quantidade de elementos de um conjunto A é chamada de cardinalidade e representaremos por $n(A)$.

Exemplo 4: O conjunto $A = \{1, 3, 5, 7\}$ tem cardinalidade 4 e o conjunto $P = \{2, 3, 5, 7, 11, ...\}$ tem cardinalidade infinita.

Para refletir

1. Descreva os elementos dos conjuntos e indique sua cardinalidade:
   a) $A = \{x \mid x$ é mês do ano$\}$
   b) $B = \{x \mid x$ é dia da semana$\}$
   c) $C = \{x \mid x$ é múltiplo positivo de 6$\}$
   d) $D = \{x \mid x$ é divisor positivo de 12$\}$

2. Relações de pertinência e inclusão

Podemos relacionar elementos com conjuntos utilizando a condição de estarem presentes no conjunto ou não, essa relação é chamada de pertinência e utilizamos os símbolos $\in$ e lemos que o elemento pertence ao conjunto ou $\notin$ e lemos não pertence.

Exemplo 5: Seja $A = \{x \mid x$ é par$\}$, então podemos dizer que $2 \in A$ e $5 \notin A$.

Dados dois conjuntos A e B, dizemos que A é um subconjunto de B se todo elemento que pertence ao conjunto A também pertence ao conjunto B, utilizamos a notação $A \subset B$, lemos A está contido em B, ou $B \supset A$, lemos B contém A.

Exemplo 6: Sejam $A = \{0,2,4,6\}$ e $B = \{0,1,2,3,4,5,6,7,8,9,10\}$, podemos dizer que $A \subset B$ ou $B \supset A$.

Se existir um elemento do conjunto A que não pertença ao conjunto B dizemos que A não é subconjunto de B e denotamos por $A \not\subset B$, lemos que A não está contido em B, ou $B \not\supset A$, lemos que B não contém A.

Exemplo 7: Sejam $A = \{0,2,4,6\}$ e $B = \{0,1,2,3,4,5\}$, podemos dizer que $A \not\subset B$ ou que $B \not\supset A$.

Note que para qualquer conjunto A, podemos dizer que $\emptyset \subset A$ ou $A \supset \emptyset$, ou seja $\emptyset$ é subconjunto de qualquer conjunto.

O conjunto $P(A)$ formado por todos os subconjuntos de um conjunto A é chamado de conjunto das partes de A ou conjunto potência e tem cardinalidade 2^n, onde n é o número de elementos do conjunto A, cuja demonstração apresentaremos no capítulo 4, usando-se o princípio de indução.

Exemplo 8: Considere o conjunto A ={ 2, 3, 5, 7} o conjunto das partes de A possui $n(P(A)) = 2^4 = 16$ elementos, que são:

$P(A)$ = {∅, {2}, {3}, {5}, {7}, {2, 3}, {2, 5}, {2, 7},{3, 5}, {3, 7}, {5, 7}, {2, 3, 5}, {2, 3, 7}, {2, 5, 7}, {3, 5, 7}, A}.

Dados dois conjuntos A e B dizemos que eles são iguais se A ⊂ B e B ⊂ A.

Exemplo 9: Os conjuntos A = {1, 2, 3} e B = {2, 1, 3} possuem os mesmos elementos, ou seja, $A = B$.

Exemplo 10: Seja A = {a, e, i, o, u} e B = {x | x é vogal} podemos dizer que $A = B$.

Para refletir

1. Analisando cada item a seguir, classifique as sentenças em verdadeiro (V) ou falso (F):
( ) 2 ∈ {0, 1, 2, 3, 4}
( ) {4} ∈ {0, 2, 4, 6}
( ) {2, 8} ⊄ {0, 2, 4, 6}
( ) ∅ ∈ {1, 2, 3}
( ) {1, 3, 5} ⊃ ∅
( ) {0} ⊂ {0, 1, 2}

2. Dado o conjunto A, que possui 7 elmentos, determine o número de elementos do conjunto das partes de A, que contém pelo menos dois elementos.

3. Considerando os conjuntos A = {5, 7, 9, 11, 13} e B = {1, 3, 5, 7, 9, 11, 13, 15}, assinale a alternativa correta:
   a) ∅ ⊄ A
   b) A ⊂ B
   c) A ⊃ B
   d) B ⊅ A
   e) 15 ∉ B

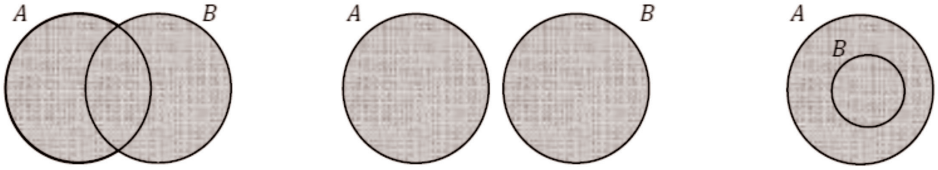
3. Operações entre conjuntos

Apresentamos nesta unidade as operações entre conjuntos: união, interseção, diferença, produto cartesiano e a diferença simétrica.

Definição: Dados dois conjuntos A e B, chamamos de união de A e B e denotamos por $A \cup B$, ao conjunto C que possui todos os elementos que pertencem a A e todos os elementos que pertencem a B e nenhum outro elemento que não esteja em um dos conjuntos.

$$A \cup B = C = \{x \mid x \in A \text{ ou } x \in B\}.$$

A união de dois conjuntos A e B pode ser representada no digrama de Venn:



Exemplo 11: Dados os conjuntos $A = \{0, 2, 4, 6, 8\}$ e $B = \{1, 2, 3, 4\}$, temos que:

$$A \cup B = \{0, 1, 2, 3, 4, 6, 8\}.$$

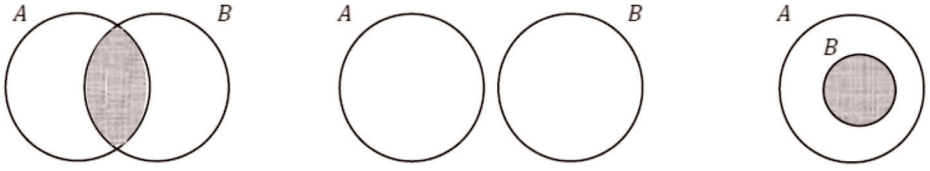
Propriedades: se A, B e C são conjuntos quaisquer, então valem as seguintes propriedades da união:

- $A \cup A = A$ (idempotente)
- $A \cup \emptyset = A$ (elemento neutro)
- $A \cup B = B \cup A$ (comutativa)
- $(A \cup B) \cup C = A \cup (B \cup C)$ (associativa).

Definição: Dados dois conjuntos A e B, chamamos de interseção de A e B ao conjunto C que possui todos os elementos que pertencem a A e pertencem a B e nenhum outro elemento que não esteja nos dois conjuntos. Representamos a interseção dos conjuntos A ∩ B por:

$$A \cap B = C = \{x \mid x \in A \text{ e } x \in B\}.$$

A interseção de dois conjuntos A e B pode ser representada no digrama de Venn:



Exemplo 12: Dados os conjuntos $A = \{0, 2, 4, 6, 8\}$ e $B = \{1, 2, 3, 4\}$, temos que:

$$A \cap B = \{2, 4\}.$$

Apresentamos agora algumas propriedades da interseção de conjuntos.

Propriedades: se A, B e C são conjuntos quaisquer, então valem as seguintes propriedades da interseção:

- $A \cap A = A$ (idempotente)
- $A \cap \emptyset = \emptyset$ (elemento neutro)

- $A \cap B = B \cap A$ (comutativa)
- $(A \cap B) \cap C = A \cap (B \cap C)$ (associativa).

Além dessas propriedades podemos, verificar que o número de elementos da união de dois conjuntos A e **B** é dada por:

$$n(A \cup B) = n(A) + n(B) - n(A \cap B).$$

Para três conjuntos A,B e C, temos que:

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C).$$

Utilizando o princípio de indução, que será apresentado no capítulo 4, poderemos estender essa conclusão para um número de elementos $n \in N$.

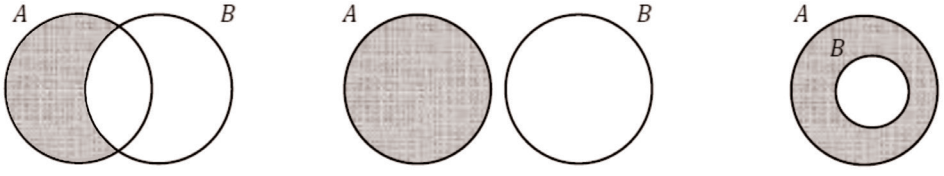
Exemplo 13: Dos onze jogadores do time de futebol ABC, oito tem pelo menos vinte cinco anos e sete tem no máximo 30 anos. Se $A = \{x \mid x$ é jogador do ABC que tem pelo menos 25 anos$\}$ e $B = \{x \mid x$ é jogador do ABC e tem no máximo 30 anos$\}$, podemos determinar o número de jogadores que possuem idade entre 25 e 30 anos. Como $A \cup B = \{x \mid x$ é jogador do time de futebol ABC$\}$, assim:

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$
$$11 = 8 + 7 - n(A \cap B)$$
$$n(A \cap B) = 4.$$

Definição: Considere dois conjuntos A e B, chamamos de diferença entre A e B ao conjunto C dos elementos de A que não pertencem a B. Denotamos por $A - B$ a diferença entre os conjuntos A e B e representamos:

$$A - B = C = \{x \mid x \in A \text{ e } x \notin B\}.$$

A diferença entre dois conjuntos $A - B$ pode ser representada no digrama de Venn:



Observamos que a diferença não é comutativa e nem associativa.

Exemplo 14: Sejam dados os conjuntos $A = \{-3, -2, -1, 0, 1, 2\}$ e $B = \{0, 1, 2, 3, 4, 5\}$. Determinamos os conjuntos $A - B$ e $B - A$ e verificamos que não possuem elementos comuns.

$A - B = \{-3, -2, -1\}$ e $B - A = \{3, 4, 5\}$, concluindo que $(A - B) \cap (B - A) = \emptyset$.

Definição: A diferença simétrica entre dois conjuntos A e B, denotada por $A \Delta B$, é o conjunto C que possui todos os elementos de A que não pertencem a B e todos os elementos de B que não pertencem a A, e nenhum outro elemento, assim,

$$A \Delta B = C = \{x \mid (x \in A \text{ e } x \notin B) \text{ ou } (x \notin A \text{ e } x \in B)\} = (A - B) \cup (B - A).$$

Podemos verificar facilmente que $(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$. Faça o diagrama de Venn para comprovar esta afirmação.

Exemplo 15: Considerando os conjuntos $A = \{1, 2, 3, 4, 5, 6\}$ e $B = \{2, 3, 5, 7, 11, 13\}$, determinamos a diferença simétrica entre A e B.

$$A \Delta B = \{1, 2, 3, 4, 5, 6, 7, 11, 13\} - \{2, 3, 5\} = \{1, 4, 6, 7, 11, 13\}.$$

Propriedades: Sejam A e B conjuntos quaisquer, valem as seguintes propriedades para a diferença simétrica:

- $A \Delta \emptyset = A$
- $A \Delta A = \emptyset$
- $A \Delta B = B \Delta A$.

Quando A e B são conjuntos com $A \subset B$, chamamos de complementar de A em relação a B ao conjunto formado pelos elementos de B que não pertencem a A, isto é, a diferença $B - A$, denotado por C_B^A e representado por

$$C_B^A = \{x \mid x \notin A \text{ e } x \in B\} = B - A.$$

Exemplo 16: Dados $A = \{1, 2, 3, 4\}$ e $B = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ podemos determinar o complementar de A em relação a B.

$$C_B^A = B - A = \{5, 6, 7, 8, 9, 10\}.$$

Definição: Dados os conjuntos A e B, chamamos de produto cartesiano, e representamos por $A \times B$, ao conjunto C formado por pares ordenados encontrados combinando cada um dos elementos do conjunto A com todos os elementos do conjunto B, nesta ordem, e nenhum outro elemento.

$$A \times B = C = \{(x,y) \mid x \in A \text{ e } y \in B\}.$$

Exemplo 17: Sejam $A = \{0, 1, 3, 5\}$ e $B = \{2, 3\}$, determinamos $A \times B$, $B \times A$ e $B \times B$.

$$A \times B = \{(0, 2), (0, 3), (1, 2), (1, 3), (3, 2), (3, 3), (5, 2), (5, 3)\}$$
$$B \times A = \{(2, 0), (2, 1), (2, 3), (2, 5), (3, 0), (3, 1), (3, 3), (3, 5)\}$$
$$B \times B = \{(2, 2), (2, 3), (3, 2), (3, 3)\}.$$

Observamos que o produto cartesiano não é comutativo, ou seja $A \times B \neq B \times A$. Podemos ainda determinar o número de elementos do produto que é:

$$n(A \times B) = n(A) \cdot n(B).$$

Exemplo 18: Dados dois conjuntos A com 5 elementos e B com 4 elementos, o número de elementos de $A \times B$ é

$$n(A \times B) = n(A) \cdot n(B) = 5 \cdot 4 = 20.$$

Para refletir

1. Dados $A = \{1, 2, 3, 4\}$, $B = \{2, 3, 6, 7, 8\}$ e $C = \{3, 4, 5, 6\}$, determine o que se pede:
   a) $A \cup B$
   b) $A \cap C$
   c) $A \cup (B \cup C)$
   d) $A - (B \cup C)$
   e) $A \Delta B$
   f) $A \times B$
2. Considere $A = \{2, 3, 5\}$ e $B = \{1, 2, 3, 4, 5, 6\}$. Determine o número de elementos de:
   a) $A \cup B$
   b) $A \times B$
3. Sejam A e B dois conjuntos distintos. Assinale a sentença verdadeira.
   a) $A - B = B - A$
   b) $(A - B) \subset (A \cap B)$
   c) $(A - B) \subset (A \cup B)$
   d) $(A - B) \cup (B - A) = A \cup B$.
4. Dados os conjuntos $A = \{0, 1, 2, 3, 4, 5, 6, 7\}$, $B = \{4, 5\}$, $C = \{1, 2\}$ e $D = \{2, 3, 4\}$. Determine:
   $(A - C) \cap (B \cup D)$.
5. Sejam $A = \{-2, -1, 0, 1, 2\}$ e $B = \{0, 1, 2\}$. Sobre o produto cartesiano, é correto afirmar que:
   a) $A \times B$ possui 8 elementos
   b) $A \times B = B \times A$
   c) $A \times A$ possui 25 elementos
   d) $B \times B$ possui 15 elementos.
6. Dados A, B e C conjuntos quaisquer, verifique se as seguintes propriedades envolvendo união e interseção são verdadeiras ou falsas:
   a) $A \cup (A \cap B) = A$
   b) $A \cap (A \cup B) = A$
   c) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
   d) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
7. Considere que $A \times B = \{(0, -2), (0, -1), (1, -2), (1, -1), (2, -2), (2, -1), (5, -2), (5, -1)\}$. Determine os conjuntos A e B.

4. Conjuntos Numéricos

Apresentamos resumidamente alguns conjuntos numéricos que serão utilizados ao longo do nosso estudo. O primeiro deles é o conjunto dos números naturais, formado pelos números 0, 1, 2, 3, 4, … e representado pela letra N.

$$N = \{0, 1, 2, 3, 4, \ldots\}$$

$$N^* = \{1, 2, 3, 4, \ldots\}.$$

No capítulo 4 estudaremos mais detalhadamente o conjunto dos naturais e os axiomas que o caracterizam.

O conjunto dos números inteiros, representado por Z, é formado por todos os números naturais, acrescidos dos números negativos, portanto:

$$Z = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Notamos que N é um subconjunto de Z, ou seja, $N \subset Z$.

O conjunto dos números racionais, representado por Q, é formado por todos os números que podem ser escritos na forma de fração, desta forma:

$$Q = \{x \mid x = \frac{a}{b}, \text{com } a, b \in Z \text{ e } b \neq 0\}.$$

São exemplos de racionais todos os números naturais, inteiros, decimais exatos, decimais infinitos periódicos.

Exemplos: 1\4 = 0,25 e -5\9 = −0,555 …

Chamaremos de conjunto dos números reais e representaremos por R, ao conjunto que possui os números racionais e os decimais infinitos não periódicos.

O conjunto formado por todos os números que não podem ser escritos na forma de fração, ou seja, decimais infinitos e não periódicos, será chamado de conjunto dos números irracionais e representado por I.

São exemplos de números irracionais: $\sqrt{2}$, $\sqrt{3}$, π = 3,14159265....

Notamos que a união do conjunto dos números racionais com o conjuntos dos irracionais resulta no conjuntos dos números reais, ou seja,

$$R = Q \cup I.$$

Ainda existem outros conjuntos numéricos fundamentais, como por exemplo, o conjunto dos números complexos, representado por C, formado por números da forma:

$c = a + bi$, com $a, b \in R$ e i é um número complexo que corresponde a $\sqrt{-1}$.

Este conjunto possui as seguintes operações de soma e produto:

(i) $(a + bi) + (c + di) = (a + c) + (b + d)i$

(ii) $(a + bi) \cdot (c + di) = (a \cdot c - b \cdot d) + (b \cdot c + a \cdot d)i$.

Os conjuntos numéricos serão analisados no capítulo 5, considerando os conceitos de grupos, anéis e corpos.

Atividades de avaliação

1. Assinale V para as sentenças verdadeiras e F para as sentenças falsas:

( ) $Z \subset R$

( ) $\sqrt{2} \in R$

( ) $I \supset Q$

( ) $-\frac{3}{5} \notin Q$

2. Verifique se as equação do segundo grau a seguir possuem raízes reais ou complexas:

a) $x^2 - 5 \cdot x + 6 = 0$

b) $2x^2 + 8 = 0$

c) $x^2 - 4 \cdot x + 5 = 0$

Síntese do capítulo

Definimos conjunto como uma coleção de objetos distintos e os objetos que fazem parte do conjunto são chamados de elementos. Chamamos a quantidade de elementos de um conjunto A de cardinalidade, representando por $n(A)$.

Estudamos as relações de pertinência, quando relacionamos elementos com conjuntos e utilizamos os símbolos $\in$, que lemos que o elemento pertence ou $\notin$, que lemos não pertence.

Definimos que A é um subconjunto de B se todo elemento que pertence ao conjunto A também pertence ao conjunto B, utilizamos a notação $A \subset B$, lemos A está contido em B, ou $B \cup A$, lemos B contém A. Se existir um elemento do conjunto A que não pertença ao conjunto B dizemos que A não é subconjunto de B e denotamos por $A \not\subset B$, lemos que A não está contido em B, ou $B \not\supset A$, lemos que B não contém A.

Definimos o conjunto das partes de A, usando a notação $P(A)$, como o conjunto formado por todos os subconjuntos do conjunto A e verificamos que $P(A)$ tem cardinalidade 2^n, onde n é o número de elementos do conjunto A.

Dados dois conjuntos A e B, apresentamos as operações entre conjuntos:

União: $A \cup B = \{x \mid x \in A \text{ ou } x \in B\}$

Interseção: $A \cap B = \{x \mid x \in A \text{ e } x \in B\}$

Diferença: $A - B = \{x \mid x \in A \text{ e } x \notin B\}$

Diferença simétrica: $A \Delta B = (A \cup B) - (A \cap B)$

Complementar: $C_B^A = B - A = \{x \mid x \notin A \text{ e } x \in B\}$, com $A \subset B$.

Definimos o produto cartesiano dos conjuntos A e B como o conjunto dos pares ordenados encontrados combinando cada um dos elementos do conjunto A com todos os elementos do conjunto B.

$$A \times B = \{(x,y) \mid x \in A \text{ e } y \in B\}$$

Verificamos que o número de elementos da união de dois A e B conjuntos é dada por:

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

Para três conjuntos A, B e C, temos que:

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C)$$

Observamos que o produto cartesiano não é comutativo, ou seja $A \times B \neq B \times A$ e ainda determinamos o número de elementos do produto que é:

$$n(A \times B) = n(A) \cdot n(B)$$

Apresentamos os conjuntos numéricos que serão utilizados ao longo do nosso estudo.

Naturais: $N = \{0, 1, 2, 3, 4, \ldots\}$

Inteiros: $Z = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

Racionais: $Q = \{x \mid x = \frac{a}{b}, \text{ com } a, b \in Z \text{ e } b \neq 0\}$.

Irracionais: formado por todos os números que não podem ser escritos na forma de fração.

Reais: $R = Q \cup I$.

Complexos: $C = \{a + bi, \text{ com } a,b \in R\}$

Esse conjunto satisfaz as seguintes regras de soma e produto:

(iii) $(a + bi) + (c + di) = (a + c) + (b + d)\,i$

(iv) $(a + bi) \cdot (c + di) = (a \cdot c - b \cdot d) + (b \cdot c + a \cdot d)i$

Leituras, filmes e sites

Sites

http://mtm.ufsc.br/~bosing/15_2/Conjuntos.pdf

http://homepages.dcc.ufmg.br/~loureiro/md/md_5TeoriaDosConjuntos.pdf

Referências

CINTRA, Glauber Ferreira. **Matemática I**. Fortaleza: RDS, 2009.

LIPSCHUTZ, S; LIPSON, M. **Matemática discreta**. 2 ED. Porto Alegre: Bookman, 2004.

MENEZES, Paulo Blath. **Matemática discreta para computação e informática**. 2 ed. Porto Alegre: Sagra Luzzatto, 2005.

Capítulo 2

Relação e Função

Objetivos

- Conhecer relações binárias e identificar suas propriedades;
- Calcular a inversa de uma relação
- Identificar relações de equivalência;
- Conhecer o conceito de função e identificar quando uma relação é função;
- Calcular a inversa de uma função;
- Identificar relações injetoras, sobrejetoras e bijetoras.

Em computação e informática, muitas construções são baseadas em relações e funções. Além disso, são conteúdos importantes da educação básica que poderão ser melhor apresentados e compreendidos com o auxílio da informática, utilizando softares educativos, jogos e programas de construção de gráficos.

1. Relação

Definição: Dados dois conjuntos A e B, uma relação binária, ou apenas relação, é um subconjunto R do produto cartesiano $A \times B$. Os pares ordenados de R associam elementos $x \in A$ com elementos $y \in B$ e podem ser denotados por xRy ou simplesmente R, ou seja,

$$R \subset A \times B.$$

Exemplo 1: Considere os conjuntos $A = \{1, 3, 5, 7\}$ e $B = \{3, 5, 7, 9, 11\}$ e a relação R definida por $R = \{(x,y) \in A \times B \mid y = 2 \cdot x - 3\}$. Os pares ordenados que fazem parte da relação R são:

$$R = \{(3, 3), (5, 7), (7, 11)\}.$$

Definição: Dada a relação R, definimos a relação inversa de R, como sendo o conjunto R^{-1} de todos os pares de R com a ordem invertida e representamos por

$$R^{-1} = \{(y,x) \mid (x,y) \in R\}.$$

Exemplo 2: Considere a relação $R = \{(1, 9), (2, 8), (3, 7), (4, 6),(5, 5)\}$. Os pares ordenados que fazem parte da relação inversa são:

$$R^{-1} = \{(9, 1), (8, 2), (7, 3), (6, 4), (5, 5)\}.$$

Propriedades: Dados um conjunto A e uma relação $R \subset A \times A$, definimos as seguintes condições.

- R é reflexiva se $(x, x) \in R$, para todo $x \in A$.
- R é simétrica se $(x, y) \in R$, então $(y,x) \in R$.
- R é transitiva se (x, y), $(y, z) \in R$, então $(x,z) \in R$.

Dizemos que uma relação R é antirreflexiva se $(x,x) \notin R$, para todo $x \in A$ e que R é antissimétrica se $(x, y) \in R$ e $(y, x) \in R \Rightarrow x = y$.

Definição: Dizemos que R é uma relação de equivalência se ela é reflexiva, simétrica e transitiva.

Exemplo 3: Verifiquemos quais das propriedades apresentadas são satisfeitas pela relação $R = \{(2, 8), (3, 7), (4, 6), (5, 5), (6, 4), (7, 3), (8, 2)\}$.

- R não é reflexiva, pois $(2, 2), (3, 3), (4, 4), (6, 6), (7, 7), (8, 8) \notin R$.
- R não é antirreflexiva, pois $(5, 5) \in R$.
- R é simétrica, pois cada $(x, y) \in R$, temos $(y, x) \in R$.
- R não é antissimétrica, pois: $(2, 8), (8, 2) \in R$ e $2 \neq 8$; $(3, 7), (7, 3) \in R$ e $3 \neq 7$ e $(4, 6), (6, 4) \in R$ e $4 \neq 6$.
- R não é transitiva, pois: $(2, 8), (8, 2) \in R$, mas $(2, 2), (8, 8) \notin R$; $(3, 7), (7, 3) \in R$, mas $(3, 3),(7, 7) \notin R$ e $(4, 6), (6, 4) \in R$, mas $(4, 4), (6, 6) \notin R$.

A relação R não é uma relação de equivalência, pois, apesar de ser simétrica, não possui as condições de ser reflexiva e transitiva.

Exemplo 4: A relação $R = \{(x, y) \mid x = y\}$ é uma relação de equivalência.

R é reflexiva, pois para todo x, temos que $x = x$, logo $(x, x) \in R$;

R é simétrica, pois para todo par (x, y), temos que $x = y$, assim $(y, x) \in R$;

R é transitiva, pois (x, y), $(y, z) \in R$, temos que $x = y$ e $y = z$, logo $x = z$, então $(x, z) \in R$.

Para refletir

1. Dados os conjuntos $A = \{1, 3, 5\}$ e $B = \{3, 5, 7, 9\}$, indique os pares ordenados das seguintes relações:
   $R_1 = \{(x, y) \in A \times B \mid y = x - 2\}$
   $R_2 = \{(x, y) \in A \times B \mid y > x\}$.
2. Considere os conjuntos $A = \{-2, -1, 0, 1, 2, 3, 4\}$ e $B = \{0, 1, 4, 8, 9\}$ e a relação $R = \{(x, y) \in A \times B \mid y = 2x + 1\}$. Determine os pares ordenados que fazem parte da relação R^{-1}.

Verifique se a relação $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4)\}$ é uma relação de equivalência sobre $A = \{1, 2, 3, 4\}$.

2. Função

Definição: Uma função de A em B é uma relação que a cada elemento do conjunto A associa um único elemento do conjunto B. Representamos a função f de A em B por f: $A \rightarrow B$. Utilizamos ainda a notação $y = f(x)$ para indicar que o par (x, y) pertence a função f.

Exemplo 5: Sejam $A = \{1, 2, 3, 4\}$, $B = \{2, 4, 6, 8, 10\}$ e a relação $R = \{(x, y) \in A \times B \mid y = 2 \cdot x\}$. Afirmamos que a relação R é uma função.

Para $x = 1$, temos que $y = 2 \cdot 1 = 2 \in B$, logo $(1, 2) \in R$;

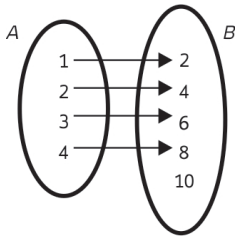
Para $x = 2$, temos que $y = 2 \cdot 2 = 4 \in B$, logo $(2, 4) \in R$;

Para $x = 3$, temos que $y = 2 \cdot 3 = 6 \in B$, logo $(3, 6) \in R$;

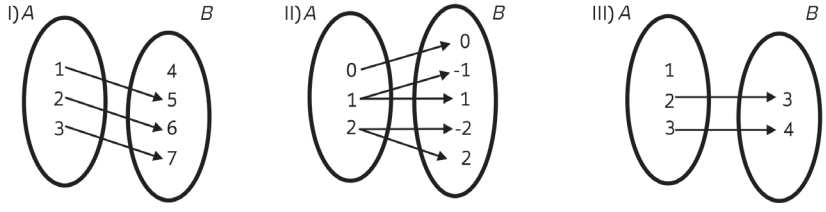
Para $x = 4$, temos que $y = 2 \cdot 4 = 8 \in B$, logo $(4, 8) \in R$;

R = {(1, 2), (2, 4), (3, 6), (4, 8)}.

Como cada elemento do conjunto A está associado a um único elemento de B, então R é função.



Exemplo 6: Identificamos através do diagrama as relações que são funções.



I é função, pois cada elemento do conjunto A está associado a um único elemento do conjunto B.

II não é função, pois existem elementos de A que estão associados a mais de um elemento de B.

III não é função, pois existe elemento de A que não está associado a nenhum elemento de B.

Chamamos de domínio da função ao conjunto que possui todos os primeiros elementos dos pares ordenados. O conjunto formado pelos elementos que estão associados a algum elemento do domínio é chamado de conjunto imagem. Quando consideramos todos os elementos do conjunto de chegada, mesmo aqueles que não estão associados a elementos do domínio, denominamos o conjunto de contradomínio.

Exemplo 7: Dados os conjuntos $A = \{0, 1, 2\}$ e $B = \{0, 1, 2, 3, 4, 5\}$. Seja $f: A \to B$ a função definida por $f(x) = 2 \cdot x + 1$. Determinamos o domínio $D(f)$, o contradomínio $CD(f)$ e a imagem $Im(f)$ de f.

Para

$x = 0$, $f(0) = 2 \cdot 0 + 1 = 1 \in B$, logo $(0, 1) \in f$;

$x = 1$, $f(1) = 2 \cdot 1 + 1 = 3 \in B$, logo $(1, 3) \in f$;

$x = 2$, $f(0) = 2 \cdot 2 + 1 = 5 \in B$, logo $(2, 5) \in f$;

Desta forma, $D(f) = \{0, 1, 2\}$, $CD(f) = \{0, 1, 2, 3, 4, 5\}$ e $Im(f) = \{1, 3, 5\}$.

Assim como nas relações, também definimos a inversa de uma função f como sendo a relação inversa de f. Denotamos a relação inversa por f^{-1}. Observamos que f^{-1} nem sempre será função.

Note que uma das condições para que uma relação seja função é que cada elemento do domínio esteja associado um único elemento do contradomínio.

Dessa forma, para que a inversa de uma função continue sendo uma função, é necessário que todos os elementos do contradomínio estejam associados a algum elemento do domínio, ou seja, o contradomínio deverá ser igual a imagem. Isto motiva a seguinte definição.

Definição: Dizemos que uma função é sobrejetora se a sua imagem é igual ao seu contradomínio.

Por outro lado, nem sempre a inversa de uma função sobrejetora é função, pois poderá possuir elementos do domínio associados a mais de um elemento da imagem, o que impediria a inversa de ser uma função. Temos mais uma condição para que a inversa de uma função também seja função, ou seja, cada elemento do domínio deverá estar associado a um elemento diferente da imagem.

Definição: Dizemos que uma função é injetora se elementos distintos do domínio possuem imagens distintas. Em outras palavras, f é injetora se, e somente se, $f(x) = f(y)$ implicar $x = y$.

Definição: Quando uma função for injetora e sobrejetora será chamada de função bijetora, e sua inversa será sempre uma função.

Exemplo 8: Sejam $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$ e a $f: A \to B$ definida por $f(x) = x + 3$.

f é função bijetora e sua inversa f^{-1} é função.

Podemos fazer a composição de funções, ou seja, dadas duas funções $f: A \to B$ e g: $Im(f) \to C$, definimos a função $(g \circ f)(x) = g(f(x))$, que é a composta de g com f, aplicada em x.

Exemplo 9: Dadas $f(x) = 5 \cdot x + 1$ e $g(x) = x^2$, determine $f \circ g$.

$$f \circ g = f(g(x)) = 5 \cdot g(x) + 1 = 5 \cdot x^2 + 1$$

Atividades de avaliação

1. Analise as relações a seguir, identificando as que são funções:
   a) $A = \{-1, 1, 2, 3\}$, $B = \{-2, 0, 1, 2\}$ e $R = \{(x,y) \in A \times B \mid y = x - 1\}$.
   b) $\{(4, 1), (1, 2), (3, 4), (3, 2), (4, 3)\}$ sobre o conjunto $A = \{1, 2, 3, 4\}$.
   c) $A = \{1, 2\}$, $B = \{3, 4, 5\}$ e $R = A \times B$.
2. Dados $A = \{1, 2\}$, $B = \{3, 4, 5\}$, considere $f: A \to B$ a função definida por $f(x) = 2 \cdot x + 1$. Determine o domínio, o contradomínio e a imagem da função.
3. Identifique se as funções a seguir são injetoras, sobrejetoras ou bijetoras. No caso das funções bijetoras identifique a inversa da função.
   a) $A = \{1 , 2, 3, 4\}$ e $f: A \to A$ definida por $f(x) = x$.
   b) $A = \{-2, -1, 0, 1, 2\}$, $B = \{-1, 0, 3, 8\}$ e $f: A \to B$ a função definida por $f(x) = x^2 - 2 \cdot x$.
   c) $A = \{1, 2, 3, 4, 5\}$, $B = \{1, 2, 3, 4, 5\}$ e $f: A \to B$ a função definida por $f(x) = 2$.
4. Dadas as funções $f(x) = 3 \cdot x - 1$ e $g(x) = x + 2$, encontre $f \circ g$ e $g \circ f$.

Síntese do capítulo

Definimos uma relação binária ou apenas relação de A em B ao conjunto de pares ordenados que associa elementos do conjunto A a elementos do conjunto B. Podemos dizer que uma relação R associa elementos $x \in A$ com elementos $y \in B$ e denotamos por xRy ou simplesmente R, ou seja,

$$R = \{(x, y) \in A \times B\} \subset A \times B.$$

Dada uma relação R, definimos a relação inversa de R, como sendo o conjunto R^{-1} de todos os pares de R com a ordem invertida e representamos por

$$R^{-1} = \{(y, x) \mid (x, y) \in R\}.$$

Propriedades: Dados um conjunto A e uma relação R, definimos as seguintes condições.

- R é reflexiva se $(x, x) \in R$, para todo $x \in A$.
- R é simétrica se $(x, y) \in R$, então $(y, x) \in R$.
- R é transitiva se $(x, y), (y, z) \in R$, então $(x, z) \in R$.

Dizemos que R é antirreflexiva se $(x, x) \notin R$, para todo $x \in A$ e que R é antissimétrica se $(x, y) \in R \Rightarrow (y, x) \in R \Rightarrow x = y$.

Dizemos que R é uma relação de equivalência se ela é reflexiva, simétrica e transitiva.

Definimos uma função de A em B como uma relação que a cada elemento do conjunto A associa um único elemento do conjunto B. Representamos a função f de A em B por $f: A \to B$. Utilizamos ainda a notação $y = f(x)$ para indicar que x se relaciona com y através da função f.

Chamamos de domínio da função ao conjunto que possui todos os primeiros elementos dos pares ordenados. O conjunto formado pelos elementos que estão associados a algum elemento do domínio é chamado de conjunto imagem. Quando consideramos todos os elementos do conjunto de chegada, mesmo aqueles que não estão associados a elementos do domínio, denominamos o conjunto de contradomínio.

Definimos a função inversa f^{-1}, observando que a inversa de uma função nem sempre será função.

Chamamos de função sobrejetora uma função que tem todos os elementos do contradomínio associados a algum elemento do domínio, ou seja, o contradomínio deverá ser igual a imagem.

Chamamos de função injetora quando cada elemento do domínio estiver associado a um elemento diferente da imagem, ou seja, elementos distintos do domínio possuem imagens distintas.

Quando uma função for injetora e sobrejetora será chamada de função bijetora e sua inversa será sempre uma função.

Leituras, filmes e sites

Sites

http://www.univasf.edu.br/~jorge.cavalcanti/Mat_Disc_Parte11.pdf

http://www.inf.ufsc.br/~mauro.roisenberg/ine5403/slides_novos/zpdfs_ppts/p23funcoes.pdf

Referências

CINTRA, Glauber Ferreira. **Matemática I.** Fortaleza: RDS, 2009.

LIMA, E. L.; CARVALHO, P. C. P.; WAGNER, E. E MORGADO, A.C. **A Matemática do Ensino Médio** Vol.1. Rio de Janeiro: SBM, 2004.

LIPSCHUTZ, S; LIPSON, M. **Matemática discreta**. 2 ED. Porto Alegre: Bookman, 2004.

MENEZES, Paulo Blath. **Matemática discreta para computação e informática**. 2 ed. Porto Alegre: Sagra Luzzatto, 2006.

Capítulo 3

Análise Combinatória

Objetivos

- Conhecer e aplicar os princípios aditivo e multiplicativo na solução de problemas;
- Identificar nos problemas de contagem a importância da ordem dos elementos;
- Utilizar fórmulas da arranjos simples, combinações, permutações simples e com repetições, para facilitar a resolução de problemas de contagem;
- Conhecer e utilizar o Triângulo de Pascal.

A análise combinatória está relacionada a problemas de contagem de conjuntos finitos e surge com frequência em problemas teóricos e práticos ligados aos computadores.

1. Princípio de contagem

Apresentamos duas ferramentas importantes para a solução de problemas de contagem: o princípio aditivo e o princípio multiplicativo.

Sejam A e B conjuntos que não possuem elementos em comum. O princípio aditivo garante que o número de elementos da união é igual ao número de elementos do conjunto A somado ao número de elementos do conjunto B, ou seja,

$$n(A \cup B) = n(A) + n(B), \text{ quando } A \cap B = \emptyset.$$

Podemos estender o princípio aditivo para um número finito de conjuntos. Dados n conjuntos $A_1, A_2, \ldots, A_n$, tais que $A_i \cap A_j = \emptyset$ para todo $i \neq j$, temos:

$$n(A_1 \cup A_2 \cup \ldots \cup A_n) = n(A_1) + n(A_2) + \cdots + n(A_n).$$

Exemplo 1: Ana deseja participar da Semana Universitária. Foram oferecidos 3 palestras e 2 seminários que interessavam a Ana, todos no mesmo horário. Note que ela tem três maneiras distintas para a escolha da palestra $n(P) = 3$ e duas maneiras distintas para a escolha do seminário $n(S) = 2$, como os eventos são mutuamente excludentes, visto que Ana não poderá assistir a uma palestra e participar de um seminário que são eventos distintos no mesmo horário, o número de possibilidades de escolhas será:

$$n(P) + n(S) = 3 + 2 = 5.$$

Dados dois conjuntos A e B, o princípio multiplicativo nos garante que o número de maneiras de escolher um primeiro elemento do conjunto A e um segundo elemento do conjunto B é igual ao número de elementos de A multiplicado pelo número de elementos de B. Em outras palavras, o número de elementos do produto cartesiano de A por B satisfaz:

$$n(A \times B) = n(A) \cdot n(B).$$

Estendendo para um número finito de conjuntos, temos que:

$$n(A_1 \times A_2 \times \ldots \times A_n) = n(A_1) \cdot n(A_2) \cdot \ldots \cdot n(A_n).$$

Exemplo 2: Os organizadores da Semana Universitária, observando o interesse dos alunos em participar de palestras e seminários resolveram oferecer as palestras em um horário e os seminários em outro. Ana poderá participar de dois eventos escolher uma palestra e um seminário. Aplicando o princípio multiplicativo temos que ela poderá fazer essa escolha de 6 maneiras distintas:

$$n(P) \cdot n(S) = 3 \cdot 2 = 6.$$

Exemplo 3: Desejamos escrever números de dois algarismos, que podem ser iguais ou não, utilizando elementos do conjunto $A = \{1, 2, 3, 4, 5, 6\}$.

Observamos que para a escolha do algarismo das dezenas temos 6 possibilidades. Como o algarismo das unidades pode ser repetido, temos ainda 6 possibilidades. Pelo princípio multiplicativo teremos:

$6 \cdot 6 = 36$ possibilidades de números com a condição dada.

Exemplo 4: Desejamos escrever números de dois algarismos distintos, utilizando elementos do conjunto $A = \{1, 2, 3, 4, 5, 6\}$.

Nesta situação para a escolha do primeiro número continuamos com 6 possibilidades, no entanto, como o segundo número deverá ser diferente do primeiro, ficamos com apenas 5 possibilidades, ou seja, o conjunto B terá 5 elementos. Pelo princípio multiplicativo teremos:

$6 \cdot 5 = 30$ possibilidades de números com a condição dada.

Existem situações mais complexas em que podemos utilizar simultaneamente os princípios aditivo e multiplicativo. Vejamos alguns exemplos.

Exemplo 5: Os alunos que apresentarem trabalhos na Semana Universitária serão classificados e premiados com 2 livros de disciplinas diferentes. Sabemos que existem 7 livros diferentes de informática (I), 4 livros diferen-

tes de matemática (M) e 5 livros diferentes de didática (D). Ana foi a primeira colocada. Podemos determinar o número de escolhas que Ana poderá fazer. Ana poderá escolher as disciplinas de três maneiras diferentes:

- Informática e Matemática, pelo princípio multiplicativo:

$$n(I \times M) = n(I) \cdot n(M) = 7 \cdot 4 = 28.$$

- Informática e Didática, pelo princípio multiplicativo:

$$n(I \times D) = n(I) \cdot n(D) = 7 \cdot 5 = 35.$$

- Matemática e Didática, pelo princípio multiplicativo:

$$n(M \times D) = n(M) \cdot n(D) = 4 \cdot 5 = 20.$$

Utilizando o princípio ativo determinamos o total de escolhas:

28+35+20=83 possibilidades de escolha.

Para refletir

1. Rafael deseja ir ao cinema de um shopping que possui 6 salas e estão sendo exibidos 2 filmes diferentes de comédia e 4 filmes diferentes de ação. De quantas maneiras diferentes ele poderá fazer a escolha dos filmes considerando que:
   a) deseja assistir apenas a um filme?
   b) deseja assistir a dois filmes quaisquer?
   c) deseja assistir a um filme de ação e uma comédia?
2. Um estacionamento possui 10 vagas. De quantas modos diferentes três carros podem ser estacionados nesse estacionamento?
3. Uma chapa composta por um homem e uma mulher, que não podem ser irmãos, deverá ser formada para concorrer às eleições do grêmio de uma escola. Estão inscritos para comporem a chapa 14 mulheres e 8 homens, dos quais 5 são irmãos (3 homens e 2 mulheres). De quantas maneiras distintas podemos formar uma chapa com pessoas deste grupo?
4. Seis atletas participam de uma maratona. Quantas possibilidades diferentes de classificação final dos participantes podemos ter, supondo que não ocorram empates?

2. Arranjos

Para facilitar nossos cálculos definimos o fatorial de um número n e representamos por $n!$, como sendo:

$$n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1.$$

Exemplo 6: Para $n = 5$, temos que $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$.

Por convenção escrevemos que $0! = 1$.

Definição: Chamamos de arranjo simples cada uma das lista ordenadas, sem repetição, formadas a partir da escolha de p elementos de um conjunto com n elementos distintos.

Exemplo 7: Considere o conjunto $A = \{1, 2, 3, 4\}$. Os arranjos de 3 elementos formados por elementos de A são: (1 , 2, 3), (1, 2, 4), (1, 3, 2), (1, 3, 4), (1, 4, 2), (1, 4, 3), (2, 1, 3), (2, 1, 4), (2, 3, 1), (2, 3, 4), (2, 4, 1), (2, 4, 3), (3, 1, 2), (3, 1, 4), (3, 2, 1), (3, 2, 4), (3, 4, 1), (3, 4, 2), (4, 1, 2), (4, 1, 3), (4, 2, 1), (4, 2, 3), (4, 3, 1), (4, 3, 2).

Exemplo 8: Considere o conjunto $A = \{1, 2, 3, 4\}$. Desejamos formar números com dois algarismos distintos com os elementos do conjunto A, ou seja, estamos em uma situação em que possuímos 4 elementos e escolhemos dois distintos. Além disso, a ordem é importante, visto que por exemplo o número 12 é diferente do número 21.

Para escolher o algarismo das dezenas temos 4 possibilidades. Depois de escolhido o primeiro número, como o segundo deve ser diferente, ficamos com apenas 3 escolhas. Para resolver problemas de arranjos podemos utilizar o princípio multiplicativo. Dessa forma, $4 \cdot 3 = 12$.

Proposição 1: Para formar um arranjo simples com p escolhas teremos n possibilidades para a escolha do primeiro. Como não podem haver repetições, teremos $n - 1$ maneiras de escolher o segundo e assim sucessivamente até a escolha do elemento da p-ésima posição que terá $n - p + 1$ possibilidades de escolha. Dessa forma, aplicando o princípio multiplicativo, temos que o número de arranjos simples que podemos formar escolhendo p elementos de um conjunto com n elementos, representado por $A_{n,p}$, é:

$$A_{n,p} = n \cdot (n - 1) \cdot (n - 2) \cdot \ldots \cdot (n - p + 1)$$

$$A_{n,p} = \frac{n \cdot (n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-p+1) \,.\, (n-p) \cdot (n-p-1) \cdot \ldots \cdot 3 \cdot 2 \cdot 1}{(n-p) \cdot (n-p-1) \cdot \ldots \cdot 3 \cdot 2 \cdot 1}$$

$$A_{n,p} = \frac{n!}{(n-p)!}$$

Exemplo 9: De quantos modos diferentes 3 pessoas podem ocupar lugares em uma fila com 8 cadeiras?

$$A_{8,3} = \frac{8!}{(8-3)!} = \frac{8!}{5!} = \frac{8 \cdot 7 \cdot 6 \cdot 5!}{5!} = 336 \text{ possibilidades.}$$

Para refletir

1. Dado o conjunto $A = \{2, 3, 5, 7, 9\}$. Quantos números de três algarismos distintos podem ser formados com os elementos do conjunto A? Quantos desses números são pares?
2. Num teatro existem fileiras com 6 cadeiras. De quantos modos diferentes três pessoas podem se sentar em uma fileira?

3. Permutações

A permutação simples é um caso particular de arranjo simples, nesse caso utilizamos todos os elementos distintos, ou seja, consideramos todas as listas ordenadas contendo todos os elementos de um conjunto.

Definição: Dados n objetos distinos, chamamos de permutação simples qualquer agrupamento ordenado desses n objetos. Representamos o número de tais permutações por P_n.

Chamamos de anagramas de uma certa palavra as palavras que resultam de uma permutação das letras da primeira. Um anagrama pode ter significado ou não.

Exemplo 10: Determine todos os anagramas que podemos formar permutando as letras da palavra FILA.

FILA – FIAL – FALI – FAIL – FLIA – FLAI
IFLA – IFAL – ILFA – ILAF – IAFL – IALF
LFIA – LFAI – LAFI – LAIF – LIFA – LIAF
AFIL – AFLI – ALFI – ALIF – AILF – AIFL.

Encontramos 24 anagramas da palavra FILA.

Proposição 2: Observamos que, para a escolha do primeiro objeto, temos *n* possibilicades. Escolhido o primeiro elemento teremos *n* - 1 possibilidades para escolher o segundo elemento e que esta escolha é independente da primeira escolha. Utilizando o princípio multiplicativo e continuando as escolhas até o último elemento poderemos escrever que o número de possibilidades de permutações simples será:

$$P_n = n \cdot (n - 1) \cdot (n - 2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1 = n!.$$

A Proposição 2 pode ser demonstrada utilizando o princípio de indução, que será apresentado no Capítulo 4.

Exemplo 11: Quantos anagramas podemos formar permutando as letras da palavra FILA?

$$P_4 = 4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24 \text{ anagramas.}$$

Observamos que a permutação simples dos elementos apresentou como condição que esses elementos fossem distintos. Logo, a Proposição 2 não poderá ser utilizada quando formos perguntados sobre o número de permutações de uma coleção de objetos em que alguns deles apareçam repetidos.

Exemplo 12: Determine todos os anagramas que podemos formar permutando as letras da palavra ARARA. Temos as seguintes possibilidades:

ARARA – ARAAR – ARRAA – AARRA – AARAR – AAARR – RRAAA –
RARAA – RAARA – RAAAR.

Portanto, temos 10 possíveis anagramas, enquanto $P_5 = 120$.

Definição: Dada uma coleção de elementos em que alguns deles aparecem com repetição, denominamos as permutações nesta coleção de permutação com repetição.

Proposição 3: Dados *n* objetos em uma lista ordenada, que podem ter repetições ou não. Se os objetos fossem todos distintos teríamos n! possibilidades de permutar esses objetos. Considerando que tenhamos n_1 cópias do objeto 1, n_2 cópias do objeto 2, e assim sucessivamente, até que o objeto k possui n_k cópias. Quando permutamos elementos iguais não alteramos a lista e pelo princípio multiplicativo temos $n_1! \cdot n_2! \cdot n_3! \cdot \ldots \cdot n_k!$ permutações envolvendo

apenas elementos iguais. Assim, para retirarmos as repetições, a quantidade de permutações com repetições será:

$$P_n^{n1, n2, \ldots, nk} = \frac{n!}{n_1! \cdot n_2! \cdot n_3! \cdot \ldots \cdot n_k!}$$

lembrando que n= $n_1 + n_2 + \cdots + n_k$.

Exemplo 13: Quantos anagramas podemos formar permutando as letras da palavra ARARA?

$$P_5^{2,3} = \frac{5!}{3! \cdot 2!} = \frac{5 \cdot 4 \cdot 3!}{3! \cdot 2 \cdot 1} = \frac{5 \cdot 4}{2} = \frac{20}{2} = 10 \text{ anagramas.}$$

Para refletir

1. De quantas maneiras podemos formar uma fila com 6 pessoas?
2. Quais são os anagramas que podemos formar com o nome RAUL?
3. Quantos anagramas podemos formar com as letras da palavra MATEMATICA?
4. De quantos modos possíveis seis pessoas podem ocupar uma fila do cinema que possui exatamente seis lugares, sabendo que dois deles desejam sentar juntos?

4. Combinações

Definição: Chamamos de combinação simples a cada um dos conjuntos formados a partir da escolha de *p* elementos de um conjunto com *n* elementos distintos.

Exemplo 14: Dos 5 professores de matemática de uma escola serão escolhidos 2 para participar de uma palestra. Sejam p_1, p_2, p_3, p_4 e p_5 os cinco professores da escola, podemos formar as seguintes comissões:

Note que se os professores escolhidos forem p_1 e p2, essa escolha é a mesma de p_2 e p_1, dessa forma, temos as seguintes possibilidades

$p_1 \text{ e } p_2 - p_1 \text{ e } p_3 - p_1 \text{ e } p_4 - p_1 \text{ e } p_5 - p_2 \text{ e } p_3 - p_2 \text{ e } p_4 - p_2 \text{ e } p_5 - p_3 \text{ e } p_4 - p_3 \text{ e } p_5 - p_4 \text{ e } p_5$:

Proposição 4: Para determinar a quantidade de combinações simples que temos a partir da escolha de *p* elementos de um total de *n* possibilidades podemos calcular o número de arranjos simples com p elementos dentre n elementos dados e dividir pela quantidade de permutações dos *p* elementos escolhidos, dado que os arranjos de p elementos permutados correspondem a uma única combinação. Dessa forma, o número de combinações simples que podemos formar escolhendo *p* elementos de um conjunto com n elementos, e representamos por $C_{n,p}$, é:

$$C_{n,p} = \frac{An,\, p}{P_p} = \frac{\frac{n!}{(n-p)!}}{p!} = \frac{n!}{(n-p)! \cdot p!}$$

Exemplo 15: Dos 5 professores de Matemática de uma escola serão escolhidos 2 para participar de uma palestra. Quantas comissões com dois destes professores podemos formar?

Existem 5 professores e devemos escolher 2:

$$C_{5,2} = \frac{5!}{(5-2)!\cdot 2!} = \frac{5!}{3!\cdot 2!} = \frac{5\cdot 4\cdot 3!}{3!\cdot 2\cdot 1} = \frac{20}{2} = 10.$$

Outra notação que também é muito utilizada para as combinações simples e as relaciona ao Triângulo de Pascal é a seguinte: $C_{n,p} = \binom{n}{p}$. O triângulo de Pascal consiste em escrever a lista desses números associados a combinações em formato de triângulo, como abaixo:

$$\binom{0}{0}$$
$$\binom{1}{0}\ \binom{1}{1}$$
$$\binom{2}{0}\ \binom{2}{1}\ \binom{2}{2}$$
$$\vdots\quad\ \vdots\quad\ \vdots\ \ddots$$
$$\binom{n}{0}\ \binom{n}{1}\ \binom{n}{2}\cdots\binom{n}{n}$$

ou seja, a n-ésima linha é composta pelos valores das combinações de p elementos de um conjunto de n elementos, com *p* variando de 0 a *n*. Calculando os valores das combinações do Triângulo de Pascal obtemos os coeficientes do conhecido Binômio de Newton

$$(x+y)^n = \binom{n}{o} x^n.y^0 + \binom{n}{1} x^{n-1}.y^1 + \cdots + \binom{n}{n-1} x^1.y^{n-1} + \binom{n}{n} x^0.y^n,$$

com $n \in N$, que são:

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋱

Exemplo 16: Desejamos calcular o termo independente de *x* no desenvolvimento do binômio

$$(x^3 - x^{-2})^{10}$$

No desenvolvimento do binômio o termo independente de x terá expoente zero, temos que o termo de ordem $n + 1$ é da forma: $T_{p+1} = \binom{n}{p} x^{n-p} \cdot y^p$.

No binômio apresentado temos:

$$T_{p+1} = \binom{10}{p} (x^3)^{10-p} \cdot (-x^{-2})^p$$

$$T_{p+1} = \binom{10}{p} (-1)^p \cdot x^{30-3p} \cdot x^{-2p}$$

$$T_{p+1} = \binom{10}{p} (-1)^p \cdot x^{30-3p-2p}$$

$$T_{p+1} = \binom{10}{p} (-1)^p \cdot x^{30-5p}.$$

Note que o expoente de x será igual a zero quando: $30 - 5p = 0 \Rightarrow p = 6$

Desta forma o termo independente de *x* é:

$$T_7 = \binom{10}{6} (-1)^6 \cdot x^0 = \frac{10!}{(10-6)!\,6!} = \frac{10!}{4! \cdot 6!} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6!}{4 \cdot 3 \cdot 2 \cdot 1 \cdot 6!} = 210$$

Atividades de avaliação

1. De quantos maneiras distintas podemos dividir 10 pessoas em dois grupos de 5?
2. De quantos modos possíveis 8 pessoas podem se organizar em grupos de 2?
3. Quantos jogos serão realizados em um campeonato com 5 times participantes, sabendo que dois times jogam uma única partida entre si e que cada time enfrenta todos outros?
4. O ENEM dividiu as disciplinas em 4 áreas de conhecimentos: Linguagens e Códigos (com Redação), Ciências da Natureza, Ciências Humanas e Matemática. Sabendo que as provas serão realizadas em dois dias, de quantas formas poderá ser feita a escolha das provas, sabendo que devem ser aplicadas duas provas por dia?
5. Sarah possui 5 tipos diferentes de frutas, quantos tipos de sucos ela poderá fazer utilizando 2 ou mais frutas?
6. Desenvolva o binômio$(x - y)^5$.

Síntese do capítulo

Apresentamos duas ferramentas importantes para a solução de problemas de contagem: o princípio aditivo e o princípio multiplicativo.

Dados dois conjuntos A e B, que não possui elementos em comum, o princípio aditivo garante que: $n(A \cup B) = n(A) + n(B)$, quando $A \cap B = \emptyset$.

Estendemos o princípio aditivo para um número finito de conjuntos. Para n conjuntos $A_1, A_2, \ldots, A_n$, tais que $A_i \cap A_j = \emptyset$ para todo $i \neq j$.

$$n(A_1 \cup A_2 \cup \ldots \cup A_n) = n(A_1) + n(A_2) + \ldots + n(A_n).$$

Dados dois conjuntos A e B, o princípio multiplicativo nos garante que:

$$n(A \times B) = n(A) \cdot n(B)$$

Estendendo para um número finito de conjuntos, temos:

$$n(A_1 \times A_2 \times \ldots \times A_n) = n(A_1) \cdot n(A_2) \cdot \ldots \cdot n(A_n).$$

Definimos o fatorial de um número como sendo:

$$n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1.$$

Definimos os arranjo simples como cada uma das lista ordenadas, sem repetição, formadas a partir da escolha de p elementos de um conjunto com n elementos distintos. Concluímos que número de arranjos simples que podemos formar escolhendo p elementos de um conjunto com n elementos, e representamos por $A_{n,p}$, é:

$$A_{n,p} = \frac{n!}{(n-p)!}$$

Dados n objetos distintos, chamamos de permutação simples e representamos por P_n qualquer agrupamento ordenado desses n objetos. A permutação simples é um caso particular do Arranjo simples, quando utilizamos todos os n elementos distintos. Concluímos que o número de possibilidades de permutações simples será:

$$P_n = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1 = n!.$$

Definimos permutações de conjuntos com elementos iguais e denominamos por permutação com repetição. Concluímos que a quantidade de permutações com repetições será:

$$P_n^{n1,n2,\ldots,nk} = \frac{n!}{n_1! \cdot n_2! \cdot n_3! \cdot \ldots \cdot n_k!}.$$

Chamamos de combinação simples a cada um dos conjuntos formados a partir da escolha de p elementos de um conjunto com n elementos distintos.

Constatamos que o número de combinações simples de um conjunto com n elementos e p escolhas é:

$$C_{n,p} = \frac{n!}{(n-p)!\,.\,p!).\,p!}.$$

Utilizamos a notação $c_{n,p} = \binom{n}{p}$ e apresentamos o triângulo de Pascal, formado por todas as possibilidades de combinações de $p = 0,1, \ldots, n$. Observamos que os valores das combinações do Triângulo de Pascal são os coeficientes do Binômio de Newton $(x+y)^n = \binom{n}{o} x^n.y^0 + \binom{n}{1} x^{n-1}.y^1 + \cdots + \binom{n}{n-1} x^1.y^{n-1} + \binom{n}{n} x^0.y^n$, com $n \in \mathbb{N}$.

$$\binom{n}{0}$$
$$\binom{n}{0}\ \binom{n}{1}$$
$$\binom{n}{0}\ \binom{n}{1}\ \binom{n}{2}$$
$$\vdots\quad \vdots\quad \vdots\quad \ddots$$
$$\binom{n}{0}\ \binom{n}{1}\ \binom{n}{2} \cdots \binom{n}{p}$$

Leituras, filmes e sites

Sites

http://pt.slideshare.net/nathannlucas/06-combinatoria?next_slideshow=1

Referências

CINTRA, Glauber Ferreira. **Matemática I.** Fortaleza: RDS, 2009.

LIMA, E. L.; CARVALHO, P. C. P.; WAGNER, E. E MORGADO, A.C. **A Matemática do Ensino Médio** Vol.2. Rio de Janeiro: SBM, 2004.

LIPSCHUTZ, S; LIPSON, M. **Matemática discreta**. 2 ED. Porto Alegre: Bookman, 2004.

MENEZES, Paulo Blath. **Matemática discreta para computação e informática**. 2 ed. Porto Alegre: Sagra Luzzatto, 2006.

OLIVEIRA, Krerley Irraciel Martins ; FERNÁNDEZ, Adán Jose Corcho. **Iniciação à Matemática**: um curso com problemas e soluções. Rio de Janeiro: SBM, 2010.

ROSEN, Kenneth H. **Matemática Discreta e suas Aplicações** Tradução da 6. ed. em inglês. Mc-Graw Hill, 2009.

Capítulo 4

Teoria dos Números

Objetivos

- Conhecer e aplicar o Princípio de Indução Finita para números naturais e inteiros;
- Compreender o conceito de divisibilidade e suas principais propriedades;
- Reconhecer a divisão com restos;
- Identificar números primos e compostos;
- Compreender os conceitos de fatoração, máximo divisor comum;
- Aplicar conhecimentos de m.d.c. para resolver Equações Diofantinas Lineares;
- Conhecer e aplicar as noções de congruências e suas principais propriedades.

Neste capítulo construiremos axiomaticamente o conjuntos dos números naturais, o que pode ser feito também para o conjunto dos números inteiros, como conjuntos bem ordenados que são. Para simplificar a exposição, optamos por abordar o conjunto nos números naturais. Além da construção, apresentamos algumas propriedades e formas de representações dos naturais.

1. Princípio de Indução Finita

Neste capítulo pretendemos apresentar uma fundamentação teórica do conjunto dos números naturais, bem como suas operações básicas de adição e multiplicação.

$\mathbb{N} = \{0, 1, 2, 3, 4, ...\}$, com as operações de adição $a + b$ e multiplicação $a \cdot b$.

Apresentamos algumas propriedades básicas dos números naturais, ou seja, nossa abordagem partirá de uma lista de axiomas.

(i) A adição e a multiplicação são bem definidas, isto é, para todo $a, b, c, d \in \mathbb{N}$, $a = b$ e $c = d \Rightarrow a + c = b + d$ e $a \cdot c = b \cdot d$.

(ii) A adição e a multiplicação são comutativas, ou seja, para quaisquer $a, b \in \mathbb{N}$, $a + b = b + a$ e $a \cdot b = b \cdot a$.

(iii) A adição e a multiplicação são associativas, para todo $a, b, c \mathbb{N}$, $a + (b + c) = (a + b) + c$ e $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(iv) A adição e a multiplicação possuem elementos neutros, ou seja, para todo $a \in \mathbb{N}$

$a + 0 = a$ e $a \cdot 1 = a$.

(v) A multiplicação possui a propriedade distributiva em relação à adição, quaisquer que sejam a, b, c ∈ N, temos que

$a(b + c) = a \cdot b + a \cdot c$.

Além dos números naturais, outros conjuntos numéricos também satisfazem os axiomas acima, como os números reais não negativos. Para melhor caracterizar o conjunto dos números naturais precisamos introduzir o Axioma de Indução Matemática.

Axioma de indução: Seja A um subconjunto dos números naturais que possui as propriedades

1. $0 \in A$;
2. $\forall\, a \in A \Rightarrow a + 1 \in A$.

Então, A contém todos os números naturais, ou seja, $A = N$.

Uma importante propriedade dos números naturais é o princípio da boa ordenação.

Princípio da boa ordenação: todo subconjunto $A \neq \emptyset$ do conjunto dos números naturais possui um menor elemento, isto é, existe $a \in A$ com a seguinte propriedade: $a \leq n$, para todo $n \in A$.

O conjunto dos números inteiros é formado pelos números positivos, negativos e o zero, com as operações de adição e multiplicação:

$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$

Para facilitar os estudos, abordaremos na maioria das vezes o conjunto dos números naturais, podendo os conceitos aqui estudados serem estendidos ao conjunto dos números inteiros.

Apresentaremos a seguir o Princípio de Indução Finita que será uma ferramenta muito importante na demonstração de teoremas, igualdades, desigualdades e problemas de divisibilidade.

Adotaremos a seguinte notação: se $A \subset N$ e $a \in N$ então $a + A = \{a + x;\ x \in A\}$.

Teorema 1 (Princípio de Indução Finita) – Seja $a \in N$ e $p(n)$ uma propriedade de n, a qual pode ser pensada como uma afirmação que envolve um número n dado. Suponha que

(i) $p(a)$ é verdadeira e

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

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

Demonstração:

Esta demonstração será feita usando o axioma de indução. Considere os subconjuntos de N definidos por $A = \{n \in \mathbb{N};\ p(n)$ é verdadeira$\}$ e $B = \{\, n \in \mathbb{N};\ a + m \in A\}$.

De (i) temos que $a = a + 0 \in A \Rightarrow 0 \in B$

Se $m \in B$, então $a + m \in A$ e por (ii) $a + m + 1 \in A$, donde conclui-se que $m + 1 \in B$. Pelo Axioma de indução, $B = \mathbb{N}$.

Corolário 1 – Não existe nenhum $n \in \mathbb{N}$ tal que $0 < n < 1$, ou seja, a afirmação $p(n)$: se $n > 0 \Rightarrow n \geq 1$, é verdadeira para todo $n \geq 1$.

Demonstração:

$p(1)$ é verdadeira, pois $1 \geq 1$.

Considerando $p(n)$ verdadeira para algum $n \in \mathbb{N}$, mostraremos que $p(n+1)$ também é verdadeira.

Temos que $p(n+1)$: $n + 1 > 0 \Rightarrow n + 1 \geq 1$ é verdade para $n \in \mathbb{N}$, pois $n + 1 \geq 1$ é equivalente a $n \geq 0$, o que já sabemos ser verdadeiro. Pelo Princípio de Indução Finita, a propriedade é verdadeira para todo $n \in \mathbb{N}$.

Observe que neste caso não foi necessário utilizar a hipótese de indução, $p(n)$ é verdade, para verificar o passo indutivo, $p(n + 1)$ é verdade.

Exemplo 1: Utilizando o Princípio de Indução Finita, podemos provar que o conjunto das partes de um conjunto A possui exatamente 2^n elementos, onde $n = n(A)$ é o número de elementos de A.

Consideremos inicialmente que $n = 0$, ou seja, o conjunto A é vazio, tem cardinalidade zero e possui apenas um subconjunto que é ele mesmo, desta forma temos que a afirmação é válida para $n = 0$.

$$2^0 = 1.$$

Tomemos como hipótese de indução que o conjunto A, contendo n elementos, possui 2^n subconjuntos.

Verificando o que acontece quando acrescentamos um elemento ao conjunto A, ou seja, consideramos o conjunto A' que possui $n + 1$ elementos. Os 2^n subconjuntos de A também são subconjuntos de A' e quando acrescentamos a cada subconjunto o novo elemento formamos outros 2^n subconjuntos que são diferentes dos primeiros 2^n. Estes são todos os subconjuntos de A', totalizando

$$2^n + 2^n = 2 \cdot 2^n = 2^{n+1} \text{ subconjuntos.}$$

Portanto a afirmação é válida para todo $n \in \mathbb{N}$.

Exemplo 2: Utilizando o Princípio de Indução Finita, provaremos a fórmula da soma dos n primeiros números naturais não nulos.

Sn = 1 + 2 + ...+ *n*, então $S_n = \frac{n\cdot(n+1)}{2}$

Verificando para *n* = 1, temos que

$S_1 = \frac{1\cdot(1+1)}{2} = \frac{2}{2} = 1$, verdade.

Supondo que a fórmula seja verdadeira para $n \in N^*$, ou seja, a hipótese de indução é que $S_n = \frac{n\cdot(n+1)}{2}$.

Para analisar o que ocorre para *n* + 1, adicionamos este número em ambos os lados da equação:

$$S_n + (n+1) = \frac{n\cdot(n+1)}{2} + (n+1)$$

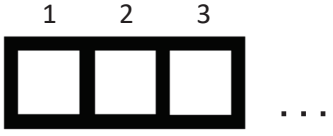
$$S_{n+1} = \frac{n\cdot(n+1)+2\cdot(n+1)}{2}$$

$$S_{n+1} = \frac{(n+1)\cdot(n+2)}{2}$$

$S_{n+1} = \frac{(n+1)\cdot[(n+1)+1]}{2}$ = , verdadeira para *n* + 1.

Portanto, pelo Princípio de Indução, a fórmula é válida para todo $n \in N$.

Exemplo 3: Na construção de quadrados conjugados com palitos, necessitamos de quatro palitos para construir o primeiro quadrado, sete palitos para construir dois quadrados, como mostra a figura, ou seja, acrescentamos três palitos para cada novo quadrado.



. . .

Mostraremos que a fórmula $a_n = 3 \cdot n + 1$ define o número de palitos utilizados na construção de n quadrados.

Verificando a validade da fórmula para *n* = 1.

$a_1 = 3 \cdot 1 + 1 \Rightarrow a_1 = 4$, fórmula válida para *n* = 1.

Supondo a fórmula verdadeira para $n \in N$, ou seja, $a_n = 3 \cdot n + 1$.

Para construir cada quadrado acrescentamos três palitos, assim,

$a_{n+1} = 3 \cdot n + 1 + 3$

$a_{n+1} = 3\cdot(n + 1) + 1$

Donde se conclui que a fórmula é válida para todo $n \in N$.

Para refletir

1. Considere $S_n = 1^2 + 2^2 + \cdots + n^2$. Prove por indução que a soma de n termos, n ∈ N, é dada pela fórmula:
$$S_n = \frac{n\cdot(n+1)\cdot(2n+1)}{6}$$
2. Mostre por indução que $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.
3. Uma sequência de números reais a_n, n ∈ N*, da qual conhecemos o primeiro elemento e $a_n = a_{n-1} + r$, onde r é fixo, é chamada progressão aritmética.
   a) Mostre que $a_n = a_1 + (n - 1) \cdot r$;
   b) Mostre que $S_n = \frac{(a_1 + a_n) \cdot n}{2}$, onde $S_n = a_1 + a_2 + ... + a_n$.
4. Uma sequência de números reais a_n, n ∈ N*, da qual conhecemos o primeiro elemento e $a_n = a_{n-1} \cdot q$, onde $q \neq 0$, $q \neq 1$ é fixo, é chamada progressão geométrica.
   a) Mostre que $a_n = a_1 \cdot q^{n-1}$;
   b) Mostre que que $Sn = \frac{a_1\cdot(q^n - 1)}{q - 1}$, onde $S_n = a_1 + a_2 + ... + a_n$.
5. Encontre as fórmulas para as seguintes somas:
   a) $1 + 2 + 4 + ... + 2^n$;

2. Divisibilidade

Sejam a e b naturais, com $a \neq 0$, dizemos que a divide b, e denotamos por $a|b$, se existe um natural c tal que $b = a \cdot c$. Podemos dizer que a é um divisor de b ou que b é um múltiplo de a. Caso a não divida b escrevemos $a \nmid b$.

De modo análogo, se a e b inteiros, com $a \neq 0$, escrevemos $a|b$, se $b = a \cdot c$, para algum inteiro c.

Exemplo 4: $2|0$; $1|3$; $3 \nmid 5$; $4|4$.

Exemplo 5: Demonstraremos que o número $5^{250} - 3$ não é divisível por 5.

Suponha, por contradição, que $5|5^{250} - 3$. Então existe um número tal que $5^{250} - 3 = 5 \cdot b \Rightarrow 3 = 5^{250} - 5 \cdot b \Rightarrow 3 = 5\,(5^{249} - b) \Rightarrow 5|3$, o que é absurdo!

Concluímos que nossa suposição inicial é falsa, então $5 \nmid 5^{250} - 3$.

Propriedades da divisibilidade

Proposição 1: Se a,b ∈ N* e c ∈ N, temos que:

a) $a|0, 1|c$ e $a|a$;

Demonstração:

$a|0$, pois $a \cdot 0 = 0$

$1|c$, pois $1 \cdot c = c$

$a|a$, pois $a \cdot 1 = a$

b) Se $a|b$ e $b|c$, então $a|c$.

Demonstração:

Se a|b e b|c, então existem $r,s \in$ N, tais que $b = a \cdot r$ e $c = b \cdot s$, substituindo b na segunda igualdade temos que

$c = b \cdot s \Rightarrow c = (a \cdot r) \cdot s \Rightarrow c = a \cdot (r \cdot s) \Rightarrow a|c$.

Proposição 2: Se $a,b,c \in$ N, com $a \neq 0$ e $a|(b + c)$, então $a|b \Leftrightarrow a|c$.

Demonstração: Se a|(b + c), então existe $r \in$ N tal que $b + c = a \cdot r$.

Supondo que a|b, então existe $s \in$ N tal que $b = a \cdot s$.

Substituindo na primeira igualdade, temos que

$$b + c = a \cdot r \Rightarrow a \cdot s + c = a \cdot r \Rightarrow c = a \cdot r - a \cdot s \Rightarrow c = a \cdot (r - s).$$

Como $b \leq b + c \Rightarrow a \cdot s \leq a \cdot r \Rightarrow s \leq r \Rightarrow r - s \geq 0$, ou seja, $r - s \in$ N.

Concluindo que $a|c$. De maneira totalmente análoga podemos provar que se $a|c$ então $a|b$.

Proposição 3: Se $a, b, c, d \in$ N, com $a \neq 0$ e $c \neq 0$, temos que, se $a|b$ e $c|d \Rightarrow a \cdot c|b \cdot d$.

Demonstração: Se $a|b$ e $c|d$, então existem $r, s \in$ N tal que $b = a \cdot r$ e $d = c \cdot s$, então $b \cdot d = (a \cdot r) \cdot (c \cdot s) \Rightarrow b \cdot d = a \cdot c \cdot (r \cdot s)$, portanto $a \cdot c|b \cdot d$.

Proposição 4: Se $a, b, c \in$ N, com $b \geq c$ e $a \neq 0$, tais que $a|(b - c)$, então $a|b \Leftrightarrow a|c$.

Demonstração: Se $a|(b - c)$, então existe $r \in$ N tal que $b - c = a \cdot r$.

Supondo que $a|b$, então existe $s \in$ N tal que $b = a \cdot s$.

Substituindo na primeira igualdade temos que

$$b - c = a \cdot r \Rightarrow a \cdot s - c = a \cdot r \Rightarrow c = a \cdot s - a \cdot r \Rightarrow c = a \cdot (s - r)$$

Como, $b - c \leq b \Rightarrow a \cdot r \leq a \cdot s \Rightarrow r \leq s \Rightarrow s - r \geq 0$, ou seja, $s - r \in$ N.

Concluindo que $a|c$. De maneira totalmente análoga podemos provar que se $a|c$ então $a|b$.

Proposição 5: Sejam $a, b, c, m, n \in$ N, com $a \neq 0$, tais que $a|b$ e $a|c$, então $a|m \cdot b + n \cdot c$.

Demonstração: Se $a|b$, então existe $r \in$ N tal que $b = a \cdot r$.

Sabemos que $a|b$, então existe $s \in$ N tal que $b = a \cdot s$.

Assim, para $m, n \in$ N, temos que

$m \cdot b + n \cdot c = m \cdot (a \cdot r) + n \cdot (a \cdot s) = a \cdot (m \cdot r + n \cdot s) \Rightarrow a|m \cdot b + n \cdot c$.

Note que se considerarmos a condição $m \cdot b \geq n \cdot c$ podemos ainda demonstrar que $a|m \cdot b - n \cdot c$.

Proposição 6: Sejam $a, b \in \mathbb{N}^*$, se $a|b \Rightarrow a \leq b$.

Demonstração: Se a|b, então existe $r \in \mathbb{N}^*$ tal que $b = a \cdot r$.

Como $r \in \mathbb{N}^* \Rightarrow r \geq 1 \Rightarrow a \leq a \cdot r \Rightarrow a \leq b$.

Proposição 7: Sejam $a, b, n \in \mathbb{N}$, com $a > b > 0$. Afirmamos que $a - b | a^n - b^n$.

Demonstração: Verificamos a veracidade para $n = 0$.

Supondo, como hipótese de indução, que a proposição seja válida para n, ou seja, $a - b | a^n - b^n$.

Devemos verificar, como tese de indução, a validade da proposição para $n + 1$.

$a^{n+1} - b^{n+1} = a \cdot a^n - b \cdot b^n$, reescrevendo temos

$a^{n+1} - b^{n+1} = a \cdot a^n - b \cdot a^n + b \cdot a^n - b \cdot b^n = (a - b) \cdot a^n + (a^n - b^n) \cdot b$.

Como $a - b | a - b$ e, por hipótese de indução, $a - b | a^n - b^n$, pela Proposição 5 temos que $a - b$ |(a-b) $\cdot a^n + (a^n - b^n) \cdot$ b.

Logo, o Princípio de Indução implica que o enunciado é válido para todo $n \in \mathbb{N}$.

Proposição 8: Sejam $a, b, n \in \mathbb{N}$, com $a + b \neq 0$. Afirmamos que $a + b | a^{2 \cdot n + 1} + b^{2 \cdot n + 1}$.

Demonstração: De maneira totalmente análoga à demonstração da Proposição 7, utilizando o Princípio de Indução Finita.

Proposição 9: Sejam $a, b, n \in \mathbb{N}$, com $a \geq b > 0$. Afirmamos que $a + b | a^{2 \cdot n} - b^{2 \cdot n}$.

Demonstração: De maneira totalmente análoga à demonstração da Proposição 7, utilizando o Princípio de Indução Finita.

Exemplo 6: Utilizamos o Princípio de Indução para mostrar: $8 | 3^{2 \cdot n} + 7$, para todo $n \in \mathbb{N}$. Considerando $n = 0$

$3^{2 \cdot 0} + 7 = 3^0 + 7 = 1 + 7 = 8$, verdadeiro para $n = 0$, pois 8|8.

Hipótese de indução $8 | 3^{2 \cdot n} + 7$.

Devemos verificar a validade para $n + 1$, ou seja, $8 | 3^{2 \cdot (n+1)} + 7$.

$3^{2 \cdot (n+1)} + 7 = 3^{2 \cdot n + 2} + 7 = 3^2 \cdot 3^{2 \cdot n} + 7 = 3^2 \cdot (3^{2 \cdot n} + 7) - 3^{2 \cdot 7} + 7 = 3^2 \cdot (3^{2 \cdot n} + 7) - 56$

Pela Proposição 5, como 8|56 e $8 | 3^{2 \cdot n} + 7$, temos que $8 | 3^{2 \cdot (n+1)} + 7$.

Pelo Princípio de Indução, verificamos a validade para todo $n \in \mathbb{N}$.

Exemplo 7: Vamos determinar para quais valores de a∈ N, temos $a + 1|a^2 + 2$. Observe que, qualquer número natural satisfaz $a + 1|(a - 1) \cdot (a + 1) = a^2 - 1$. Logo, pela Proposição 5, temos que:

se a satisfaz à propriedade desejada, então $a+1|(a^2 + 2) - (a^2 - 1)$, e assim, $a + 1|3$.

Os divisores positivos de 3 são apenas 1 e 3, logo as únicas possibilidades são $a = 0$ ou $a = 2$. Observe que estes dois valores realmente satisfazem ao enunciado.

Para refletir

1. Sejam $a, c \in \mathbb{N}^*$ e $b \in \mathbb{N}$. Mostre que $a \cdot c | b \cdot c \Leftrightarrow a | b$.
2. Utilize o método de indução finita para mostrar que, para todo $n \in \mathbb{N}$, temos que $9 | 10^n - 1$.
3. Mostre por indução que, para $a > b \geq 0$ e $n \in \mathbb{N}$, $n \geq 2$, temos que
$$\frac{(a^n - b^n)}{a - b} = a^{n-1} + a^{n-2} \cdot b + \cdots + a \cdot b^{n-2} + b^{n-1}$$
4. Determine os valores de a ∈ N que satisfazem $a + 2 | a^3 - 4$.
5. Mostre que $a^5 - a$ é divisível por 5, para todo $a \in \mathbb{N}$. (Use indução)

3. Divisão com resto

Euclides, por volta de 300 a.C., enuncia que é sempre possível efetuar a divisão entre dois números naturais, com divisor diferente de zero, e que se o número não divide exatamente, obtemos um resto. Mais precisamente, temos o seguinte enunciado.

Teorema 2: Sejam $a, b \in \mathbb{N}^*$. Então existem, e são únicos, $q, r \in \mathbb{N}$ tais que

$b = a \cdot q + r$, com $r < a$.

Demonstração: Seja $R = \{b - a \cdot q \in \mathbb{N}^*, q \in \mathbb{N}\}$. Como $b = b - a \cdot 0 \in \mathbb{N}^*$, temos que $b \in R$, logo, R não é vazio.

Pelo Princípio da Boa Ordem, R possui um menor elemento $r = b - a \cdot q$. Desejamos provar que $r \leq a$.

Suponha, por contradição, que $r > a$. Então, existiria $c \in \mathbb{N}^*$ tal que $r = a + c \Rightarrow a + c = b - a \cdot q \Rightarrow c = b - a \cdot (q + 1) \in \mathbb{R}$. Por outro lado, $c < r$ o que contradiz o fato de que r é o menor elemento de R. Sendo assim, $r \leq a$.

Desta forma garantimos a existência de números q e r tal que $b = a \cdot q + r$, com $r \leq a$. Temos duas possibilidades: $r = a$ e $a|b$, ou $r < a$. O que encerra a parte da existência do enunciado do teorema. Para verificar a unicidade, consideremos r_1 e r_2 elementos distintos de R, com $r_1 < r_2 <$ a, então existem $q_1, q_2 \in \mathbb{N}$, tais que

$r_1 = b - a \cdot q_1$ e $r_2 = b - a \cdot q_2$

$r_2 - r_1 = b - a \cdot q_2 - b + a \cdot q_1$

$= a \cdot (q_1 - q_2)$, então $r_2 - r_1 \geq a \Rightarrow r_2 \geq r_1 + a \geq a$, o que é absurdo, pois $r_2 < a$.

Logo, $r_1 = r_2$. O que mostra a unicidade dos restos. Diante disto, é imediato verificar a unicidade dos quocientes.

Vale ressaltar que todo número $n \in \mathbb{N}$ será da forma $2 \cdot n$ quando for par e $2 \cdot n + 1$ quando for ímpar.

De modo geral, para todo $n \in \mathbb{N}$ e $m \geq 2$, podemos escrever, de maneira única, $n = m \cdot k + r$, com $k, r \in \mathbb{N}$ e $r < m$.

Em particular, todo número pode ser escrito em função de um múltiplo de um outro número dado mais um resto. Podemos escrever, por exemplo: todo número pode ser escrito em uma das formas

$$4 \cdot n,\ 4 \cdot n + 1,\ 4 \cdot n + 2 \text{ ou } 4 \cdot n + 3.$$

Exemplo 8: Podemos determinar o quociente e o resto da divisão de 35 por 6.

$$35 = 6 \cdot 5 + 5 \Rightarrow q = 5 \text{ e } r = 5.$$

Corolário 2: Sejam $a, b \in \mathbb{N}$ com $1 < a \leq b$, existe $n \in \mathbb{N}$ tal que

$$n \cdot a \leq b < (n+1) \cdot a$$

Demonstração: Pelo Teorema de Euclides, Teorema 2 acima, sabemos que existem, e são únicos, $n, r \in \mathbb{N}$, com $0 \leq r < a$ tais que

$$b = a \cdot n + r$$

Desta forma,

$$n \cdot a \leq b = n \cdot a + r < n \cdot a + a = (n + 1) \cdot a$$

Exemplo 9: Consideremos $a = 5$ e $b = 18$, podemos escrever

$$5 \cdot 3 < 18 < 5 \cdot 4$$

Exemplo 10: Seja $b = 7 \cdot q + 5$, com $q < b$. Desejamos encontrar o resto da divisão de $10 \cdot b + 1$ por 7.

$10 \cdot b = 70 \cdot q + 50$

$10 \cdot b + 1 = 70 \cdot q + 50 + 1$

$= 70 \cdot q + 7 \cdot 7 + 2$

$= 7 \cdot (10 \cdot q + 7) + 2$

Logo, o resto da divisão de $10 \cdot b + 1$ por 7 é r = 2.

Proposição 10: Sejam $a, b, c \in \mathbb{N}$, com $a \in \mathbb{N}^*$. Sejam r e s os restos das divisões de b e c por a, respectivamente. Então, o resto da divisão de $b \cdot c$ por a é igual ao resto da divisão de $r \cdot s$ por a.

Demonstração:

Temos que $b = a \cdot q + r$ e $c = a \cdot t + s$, onde q e t são os respectivos quocientes. Então

$$b \cdot c = (a \cdot q + r)(a \cdot t + s) = a \cdot Q + r \cdot s$$

onde $Q = a \cdot q \cdot t + q \cdot s + r \cdot t$. Logo, a demonstração segue pela unicidade do Teorema 2.

Exemplo 11: O produto de dois números naturais consecutivos é sempre divisível por 2.

Considere $n \in \mathbb{N}$, n+1 é o seu consecutivo e $a = n \cdot (n + 1)$. Desejamos mostrar que $2 | n \cdot (n + 1)$. Podemos escrever todos os números naturais na forma $2 \cdot n$ e $2 \cdot n + 1$, isto é, o resto da divisão de n por 2 é 0 ou 1.

Quando $r = 0$, o resto da divisão de a por 2 é o mesmo resto da divisão de $0 \cdot (0 + 1) = 0$ por 2, ou seja, $2|a$. A igualdade dos restos é consequência da Proposição 10.

Quando $r = 1$, o resto da divisão de a por 2 é igual ao resto da divisão de $1 \cdot (1 + 1) = 1 \cdot 2 = 2$ por 2, ou seja, $2|a$. Concluímos que, em qualquer dos casos, $2|a$ para todo $n \in \mathbb{N}$.

Para refletir

1. Para $a = 55$ e $b = 6$, determine o quociente e o resto da divisão, satisfazendo o Teorema de divisões de Euclides.
2. Mostre que, para $a \in \mathbb{N}$ e $n \in \mathbb{N}^*$, a é par, se e somente se, a^n é par.
3. (ENC-2001) Seja n um número natural; prove que a divisão de n^2 por 6 nunca deixa resto 2.
4. (ENC-2002) O resto da divisão do inteiro n por 20 é 8. Qual é o resto da divisão de n por 5?

4. Números Primos

Definição: Um número natural $a > 1$ é chamado de número primo se possui somente dois divisores naturais. Se $a > 1$ não é primo, dizemos que ele é um número composto.

Exemplo 12: Mostraremos que 2 é o único número primo que pode ser escrito da forma $a^3 + 1$.

Temos que 2 é um número primo, visto que só é divisível por 1 e por 2. Podemos escrever o número $2 = 1^3 + 1$.

Consideremos $a > 1$, temos, pela Proposição 8, que os números da forma podem ser divididos por $a + 1$. Se $a^3 + 1$ fosse um número primo então teríamos que $a + 1 = 1$ ou $a+1= a^3 + 1 \Rightarrow a = 0$ ou $a = 1$, mas $a > 1$, logo $a^3 + 1$ não é primo.

Para refletir

1. Considerando que p é primo e p, $p + 2$ e $p + 4$ são números primos, mostre que $p = 3$.
2. Mostre que todo $n \in \mathbb{N}$, com $n > 11$ é a soma de dois números compostos.
3. Verifique se o número $2^{20} - 5^8$ é primo ou composto.

5. Equações Diofantinas Lineares

Sejam $a, b \in \mathbb{Z}^*$ e $c \in \mathbb{Z}$. Chamamos de Equação Diofantina Linear a equação do tipo

$$a \cdot x + b \cdot y = c.$$

Os pares (x, y), com $x, y \in \mathbb{Z}$, que satisfazem a equação são chamados de soluções da equação, ou seja, as soluções são os pontos de coordenadas inteiras na reta que representa a equação.

Dos problemas de divisibilidade surgem conceitos importantes como o Máximo Divisor Comum (m.d.c.) e o Mínimo Múltiplo Comum (m.m.c). Neste caso, estamos interessados na definição do m.d.c. que nos ajudará a encontrar as soluções das Equações Diofantinas Lineares.

Definição: O Máximo Divisor Comum (m.d.c.) entre os números $a, b \in \mathbb{Z}^*$ é um número $d \in \mathbb{Z}$ tal que

i) $d|a$ e $d|b$;

ii) d é o maior com a propriedade (i), o que implica que d é divisível por todos os divisores comuns de a e b.

Denotamos por $d = (a, b)$ o m.d.c. entre a e b.

Proposição 11: Seja $d = (a, b)$ o m.d.c. de a e b. Então os números inteiros $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si, ou seja, $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Demosntração: O fato de que as frações acima são números inteiros é uma consequência imediata de que *d* divide *a* e *b*. Suponha, por contradição, que $c = \left(\frac{a}{d}, \frac{b}{d}\right)$ é maior que 1. Temos ainda que $c \mid \frac{a}{d}$ implica que $c \cdot d | a$. De modo análogo, $c \cdot d | b$. Portanto, $c \cdot d$ é um divisor comum de *a* e *b* que é estritamente maior que *d*, pois $c > 1$. O que contradiz a escolha de *d* como o m.d.c. entre os números *a* e *b*. Donde concluímos que $c = 1$, e a demonstração está completa.

Enunciamos o Teorema de Bachet-Bêzout, este resultado é uma consequência do Algorítmo de Euclides que será discutido nesta seção. Este resultado será utilizado para garantir a existência de soluções de Equações Diofantinas Lineares.

Teorema 3: Seja $d = (a, b)$ o m.d.c. de *a* e *b*, então existem $x_o, y_o \in Z$ tais que $d = a \cdot x_o + b \cdot y_o$.

Em seguida, aplicaremos o Teorema 3 na resolução de equações diofantinas lineares.

Proposição 12: Sejam $a, b, c \in Z$, com a 0 e $b \neq 0$. A equação diofantina linear $a \cdot x + b \cdot y = c$ possui solução se, e somente se, $d = (a, b) | c$. Se (x_1, y_1) é uma solução da equação, então o conjunto dos pares que são soluções da equação são do tipo

$$\left(x_1 + t \cdot \frac{b}{d}, y_1 - t \cdot \frac{a}{d}\right) \text{ com t} \in Z.$$

Demonstração: Vamos mostrar que se a equação diofantina possui solução então $d = (a, b) | c$. Considere (x_1, y_1) uma solução inteira da equação diofantina linear e seja $d = (a, b)$ o m.d.c. de *a* e *b*. Desta forma:

$$a \cdot x_1 + b \cdot y_1 = c$$

Como d|a e d|b existem $k_1, k_2 \in Z$ tais que $a = d \cdot k_1$ e $b = d \cdot k_2$.

Substituindo na equação, temos:

$$d \cdot k_1 \cdot x_1 + d \cdot k_2 \cdot y_1 = c$$
$$d \cdot (k_1 \cdot x_1 + k_2 \cdot y_1) = c \Rightarrow d | c$$

Devemos mostrar também que se $d | c$, então existe solução. O Teorema de Bêzout afirma que existem $x_o, y_o \in Z$ tais que

$$d = a \cdot x_o + b \cdot y_o$$

Se $d|c$ então existe $k \in Z$ tal que $c = k \cdot d$. Multiplicando a equação acima por k, obtemos

$$k \cdot d = a \cdot k \cdot x_o + b \cdot k \cdot y_o$$
$$a \cdot (k \cdot x_o) + b \cdot (k \cdot y_o) = c$$

Donde conclui-se que a equação diofantina tem solução.

Estamos interessados ainda em mostrar que, quando existem, as soluções são infinitas e podemos apresentar uma forma para o conjunto solução.

Consideremos (x, y) uma solução, possivelmente diferente de (x_1, y_1). Podemos escrever que

$$a \cdot x + b \cdot y = c \text{ e } a \cdot x_1 + b \cdot y_1 = c$$
$$a \cdot x + b \cdot y = a \cdot x_1 + b \cdot y_1$$
$$a \cdot (x - x_1) = b \cdot (y_1 - y)$$

Dividindo por d, temos

$$\frac{a}{d} \cdot (x - x_1) = \frac{b}{d} \cdot (y_1 - y).$$

Pela Proposição 11, sabemos que $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, logo estas frações são primas entre si e podemos concluir

$\frac{a}{d}|(y_1 - y) \Rightarrow$ existe t tal que $y_1 - y = \frac{a}{d}\ t$, e

$\frac{b}{d}|(x - x_1) \Rightarrow$ existe s tal que $x - x_1 = \frac{b}{d} \cdot s$.

Pela relações que temos é imediato verificar que $s = t$ é igual ao quociente das divisões de $(y_1 - y)$ por $\frac{a}{d}$, ou de $(x - x_1)$ por $\frac{b}{d}$.

Podemos verificar facilmente que $x = x_1 + t \cdot \frac{b}{d}$ e $y = y_1 - t \cdot \frac{a}{d}$ são soluções da equação diofantina linear $a \cdot x + b \cdot y = c$, para todo $t \in Z$. O que encerra a demonstração.

Exemplo 13: Verifiquemos se as Equações Diofantinas Lineares possuem soluções inteiras:

a) $2 \cdot x + 18 \cdot y = 234$

mdc (2,18)=2 e 2|234, logo a equação possui soluções inteiras.

b) $5 \cdot x + 3 \cdot y = 50$

mdc (5,3)=1 e 1|50, logo a equação possui soluções inteiras.

c) $5 \cdot x + 15 \cdot y = 23$

mdc (5, 15) = 5 e 5ł23, logo a equação não possui soluções inteiras.

Exemplo 14: Podemos determinar todas as soluções inteiras da equação $3 \cdot x + 5 \cdot y = 50$ e apresentar soluções em que $x, y \in N$.

Sabemos que a equação possui soluções inteiras pois, mdc (3, 5) = 1 e 1|50.

Podemos determinar facilmente, por tentativa, uma solução. O par (0, 10) é solução da equação.

Utilizando a Proposição 12, temos que

$x_1 = 0 + \frac{5}{1} \cdot t = 5t$ e $y_1 = 10 - \frac{3}{1} \cdot t = 10 - 3t$, com $t \in Z$, são as soluções inteiras da equação.

Podemos identificar que para t=0, 1, 2, 3 as soluções são pares de números naturais, que são (0, 10), (5, 7), (10, 4) e (15, 1). Portanto, existem quatro pares de inteiros positivos que resolvem a equação diofantina acima apresentada.

Lema 1: (Lema de Euclides) Se $a, b, n \in N$, com $a < n \cdot a < b$. Então $(a, b - n \cdot a) = (a, b)$.

Demonstração: Seja $d = (a, b - n \cdot a)$. Então $d|a$ e $d|b - n \cdot a$. Pela Proposição 5,

$$d|(b - n \cdot a) + n \cdot a = b.$$

Logo, d é divisor comum de a e b, o que implica que $d|(a, b)$.

Seja $d_1=(a,b)$. Temos que $d_1|a$ e $d_1|b$, e, pela Proposição 5, concluímos que $d_1|b - n \cdot a$. Logo, d_1 é divisor comum de a e $b - n \cdot a$, o que implica que $d_1|d$.

Portanto, $d|d_1$ e $d_1|d$ implicam que $d_1 = d$, ou seja, $(a, b - n \cdot a) = (a, b)$.

Algoritmo de Euclides

Sejam $a, b \in N$, supondo $a \leq b$, sem perda de generalidade. Sabemos que nos casos $a = 1$, $a = b$ e $a|b$, temos $(a, b) = a$. Se ałb, temos que

$b = a \cdot q_1 + r_1$, com $r_1 < a$.

Se $r_1|a$, pelo Lema 1,

$$r_1 = (a, r_1) = (a, b - a \cdot q_1) = (a, b).$$

Se r_1ła, então

$a = r_1 \cdot q_2 + r_2$, com $r_2 < r_1$.

Se $r_2|r_1$, pelo Lema 1

$$r_2 = (r_1, r_2) = (r_1, a - r_1 \cdot q_2) = (r_1, a) = (a, b).$$

Poderemos repetir este procedimento uma quantidade finita de vezes, pois pelo Princípio da boa ordem a sequência $a > r_1 > r_2 \ldots$ possui um menor elemento, o que implica que para algum $n \in \mathbb{N}$, $r_n | r_{n-1}$. Quando isto acontecer, teremos que $r_n = (a, b)$.

Exemplo 15: Determinamos o m.d.c. dos números 270 e 345, utilizando o Algoritmo de Euclides.

	$q_1 = 1$	$q_2 = 3$	$q_3 = 1$	$q_4 = 1$	$q_5 = 2$	
345	270	75	45	30	15	← mdc
$r_1 = 75$	$r_2 = 45$	$r_3 = 30$	$r_4 = 15$	$r_5 = 0$		

O algoritmo de Euclides também pode ser utilizado para expressar o m.d.c. como combinação linear dos números dados, como enunciado no Toerema 3. De fato, a demonstração deste resultado é uma aplicação do algoritmo de Euclides. Vejamos um exemplo.

Exemplo 16: Escrevemos, utilizando o Algoritmo de Euclides, o número como combinação linear dos números 345 e 270.

Utilizamos os resultados do Algoritmo de trás para frente, temos:

$$15 = 45 - 1 \cdot 30$$
$$15 = 45 - 1 \cdot (75 - 1 \cdot 45)$$
$$15 = -1 \cdot 75 + 2 \cdot 45$$
$$15 = -1 \cdot 75 + 2 \cdot (270 - 3 \cdot 75)$$
$$15 = 2 \cdot 270 - 7 \cdot 75$$
$$15 = 2 \cdot 270 - 7 \cdot (345 - 1 \cdot 270)$$
$$15 = -7 \cdot 345 + 9 \cdot 270$$

Em particular, a utilização do Algoritmo de Euclides possibilita a determinação de uma solução inteira para as equações diofantinas lineares.

Para refletir

1. Resolva as equações:
   a) $5 \cdot x + 7 \cdot y = 100$
   b) $7 \cdot x + 11 \cdot y = 116$
2. Calcule o m.d.c. dos números:
   a) 246 e 384
   b) 234 e 542
   c) 648 e 1218
3. De quantas maneiras podemos comprar selos de R$ 10,00 e R$ 14,00 se desejamos gastar exatamente R$ 100,00?

6. Fatoração

Nesta seção apresentaremos o Teorema Fundamental da Aritmética. Segundo o qual, todo número admite fatoração única como produto de primos. A fim de apresentar este resultado usaremos o seguinte lema.

Lema 2: Sejam p, m e n números inteiros. Se p é primo e $p|m \cdot n$, então $p|m$ ou $p|n$.

Demonstração: Suponha que $p \nmid m$. Como p é primo, temos que $(p, m) = 1$. Pelo Teorema 3, sabemos que existem inteiros x_o, $y_o \in Z$ tais que

$$1 = p \cdot x_o + m \cdot y_o.$$

Multiplicando ambos os lados desta equação por n, temos $n = p \cdot n \cdot x_o + m \cdot n \cdot y_o$. E pela Proposição 5, concluímos que $p|n$. Isto encerra a demonstração.

Com isto, podemos demonstrar o Teorema Fundamental da Aritmética.

Teorema 4: (Teorema Fundamental da Aritmética) Todo número $n \in N$, com $n > 1$, pode ser representado de maneira única, a menos da ordem, como um produto de fatores primos.

Demonstração: Considerando n um número primo, não precisamos demonstrar nada.

Consideremos agora o caso em que n não seja primo, garantimos que existe um número primo $p_1 > 1$ que é o menor divisor de n. Se o menor divisor de n, que existe pelo Princípio da boa ordenação, não fosse primo existiria um número p, com $1 < p < p_1$ tal que $p|p_1$. Neste caso, teríamos $p|p_1$ e $p_1|n$, logo, $p|n$ contradizendo o fato de que p_1 é o menor divisor de n. Desta forma, podemos escrever que

$$n = p_1 \cdot n_1.$$

Se n_1 for primo p será um produto de fatores primos, concluindo a demonstração. Se n_1 não for primo, de maneira análoga ao raciocínio acima, garantimos que existe um número primo $p_2 > 1$ que é o menor divisor de n_1. Desta forma escrevemos que

$$n = p_1 \cdot p_2 \cdot n_2.$$

Podemos repetir este processo uma quantidade finita de vezes, considerando que $n_1 > n_2 > n_3 > \cdots > n_m$. Como esta sequencia é estritamente decrescente, o processo deve acabar depois de uma quantidade finita de iterações. Observe que os primos $p_1, p_2, \ldots p_r$ não são necessariamente distintos, podemos escrever que

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_r^{a_r}.$$

Necessitamos demonstrar ainda, que este produto é único, a menos da ordem. Usaremos o princípio de indução.

Como $n \in \mathbb{N}$, com $n > 1$, verificamos a veracidade para $n = 2$.

Consideremos, como hipótese de indução, que a afirmação é verdadeira para todo os números menores que n. Devemos mostrar a veracidade para n.

Se n for primo, a afirmação é verdadeira pois n só tem a fatoração óbvia. Considerando que n seja composto e possua duas fatorações distintas, podemos escrever que

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r = q_1 \cdot q_2 \cdot \ldots \cdot q_s.$$

Como $p_1 | q_1 \cdot q_2 \cdot \ldots \cdot q_s$, pelo Lema 2, ele divide algum dos fatores. Sem perda de generalidade, podemos supor que $p_1 | q_1$, mas p_1 e q_1 são primos, logo $p_1 = q_1$.

$$\frac{n}{p_1} = p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot q_s.$$

Como $1 < \frac{n}{p_1} < n$, por hipótese de indução possui uma única fatoração, o que significa que r=s e, a menos de uma reordenação, $p_1 = q_1$, $p_2 = q_2$, …, $p_r = q_r$.

Exemplo 17: Se 2 aparece na fatoração de um número n, podemos concluir que n é da forma $2 \cdot k$, o que garante que n é par. Demonstraremos que se n é par, então o número 2 aparece na fatoração de n.

De fato, se n é par, então também podemos escrever que $n = 2 \cdot k$, para algum número natural k. Consideremos as fatorações

$n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_r^{a_r}$ e $k = q_1^{b_1} \cdot q_2^{b_2} \cdot q_3^{b_3} \cdot \ldots \cdot q_s^{b_s}$.

Desta forma,

$$p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_r^{a_r} = 2 \cdot q_1^{b_1} \cdot q_2^{b_2} \cdot q_3^{b_3} \cdot \ldots \cdot q_s^{b_s}.$$

O número 2 aparece na fatoração, pois como a fatoração é única, algum dos números p_i é igual a 2.

Para refletir

1. Verifique se o número $2^5 \cdot 5$ é um múltiplo de 10.
2. Sabendo que o número $3 \cdot x$ é divisível por 5, podemos afirmar que x é divisível por 5?
3. Encontre dois números naturais x e y, de tal forma que $x^2 - y^2 = 17$.
4. (ENC-2002) Qual é o menor valor do número natural n que torna $n!$ divisível por 1000?

7. Congruências

Finalizamos o capítulo com a aritmética dos restos, introduzida por Gauss.

Definição: Sejam $a, b, m \in \mathbb{N}$, com $m \neq 0$. Dizemos que a e b são congruentes módulo m se os restos de suas divisões por m são iguais. Escrevemos

$$a \equiv b \bmod m$$

Exemplo 18: Os números 43 e 28 são congruentes módulo 5.

Observamos que na divisão euclidiana de 43 por 5 e de 28 por 5 encontramos o mesmo resto igual a 3, portanto

$$43 \equiv 28 \bmod 5$$

Proposição 13: Sejam $a, b, c, m \in \mathbb{N}$, com $m > 1$, temos que

(i) $a \equiv a \bmod m$

(ii) $a \equiv b \bmod m$, então $b \equiv a \bmod m$

(iii) $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $a \equiv c \bmod m$

Demonstração: Decorre diretamente da definição.

Com a propriedade a seguir torna-se desnecessária a divisão dos números para a comparação dos restos.

Proposição 14: Sejam $a, b, m \in \mathbb{N}$, com $m \neq 0$ e $a \geq b$, então $a \equiv b \bmod m$ se, e somente se, $m|a - b$.

Demonstração: Considere $a = m \cdot q + r$ e $b = m \cdot q_1 + r_1$, com $r, r_1 < m$.

Temos que

$$a - b = m \cdot (q - q_1) + (r - r_1),$$

com $-m < r - r_1 < m$. É imediato verificar que $m|a - b$ se, e somente se, $m|r - r_1$. Como $r - r_1$ é um inteiro maior que $-m$ e menor que m, vemos que $m|r - r_1$ se, e só se, $r = r_1$.

Donde concluímos que $m|a - b$ se, e somente se, $r = r_1$, ou seja, $a \equiv b \bmod m$.

Exemplo 19: Utilizando a Proposição 14, mostramos que $43 \equiv 29 \bmod 7$.

$43 - 29 = 14$ e $7|14$, logo $43 \equiv 29 \bmod 7$.

Todo número natural, quando dividido por m, é congruente a um dos números 0, 1, 2, …, $m - 1$. As operações de adição e multiplicação nas congruências são equivalentes às operações com inteiros.

Proposição 15: Se $a, b, c, d, m \in \mathbb{N}$ e $m > 1$, temos que:

(i) $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a + c \equiv b + d \bmod m$

(ii) $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a \cdot c \equiv b \cdot d \bmod m$

Demonstração: Podemos supor, sem perda de generalidade, que $a \geq b$ e $c \geq d$, logo

$m|a - b$ e $m|c - d$ e temos que

(i) $m|(a - b) + (c - d) \Rightarrow m|(a + c) - (b + d) \Rightarrow a + c \equiv b + d \bmod m$

(ii) $m|c \cdot (a - b) + b \cdot (c - d) = a \cdot c - b \cdot d \Rightarrow a \cdot c \equiv b \cdot d \bmod m$.

Exemplo 20: Desejamos encontrar o resto da divisão de $1 + 2 + 2^2 + \cdots + 20^{20}$ por 4.

Temos que

$1 \equiv 1 \bmod 4$, $2 \equiv 2 \bmod 4$, $2^2 = 4 \equiv 0 \bmod 4$, $2^3 = 8 \equiv 0 \bmod 4$, ... , $2^{20} = 8 \equiv 0 \bmod 4$

Note que a partir de 2^2 os demais termos são todos múltiplos de 4 e deixam resto 0 na divisão por 4.

Assim, utilizando a Proposição 15 (i), temos que

$$1 + 2 + 2^2 + \cdots + 20^{20} \equiv 1 + 2 + 0 + \cdots + 0 \bmod 4 \equiv 3 \bmod 4$$

Concluímos que o resto da divisão é 3.

Atividades de avaliação

1. (ENC 2000) Se $x^2 \equiv 1 \bmod 5$, então,

a) $x \equiv 1 \bmod 5$

b) $x \equiv 2 \bmod 5$

c) $x \equiv 4 \bmod 5$

d) $x \equiv 1 \bmod 5$ ou $x \equiv 4 \bmod 5$

e) $x \equiv 2 \bmod 5$ ou $x \equiv 4 \bmod 5$

2. Encontre o resto da divisão de $1! + 2! + \cdots + 100!$ por 40.

Síntese do capítulo

Neste capítulo apresentamos o conjunto dos números naturais, bem como suas operações básicas de adição e multiplicação. $N = \{0, 1, 2, 3, 4, ...\}$, com as operações de adição $a + b$ e multiplicação $a \cdot b$, bem como o princípio da boa ordenação.

Enunciamos e aplicamos o axima de indução: seja A um subconjunto dos números naturais que possui as propriedades

(i) $0 \in A$;

(ii) $\forall\, a \in A \Rightarrow a + 1 \in A$.

Então, A contém todos os números naturais, ou seja, A = N.

Apresentamos o conjunto dos números inteiros $Z = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$

Enunciamos e demonstramos o Princípio de Indução Finita que é uma forte ferramenta na demonstração de teoremas, igualdades, desigualdades e problemas de divisibilidade.

Teorema 1 (Princípio de Indução Finita) – Seja $a \in N$ e $p(n)$ uma propriedade de n, a qual pode ser pensada como uma afirmação que envolve um número n dado. Suponha que

(i) $p(a)$ é verdadeira e

(ii) se $p(n)$ é verdadeira $\Rightarrow p(n + 1)$ é verdadeira, $\forall\, n \geq a$

Teorema 2: Sejam $a, b \in N^*$. Então existem, e são únicos, $q, r \in N$ tais que

$b = a \cdot q + r$, com $r < a$.

Definimos que um número natural $a > 1$ é chamado de número primo se possui somente dois divisores naturais. Se a não é primo, dizemos que ele é um número composto.

Sejam $a, b \in Z^*$ e $c \in Z$. Chamamos de Equação Diofantina Linear a equação do tipo

$$a \cdot x + b \cdot y = c.$$

Os pares (x, y), com $x, y \in Z$, que satisfazem a equação são chamados de soluções da equação, ou seja, as soluções são os pontos de coordenadas inteiras na reta que representa a equação.

Definimos o Máximo Divisor Comum (m.d.c.) entre os números $a, b \in Z^*$ é um número $d \in Z$ tal que

(i) $d|a$ e $d|b$;

(ii) d é o maior com a propriedade (i), o que implica que d é divisível por todos os divisores comuns de a e b

Teorema 3: Seja $d = (a, b)$ o m.d.c. de a e b, então existem $x_o, y_o \in Z$ tais que $d = a \cdot x_o + b \cdot y_o$.

Ressaltamos um resultado importante dado na proposição 12. Sejam $a, b, c \in Z$, com $a \neq 0$ e $b \neq 0$. A equação diofantina linear $a \cdot x + b \cdot y = c$ possui solução se, e somente se, $d = (a, b) | c$. Se (x_1, y_1) é uma solução da equação, então o conjunto dos pares que são soluções da equação são do tipo

$$\left(x_1 + t \cdot \frac{b}{d}, y_1 - t \cdot \frac{a}{d}\right) \text{ com } t \in \mathbb{Z}.$$

Teorema 4: (Teorema Fundamental da Aritmética) Todo número $n \in N$, com $n > 1$, pode ser representado de maneira única, a menos da ordem, como um produto de fatores primos.

Definimos, considerndo $a, b, m \in N$, com $m \neq 0$, que a e b são congruentes módulo m se os restos de suas divisões por m são iguais. Escrevemos

$$a \equiv b \bmod m.$$

Leituras, filmes e sites

Sites

http://docslide.com.br/documents/matematica-discreta-para-computacao-e-informatica-paulo-blauth-menezes.html

http://homepages.dcc.ufmg.br/~loureiro/md/md_0Introducao.pdf

http://www.dsc.ufcg.edu.br/~ulrich/disciplinas/MaDi.html

Referências

HEFEZ, Abramo. **Elementos de Aritmética**. 2 ed. Rio de Janeiro: SBM, 2011.

MENEZES, Paulo Blath. **Matemática discreta para computação e informática**. 2 ed. Porto Alegre: Sagra Luzzatto, 2005.

OLIVEIRA, Kreley Irraciel Martins; FERNÁNDEZ, Adán Jose Corcho. **Iniciação à Matemática**: um curso com problemas e soluções. Rio de Janeiro: SBM, 2010.

SANTOS, José Plínio de Oliveira. **Introdução à Teoria dos Números**. 2 ed. Rio de Janeiro: SBM, 2010.

Capítulo 5

Objetivos

- Definir, apresentar propriedades e exemplos de grupos;
- Definir e apresentar exemplos de subgrupos, homomorfismos e isomorfismos;
- Definir, apresentar propriedades e exemplos de anéis;
- Definir, subanéis, ideais e anéis quocientes;
- Definir, apresentar propriedades e exemplos de corpos.

No capítulo 4 definimos, através de axiomas, o conjunto dos números naturais suas propriedades e formas de representações, que podem ser estendidas ao conjunto dos números inteiros. Observamos, ainda, divisões que não são exatas e sentimos a necessidade de formalizar a estrutura destes conjuntos. Neste capítulo, apresentamos definições básicas e conceitos que possibilitarão uma introdução ao estudo dessas estruturas algébricas.

1. Definição e propriedades dos grupos

Definição: Seja G um conjunto, munido de uma operação $(G, \cdot)$. Neste ponto, a operação pode ser pensada como um produto ou uma soma entre dois números, por exemplo. Em geral, $\cdot$ é uma operação abstrata definida para pares de elementos de G. Dizemos que G é um grupo de satisfaz as propriedades:

(i) O conjunto é fechado, ou seja, para todo $a, b \in G$

$a \cdot b \in G$.

(ii) A operação é associativa, ou seja, para todo $a, b, c \in G$

$a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(iii) Existe elemento neutro em relação a operação, isto é, existe $e \in G$, tal que

$a \cdot e = e \cdot a = a$, para todo $a \in G$.

(iv) Para cada $a \in G$, existe $b \in G$, chamado de inverso em relação à operação, tal que

$a \cdot b = b \cdot a = e$.

O grupo será chamado de comutativo ou abeliano se, além das propriedades já citadas, possuir a propriedade a seguir.

(v) A operação é comutativa, isto é, para todo $a, b \in G$ temos que

$a \cdot b = b \cdot a$.

Exemplo 1: O conjunto dos números inteiros com a operação de adição é um grupo abeliano, isto é, (Z, +) é um grupo abeliano. O elemento neutro é o número zero e para cada $n \in Z$, o inverso de n neste grupo é dado por $-n$.

Exemplo 2: O conjunto dos números inteiros com a operação de multiplicação não é grupo pois não possui elemento inverso.

Exemplo 3: O conjunto dos inteiros ímpares com relação a operação da adição não é grupo, pois não é fechado, ou seja, dados dois números ímpares $2 \cdot m + 1$ e $2 \cdot n + 1$, temos que

$2 \cdot m + 1 + 2 \cdot n + 1 = 2 \cdot (m + n + 1)$ que é par.

Exemplo 4: O conjunto dos números inteiros congruentes módulo 6 com a operação de adição é um grupo. Uma maneira formal de descrever este grupo é utilizando as relações de equivalências introduzidas no início do material. Definimos em Z a relação de equivalência que m é equivalente a n se $m \equiv n \bmod 6$. O conjunto que estamos tratando neste exemplo é o conjunto das classes de equivalência dessa relação, o qual pode ser descrito por $Z_6 = \{0, 1, 2, 3, 4, 5\}$. Aqui, 2 representa a classe dos inteiros que deixam resto 2 quando divididos por 6. A operação de adição usual dos inteiros induz a seguinte operação em Z_6:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	$6 \equiv 0 \bmod 6$
2	2	3	4	5	$6 \equiv 0 \bmod 6$	$7 \equiv 1 \bmod 6$
3	3	4	5	$6 \equiv 0 \bmod 6$	$7 \equiv 1 \bmod 6$	$8 \equiv 2 \bmod 6$
4	4	5	$6 \equiv 0 \bmod 6$	$7 \equiv 1 \bmod 6$	$8 \equiv 2 \bmod 6$	$9 \equiv 3 \bmod 6$
5	5	$6 \equiv 0 \bmod 6$	$7 \equiv 1 \bmod 6$	$8 \equiv 2 \bmod 6$	$9 \equiv 3 \bmod 6$	$10 \equiv 4 \bmod 6$

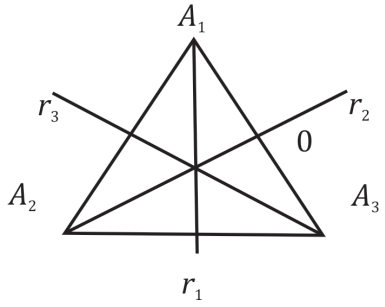
Essa operação é comutativa, associativa, 0 é o elemento neutro e todo elemento possui um inverso, logo $(Z_6,+)$ é um grupo abeliano.

Exemplo 5: O conjunto S_Δ das simetrias espaciais de um triângulo equilátero é um grupo.

Considere o triângulo equilátero A_1, A_2, A_3, com centro de gravidade na origem e as retas r_1, r_2, r_3 passando pelas medianas do triângulo, como na figura abaixo.

Podemos descrever as transformações espaciais que preservam o triângulo:

- id, R_{120}, R_{240} (rotações centradas no 0 e no sentido anti-horário); id é a identidade, e R_{120} e R_{240} são as rotações de120º e 240º, respectivamente;
- R_1, R_2, R_3 (reflexões relativas às retas r_1, r_2, r_3, as quais podem ser vistas como rotações espaciais de180º relativas aos respectivos eixos).



O conjunto $S_\Delta = \{id, R_{120}, R_{240}, R_1, R_2, R_3\}$ com a operação de composição de funções é um grupo. Na tabela abaixo, a composição da simetria indicada na primeira linha com a simetria da primeira coluna esta representada na respectiva lacuna. Por exemplo, $R_{120} \circ R_1 = R_2$, corresponde à informação contida na lacuna associada a coluna da rotação R_{120} e linha do reflexão R_1.

$\circ$	id	R_{120}	R_{240}	R_1	R_2	R_3
id	id	R_{120}	R_{240}	R_1	R_2	R_3
R_{120}	R_{120}	R_{240}	id	R_3	R_1	R_2
R_{240}	R_{240}	id	R_{120}	R_2	R_3	R_1
R_1	R_1	R_2	R_3	id	R_{120}	R_{240}
R_2	R_2	R_3	R_1	R_{240}	id	R_{120}
R_3	R_3	R_1	R_2	R_{120}	R_{240}	id

Propriedades dos grupos:

1. O elemento neutro é único

   Consideremos e e e' elementos neutros do grupo G. Como e' é elemento neutro então $e' \cdot e = e$. Por outro lado, e também é elemento neutro, logo $e \cdot e' = e'$. Concluímos que

$$e = e' \cdot e = e \cdot e' = e' \Rightarrow e = e'$$

2. O elemento inverso é único

   Consideremos $a \in G$ e sejam b, $b' \in G$ dois elementos inversos do elemento a. Como b e b' são inversos de a, $a \cdot b = e$ e $a \cdot b' = e$, dessa forma

$$b = b \cdot e = b \cdot (a \cdot b') = (b \cdot a) \cdot b' = e \cdot b' = b'.$$

Para refletir

1. Mostre que o conjunto dos números naturais com a operação de adição (N, +), não é um grupo.
2. Verifique se o conjunto $A = \{-1, 1\}$ com a operação de multiplicação de inteiros é um grupo abeliano.
3. Verifique se o conjunto das simetrias espaciais S_Δ de um triângulo equilátero é um grupo abeliano.
4. Seja Z_n o conjunto das classes de restos modulo n, com a operação de adição sobre Z_n definida por $\bar{a} + \bar{b} = \overline{a + b}$ (Veja a Proposição 14 (i) do Capítulo 4). Analise se $(Z_n, +)$ é um grupo abeliano.
5. Descreva o grupo das simetrias espaciais de um quadrado, bem como a tabela contendo as composições de todos os possíveis pares de simetrias.

2. Subgrupos

Definição: Seja $(G, \cdot)$ um grupo e H um subconjunto não vazio de G. Dizemos que H é um subgrupo de G se, com a operação de G, o conjunto H é um grupo.

A associatividade será sempre satisfeita, pois os elementos pertencem a um grupo. Observamos também que o elemento neutro e o inverso serão iguais aos do grupo. Na prática, para verificar se um subconjunto de um grupo é um subgrupo, necessitamos apenas mostrar o fechamento e que o inverso de cada elemento também faz parte do subconjunto. Além da inclusão da identidade, é claro.

Exemplo 6: Dado o grupo G, podemos imediatamente apresentar dois subgrupos de G, a saber, $\{e\}$ e G.

Exemplo 7: O subconjunto $2Z = \{2 \cdot z \mid z \in Z\}$ é um subgrupo de $(Z, +)$.

Exemplo 8: São subgrupos do grupo S_Δ das simetrias espaciais triângulo equilátero $\{id, R_1\}$ e $\{id, R_{120}, R_{240}\}$.

Para refletir

1. Verifique se o conjunto $H = \{x \in Z \mid x \text{ é par}\}$, com a operação usual da adição de inteiros é um subgrupo de $(Z, +)$.
2. Descreva os subgrupos do grupo de simetrias espaciais de um quadrado.

3. Homomorfismos e Isomorfismo

Definição: Dados os grupos $(G, \cdot)$ e $(G', *)$. Entendemos por homomorfismo uma função $f: G \to G'$ que preserva a estrutura de grupo, isto é, para todo $a, b \in G$ temos que

$$f(a \cdot b) = f(a) * f(b).$$

Exemplo 9: Seja $G = (\mathbb{Z}, +)$, então $f: G \to G$, definida por $f(x) = 2 \cdot x$ é um homomorfismo de grupos. De fato, $f(x + y) = 2 \cdot (x + y) = 2 \cdot x + 2 \cdot y = f(x) + f(y), \forall x, y \in G$

Exemplo 10: Fixe $n \in \mathbb{Z}$. A aplicação que associa a cada inteiro k o resto da divisão de k por n, visto como elemento de $\mathbb{Z}_n$, é um homomorfismo de $(\mathbb{Z}, +)$ em $(\mathbb{Z}_n, +)$. Isto é uma consequência imediata da definição da operação de adição de classes de equivalência em $\mathbb{Z}_n$, $\bar{a} + \bar{b} = \overline{a + b}$, como feito na atividade 4. da seção 5.1.

Em particular, se $n = 2$, este homomorfismo $f:(\mathbb{Z},+) \to (\mathbb{Z}_n, +)$ é dado por $f(k) = \bar{0}$, se k é par, e $f(k) = \bar{1}$, se k é ímpar.

Definição: Seja $f:(G,\cdot) \to (G', *)$ um homomorfismo. Dizemos que f é um isomorfismo quando existir um homomorfismo $g:(G', *) \to (G, \cdot)$ tal que $f \circ g = I_{G'}$ e $g \circ f = I_G$.

Exemplo 11: Dados $G = (\mathbb{R}^*_+, \cdot)$ e $G' = (\mathbb{R}, +)$ e a função $f: \mathbb{R}^*_+ \to \mathbb{R}$ definida por $f(x) = \log(x)$. Afirmamos que a função f é um isomorfismo. Primeiramente, observe que f é homomorfismo:

$\forall x, y \in \mathbb{R}^*_+$, temos que $f(x \cdot y) = \log(x \cdot y) = \log(x) + \log(y) = f(x) + f(y)$.

Além disso, f é bijetora e tem como inversa a função exponencial $g(x) = e^x$. A exponencial também é homomorfismo, pois $e^{x+y} = e^x \cdot e^y$, para todos $x, y \in \mathbb{R}$.

Para refletir

1. Sejam $G = (\mathbb{Z}, +)$ e $G' = (\mathbb{Z}, +)$ e a função $f: G \to G'$ definida por $f(x) = 5 \cdot x$. Verifique se f é um homomorfismo.
2. Considere $G = (\mathbb{Z}, +)$ e $G' = (\mathbb{Z}, +)$ e a função $f: G \to G'$ definida por $f(x) = 3 \cdot x^2$. Verifique se f é um homomorfismo.

4. Definição de anel e domínio de integridade

Definição: Dado A um conjunto não vazio, com duas operações $(A, +, *)$. Dizemos que A é um anel se satisfaz as propriedades:

(i) $(A,+)$ é um grupo abeliano;

(ii) A operação $(A, *)$ satisfaz:

1. $\forall a, b, c \in A$, temos que $(a * b) * c = a * (b * c)$.
2. Existe um elemento $1 \in A$ tal que $a * 1 = 1 * a = a$, $\forall a \in A$.

(iii) A operação * é distributiva em relação a operação +: $\forall a, b, c \in$ A, temos:

$a * (b + c) = a * b + z * c$, e

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

Em geral, a operação + é pensada como uma adição e * como uma multiplicação em A.

Exemplo 12: conjunto dos inteiros com as operações de adição e multiplicação, $(Z, +, \cdot)$, é um anel com as operações de adição e multiplicação usuais.

Exemplo 13: São exemplos de anéis: $(Q, +, \cdot)$, $(R, +, \cdot)$ e $(C, +, \cdot)$.

Definição: Seja $(D, +, *)$. um anel. Dizemos que D é um domínio de integridade se:

1. o elemento neutro 1 da operação * é diferente do elemento neutro $0 \in A$ da +,
2. a opereção * é comutativa, e
3. $\forall a, b \in A$, com $a \neq 0$ e $b \neq 0$, temos que $a * b \neq 0$. Em outras palavras, se $a * b = 0$, então $a = 0$ ou $b = 0$.

Exemplo 14: $(Z, +, \cdot)$ é um domínio de integridade.

Exemplo 15: Consideremos $Z(i) = \{a + bi \in C \mid a, b \in Z\}$. Temos que $(Z(i), +, \cdot)$ é um domínio de integridade.

Para refletir

1. Mostre que o conjunto dos inteiros com as operações usuais de adição e multiplicação é um domínio de integridade.
2. Mostre que o conjuntos $M_{2x2}(Z)$ das matrizes 2 x 2 com entradas inteiras, e munido das operações usuais de soma e multiplicação de matrizes, é um anel, mas não é um domínio de integridade.

5. Subanéis, ideais, anéis quocientes e corpos

Definição: Seja B um subconjunto não vazio de A, onde $(A, +, *)$ é um anel. Dizemos que B é subanel se:

(i) B é fechado para as duas operações;

(ii) $(B,+ , *)$ é um anel

Exemplo 16: $\mathbb{Z}$ é subanel de $\mathbb{Q}$, $\mathbb{Q}$ é subanel de $\mathbb{R}$ e $\mathbb{R}$ é subanel de $\mathbb{C}$.

Definição: Seja I um subconjunto não vazio de um anel $(A, +, *)$. Dizemos que I é um ideal de A se:

(i) $\forall a, b \in I$, então $a+ b \in I$; em outras palavras, $(I, +)$ é subgrupo de $(A, +)$, e

(ii) $\forall a \in A$ e $b \in I$, então $a * b, b * a \in I$.

Exemplo 17: Considere $n \in \mathbb{Z}$, com $n \geq 1$, temos que o subconjunto dos inteiros $n\mathbb{Z} = \{n \cdot z \mid z \in \mathbb{Z}\}$ é um ideal do anel $(\mathbb{Z}, +, \cdot)$.

A relação de congruência em $\mathbb{Z}$ pode ser analisada em termos de um ideal I de uma anel qualquer.

$a \equiv b \bmod I \Leftrightarrow b - a \in I$.

Definição: Sejam $(A, +, *)$ um anel e I um ideal de A. A classe residual de a módulo I é definida por $\overline{a} = a + I = \{a + b \mid b \in I\}$. O anel $(A/I, +, *)$ das classes residuais módulo I, ou seja, das classes de equivalência módulo I, é chamado de anel quociente de A módulo I.

Exemplo 18: Considere $n \in \mathbb{Z}$. O quociente do anel dos inteiros pelo ideal $n\mathbb{Z}$, introduzido no Exemplo 17 acima, será denotado por $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, ..., (n - 1) + n\mathbb{Z}\}$. Isto induz uma estrutura de anel nos conjuntos das classes de restos módulo n.

Definição: Seja $(K, +, *)$ um anel. Dizemos que K é um corpo se satisfaz as seguintes condições:

1. $\forall a \in K$ com $a \neq 0$, existe $b \in K$ tal que $a * b = b * a = 1$, e
2. $(\{a \in K \mid a \neq 0\},*)$ é grupo abeliano.

Exemplo 19: São exemplos de corpos $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$.

Atividades de avaliação

1. Mostre que o conjunto 2Z é um ideal de Z com as operações usuais de adição e multiplicação dos inteiros.
2. Verifique que 6Z é um ideal de 2Z e apresente a forma dos elementos de 2Z/6Z.
3. Explique porque (Z, +, ·) não é um corpo.
4. Verifique se o anel Z_9 é um corpo. Justifique.
5. Mostre que se p é primo então Z_p é corpo.

Síntese do capítulo

Neste capítulo apresentamos definições que possibilitam uma introdução ao estudo de estruturas algébricas.

Definição: Seja G um conjunto, munido de uma operação $(G, \cdot)$. Neste ponto, a operação pode ser pensada como um produto ou uma soma entre dois números. Em geral, $\cdot$ é uma operação abstrata definida para pares de elementos de G. Dizemos que G é um grupo de satisfaz as propriedades:

(i) O conjunto é fechado, ou seja, para todo $a, b \in G$

$a \cdot b \in G$.

(ii) A operação é associativa, ou seja, para todo $a, b, c \in G$

$a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(iii) Existe elemento neutro em relação a operação, isto é, existe $e \in G$, tal que

$a \cdot e = e \cdot a = a$, para todo $a \in G$.

(iv) Para cada $a \in G$, existe $b \in G$, chamado de inverso em relação à operação, tal que

$a \cdot b = b \cdot a = e$.

O grupo será chamado de comutativo ou abeliano se, além das propriedades já citadas, possuir a propriedade a seguir.

(v) A operação é comutativa, isto é, para todo $a, b \in G$ temos que

$a \cdot b = b \cdot a$.

Definição: Seja $(G, \cdot)$ um grupo e H um subconjunto não vazio de G. Dizemos que H é um subgrupo de G se, com a operação de G, o conjunto H é um grupo.

Definição: Dados os grupos $(G, \cdot)$ e $(G', *)$. Entendemos por homomorfismo uma função $f: G \to G'$ que preserva a estrutura de grupo, isto é, para todo $a, b \in G$ temos que

$$f(a \cdot b) = f(a) * f(b).$$

Definição: Seja $f:(G, \cdot) \to (G', *)$ um homomorfismo. Dizemos que f é um isomorfismo quando existir um homomorfismo $g:(G', *) \to (G, \cdot)$ tal que $f \circ g = I_{G'}$ e $g \circ f = I_G$.

Definição: Dado A um conjunto não vazio, com duas operações $(A, +, *)$. Dizemos que A é um anel se satisfaz as propriedades:

(i) (A,+) é um grupo abeliano;

(ii) A operação (A,*) satisfaz:

1. $\forall a, b, c \in A$, temos que $(a * b) * c = a * (b * c)$.
2. Existe um elemento $1 \in A$ tal que $a * 1 = 1 * a = a$, $\forall a \in A$

(iii) A operação * é distributiva em relação a operação +: $\forall a, b, c \in A$, temos:

$a * (b + c) = a * b + z * c$, e

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

Em geral, a operação + é pensada como uma adição e * como uma multiplicação em A.

Definição: Seja $(D, +, *)$. um anel. Dizemos que D é um domínio de integridade se:

1. o elemento neutro 1 da operação * é diferente do elemento neutro $0 \in A$ da +,
2. a opereção * é comutativa, e
3. $\forall a, b \in A$, com $a \neq 0$ e $b \neq 0$, temos que $a * b \neq 0$. Em outras palavras, se $a * b = 0$, então $a = 0$ ou $b = 0$.

Definição: Seja B um subconjunto não vazio de A, onde $(A, +, *)$ é um anel. Dizemos que B é subanel se:

(i) B é fechado para as duas operações;

(ii) $(B, +, *)$ é um anel.

Definição: Seja I um subconjunto não vazio de um anel $(A, +, *)$. Dizemos que I é um ideal de A se:

(i) $\forall a, b \in I$, então $a + b \in I$; em outras palavras, $(I, +)$ é subgrupo de $(A, +)$, e

(ii) $\forall a \in A$ e $b \in I$, então $a * b, b * a \in I$.

Definição: Sejam (A, +, *) um anel e I um ideal de A. A classe residual de a módulo I é definida por $\bar{a} = a + I = \{a + b \mid b \in I\}$. O anel $(A/I, +, *)$ das classes residuais módulo I, ou seja, das classes de equivalência módulo I, é chamado de anel quociente de A módulo I.

Definição: Seja $(K, +, *)$ um anel. Dizemos que K é um corpo se satisfaz as seguintes condições:

1. $\forall a \in K$ com $a \neq 0$, existe $b \in K$ tal que $a * b = b * a = 1$, e
2. $(\{a \in K \mid a \neq 0\}, *)$ é grupo abeliano.

Leituras, filmes e sites

http://www.dca.fee.unicamp.br/~marco/cursos/ia012_14_1/slides/grupos-aneis-corpos.pdf

http://www.dm.ufscar.br/profs/sampaio/capitulo1.PDF

http://denebola.if.usp.br/~jbarata/Notas_de_aula/arquivos/nc-cap02.pdf

http://www.mat.ufmg.br/~marques/Apostila-Aneis.pdf

http://www.mat.ufpb.br/lenimar/textos/intalgebra_lna.pdf

Referências

GARCIA, Arnaldo; LEQUAIN, Yves. **Elementos de álgebra**. 4.ed. Rio de Janeiro: IMPA, 2006.

Gabarito: Matemática discreta

Capítulo 1

Seção 1.1

1.
   a) A = {janeiro, fevereiro, março, abril, maio, junho, julho, agosto, setembro, outubro, novembro, dezembro} e $n(A) = 12$
   b) B = {segunda, terça, quarta, quinta, sexta, sábado, domingo} e $n(A) = 7$
   c) C = {0, 6, 12, 18, ...} e $n(A) = \infty$
   d) D = {1, 2, 3, 4, 6, 12} e $n(A) = 6$

Seção 1.2

1. V – F – V – F – V – V
2. $2^7 - 8 = 120$, retiramos Ø e os 7 conjunto que possuem 1 elemento 1 + 7 = 8
3. b

Seção 1.3

1.
   a) {1,2,3,4,6,7,8}
   b) {3,4}
   c) {1,2,3,4,6}
   d) {1,2,3,4,5,6,7,8}
   e) {1}
   f) {(1,2), (1,3), (1,6), (1,7), (1,8), (2,2), (2,3), (2,6), (2,7), (2,8), (3,2), (3,3), (3,6), (3,7), (3,8), (4,2), (4,3), (4,6), (4,7), (4,8)}
2.
   a) 6
   b) 18
3. C
4. {3,4,5}
5. C
6. V – V – V – V
7. $A = \{0,1,2,5\}$ e $B = \{-2, -1\}$

Seção 1.4

1.
   a) V
   b) V
   c) F
   d) F
2.
   a) 2 e 3, duas raízes reais
   b) $2i$ e $-2i$, duas raízes complexas
   c) $2 + i$ e $2 - i$, duas raízes complexas

Capítulo 2

Seção 2.1

1.
   a) {(5,3)}
   b) {(1,3), (1,5), (1,7), (1,9), (3,5), (3,7), (3,9), (5,7), (5,9)}
2. {(1,0), (9,4)}
3. $A = \{1,2,3,4\}$

Reflexiva

$(1,1) \in R$
$(2,2) \in R$
$(3,3) \in R$
$(4,4) \in R$

Simétrica

(1,1)
(2,2)
(3,3)
(4,4)
(1,2) e (2,1)

Transitiva

$(1,2), (2,1) \in R$ e $(1,1) \in R$
$(2,1), (1,2) \in R$ e $(2,2) \in R$
$(1,1), (1,2) \in R$ e $(1,2) \in R$
$(1,1), (2,1) \in R$ e $(1,1) \in R$
$(2,1), (1,1) \in R$ e $(2,1) \in R$
$(1,2), (1,1) \in R$ e $(1,1) \in R$
$(1,2), (2,2) \in R$ e $(1,2) \in R$
$(2,2), (1,2) \in R$ e $(2,2) \in R$
$(2,1), (2,2) \in R$ e $(2,2) \in R$
$(2,2), (2,1) \in R$ e $(2,1) \in R$

Seção 2.2

1.
   a) É função
   b) Não é função
   c) Não é função
2. $Dm = \{1,2\}$, $CD = \{3,4,5\}$ e $Im = \{3,5\}$
3.
   a) Bijetora $f^{-1} = \{(1,1), (2,2), (3,3), (4,4)\}$
   b) Sobrejetora, não injetora, não admite inversa
   c) Não é sobrejetora, não é injetora, não admite inversa
4. $gof = 3x + 1$ e $fog = 3x + 5$

Capítulo 3

Seção 3.1

1.
   a) 6
   b) 15
   c) 8
2. 720
3. 106
4. 720

Seção 3.2

1. 60 números e 12 deles são pares
2. 120

Seção 3.3

1. 720
2. 24
3. 151200
4. 240

Seção 3.4

1. 126
2. 210
3. 10
4. 6
5. 26
6. $x^5 - 5x^4y + 10x^3y^2 - 10x^2y^3 + 5xy^4 - y^5$

Capítulo 4

Seção 4.1

1. Para n=1, $S_1 = 1$

   Supondo verdadeiro para n, isto é

$$S_n = \frac{n \cdot (n+1) \cdot (2n+1)}{6}$$

   Verificando para $n + 1$

$$S_{n+1} = 1^2 + \cdots + n^2 + (n+1)^2$$
$$S_{n+1} = \frac{n \cdot (n+1) \cdot (2n+1)}{6} + (n+1)^2$$
$$S_{n+1} = \frac{(n+1) \cdot (n+2) \cdot [2(n+1)+1]}{6}$$

   Logo válido para todo $n \in \mathbb{N}$.

2.

$$1 + 3 + 5 + \cdots + (2n-1) = n^2$$

   Para n = 1 temos que $1 = 1^2$

   Para n = 2 temos que $1 + 3 = 2^2$

   Supondo verdade para n

$$1 + 3 + 5 + \cdots + (2n-1) = n^2$$

   Devemos verificar a veracidade para $n + 1$

$$1 + 3 + 5 + \cdots + (2n-1) + [2(n+1) - 1] = n^2 + 2n + 2 - 1 = (n+1)^2$$

   Válido para todo $n \in \mathbb{N}$

3.

   a) Para $n = 1$ temos a_1

   Para $n = 2$ $a_2 = a_1 + r$

   Supondo verdade para n

   Verificando a validade para $n + 1$

$$a_{n+1} = a_n + r$$
$$a_{n+1} = a_1 + (n-1) \cdot r + r$$
$$a_{n+1} = a_1 + [(n-1)+1] \cdot r$$
$$a_{n+1} = a_1 + [(n+1)-1] \cdot r$$

   Logo válido para todo $n \in \mathbb{N}$.

   b) $S_1 = a_1$

   $S_2 = a_1 + a_2$ ok!

Supondo verdade para n e verificando para $n+1$

$$S_{n+1} = a_1 + a_2 + \ldots + a_n + a_{n+1}$$
$$S_{n+1} = S_n + a_{n+1}$$
$$S_{n+1} = \frac{(a_1 + a_n)\cdot n}{2} + a_{n+1}$$
$$S_{n+1} = \frac{(a_1 + a_{n+1})\cdot (n+1)}{2}$$

Válido para todo $n \in \mathbb{N}$.

4.

a) Para $n = 1$ temos a_1
Para $n = 2$ $a_2 = a_1 \cdot q$
Supondo verdade para n
Verificando a validade para $n+1$

$$a_{n+1} = a_n \cdot q$$
$$a_{n+1} = a_1 \cdot q^{n-1} \cdot q$$
$$a_{n+1} = a_1 \cdot q^n$$

Logo válido para todo $n \in \mathbb{N}$.

b) $S_1 = a_1$
$S_2 = a_1 + a_2$ ok!
Supondo verdade para n e verificando para $n+1$

$$S_{n+1} = a_1 + a_2 + \ldots + a_n + a_{n+1}$$
$$S_{n+1} = S_n + a_{n+1}$$
$$S_{n+1} = \frac{a_1 \cdot (q^n - 1)}{q-1} + a_{n+1}$$
$$S_{n+1} = \frac{a_1 \cdot (q^{n+1} - 1)}{q-1}$$

Válido para todo $n \in \mathbb{N}$.

5. PG de razão 2 $a_n = 2^{n-1}$
$S_1 = 1$
$S_2 = 1 + 2 = 3$
$S_3 = 1 + 2 + 4 = 7$
$\vdots$
$S_n = 2^n - 1$
Verificando a validade por indução
$S_1 = 2^1 - 1$
$S_2 = 2^2 - 1$
Supondo verdade para n e analisando $n+1$
$S_{n+1} = S_n + a_{n+1}$
$S_{n+1} = 2^n - 1 + 2^{n+1-1}$
$S_{n+1} = 2^n - 1 + 2^n$
$S_{n+1} = 2 \cdot 2^n - 1$
$S_{n+1} = 2^{n+1} - 1$
Válido para todo $n \in \mathbb{N}$.

Seção 4.2

1. $a \cdot c | b \cdot c \Leftrightarrow a | b$
$\Leftarrow$ Se $a|b$, então existe $n \in \mathbb{N}$ tal que $b = n \cdot a$ e para algum $c \in \mathbb{N}^*$ te
$b \cdot c = n \cdot a \cdot c \Rightarrow a \cdot c | b \cdot c$
$\Rightarrow a \cdot c | b \cdot c \Rightarrow$ existe $k \in \mathbb{N}$ tal que $b \cdot c = k \cdot a \cdot c$ com $c \in \mathbb{N}^* \Rightarrow b =$
2. $9|10^n - 1$
Para $n = 1$
$9|10^1 - 1 = 9$
Supondo verdade para $n \in \mathbb{N}$, ou seja, que $9|10^n - 1$
Verificando para $n+1$
$10^{n+1} - 1 = 10 \cdot 10^n - 1 = 10.10^n - 10 + 9 = 10(10^n - 1) + 9$ pela propriedade 5 ($a|b$ e $a|c$, então $a|m \cdot b + n \cdot c$), como $9|9$ e pela hipótese de indução temos que $9|10^n - 1$, então $9|10(10^n - 1) + 9$. Válido para todo $n \in \mathbb{N}$.
3. $n = 2$
$\frac{a^2 - b^2}{a-b} = \frac{(a-b)\cdot(a+b)}{a-b} = a + b = a^{2-1} - b^{2-1}$
Supondo verdade para n
$\frac{a^n - b^n}{a-b} = a^{n-1} + a^{n-2} \cdot b + \cdots + a \cdot b^{n-2} + b^{n-1}$
Verificando o que ocorre para $n+1$
$a^{n+1} - b^{n+1} = a^n \cdot a - b \cdot a^n + b \cdot a^n - b \cdot b^n$
$a^{n+1} - b^{n+1} = a^n \cdot (a-b) + b \cdot (a^n - b^n)$
Como $a - b | a - b$ e pela hipótese de indução $a - b | a^n - b^n$, pela proposição 5 temos que
$a - b | a^n \cdot (a-b) + b \cdot (a^n - b^n)$
Logo é válido para todo $n \in \mathbb{N}$

4. $a + 2 | a^3 - 4$
$a^3 - 4 = a^3 + 8 - 12 = (a^3 + 2^3) - 12$
Pelas proposições 2 e 8 temos que $a + 2 | a^3 + 2^3$ então para que $a + 2 | 12$ devemos ter
$a = \{0,1,2,4,10\}$

5. Para $a = 1$, temos que $5|1^5 - 1 = 0$
   Supondo verdade para $a \in \mathbb{N}$
   $5|a^5 - a$
   Verificando para $a + 1$
   $(a+1)^5 - (a+1) = a^5 + 5a^4 + 10a^3 + 10a^2 + 5a + 1 - a - 1$
   $= a^5 - a + 5(a^4 + 2a^3 + 2a^2 + a)$
   $5|a^5 - a$ e $5|5$, logo $5|(a+1)^5 - (a+1)$
   Válido para todo $a \in \mathbb{N}$

Seção 4.3

1. $55 = 6 \cdot 9 + 1$
2. $a \in \mathbb{N}$ e $n \in \mathbb{N}^*$
   a é par $\Leftrightarrow a^n$ é par
   $\Rightarrow$ Se a é par $\Rightarrow a = 2 \cdot k$, com $k \in \mathbb{N}$
   Para $n \in \mathbb{N}^*$
   $a^n = (2 \cdot k)^n = 2 \cdot (2^{n-1} \cdot k^n)$, logo a^n é par.
   $\Leftarrow$ Se a^n é par então ele é da forma $2 \cdot k$ e não pode ser potência de um número ímpar pois toda potência de ímpar é ímpar
   $$(2 \cdot x + 1)^n = (2 \cdot x)^n + (2 \cdot x)^{n-1} + \cdots + 2 \cdot x + 1 = 2 \cdot k + 1$$
3. Se $n \in \mathbb{N}$, podemos escrever n como
   $n = 6 \cdot k \Rightarrow n^2 = 36 \cdot k^2$ resto 0
   $n = 6 \cdot k + 1 \Rightarrow n^2 = 6 \cdot (k^2 + 2 \cdot k) + 1$ resto 1
   $n = 6 \cdot k + 2 \Rightarrow n^2 = 6 \cdot (6 \cdot k^2 + 4 \cdot k) + 4$ resto 4
   $n = 6 \cdot k + 3 \Rightarrow n^2 = 6 \cdot (6 \cdot k^2 + 6 \cdot k + 1) + 3$ resto 3
   $n = 6 \cdot k + 4 \Rightarrow n^2 = 12 \cdot (3 \cdot k^2 + 4 \cdot k + 1) + 4$ resto 4
   $n = 6 \cdot k + 5 \Rightarrow n^2 = 12 \cdot (3 \cdot k^2 + 5 \cdot k + 2) + 1$ resto 1
   Os possíveis restos da divisão por 6 são 0, 1, 3 e 4, não pode ter resto 2.
4. $n = 20 \cdot k + 8$, com $k \in \mathbb{N}$
   $n = 20 \cdot k + 5 + 3$
   $n = 5 \cdot (4 \cdot k + 1) + 3$, resto 3.

Seção 4.4

1. p é primo e $p, p+2$ e $p+4$
   Todo número natural pode ser escrito como:
   $3 \cdot k$, $3 \cdot k + 1$ ou $3 \cdot k + 2$
   Se $p = 3$ e $k = 1$, então os números são 3, 5 e 7 todos primos.
   Se p é da forma $3 \cdot k + 1$
   Para $3 \cdot k + 1$, $3 \cdot k + 1 + 2 = 3 \cdot k + 3$ e $3 \cdot k + 1 + 4 = 3 \cdot k + 5$, ou seja, $3 \cdot k + 1 + 2$ não é primo.
   Se p é da forma $3 \cdot k + 2$
   Para $3 \cdot k + 2$, $3 \cdot k + 2 + 2 = 3 \cdot k + 4$ e $3 \cdot k + 2 + 4 = 3 \cdot k + 6$, ou seja, $3 \cdot k + 2 + 4$ não é primo.
2. $n > 11$, $n \in \mathbb{N}$ é soma de dois compostos
   Se n é par, $n = 2 \cdot k$, para $k > 5$
   $n = 2 \cdot k - 4 + 4 = 2 \cdot (k - 2) + 4$ soma de compostos com $n > 11$
   Se n é impar, $n = 2 \cdot k + 1$, para $k > 5$
   $n = 2 \cdot k - 8 + 8 + 1 = 2 \cdot (k - 4) + 9$ soma de compostos com $n > 11$
3. Pela proposição 7, $a - b|a^n - b^n$
   Assim, $2^{10} - 5^4 | (2^{10})^2 - (5^4)^2 \Rightarrow 399 | (2^{10})^2 - (5^4)^2$. Como $399 \neq 2^{20} - 5^8$, temos que $2^{20} - 5^8$ não é primo.

Seção 4.5

1.
   a) $5 \cdot x + 7 \cdot y = 100$
      $mdc(5,7) = 1$ e $1|100$, tem solução
      Observamos que (13,5) é solução, então as soluções são:
      $(13 + 7 \cdot t, 5 - 5 \cdot t)$, com $t \in \mathbb{Z}$
   b) $7 \cdot x + 11 \cdot y = 116$
      $mdc(7,11) = 1$ e $1|116$, tem solução
      Observamos que (15,1) é solução, então as soluções são:
      $(15 + 11 \cdot t, 1 - 7 \cdot t)$, com $t \in \mathbb{Z}$

2.
   a)

	1	1	1	3	1	1	2
384	246	138	108	30	18	12	6
138	108	30	18	12	6	0	

   mdc = 6

   b)

	2	3	6	6
542	234	74	12	2
74	12	2	0	

   mdc = 2

   c)

	1	1	7	3	4
1218	648	570	78	24	6
570	78	24	6	0	

   mdc = 6

3. $10 \cdot x + 14 \cdot y = 100$
   mdc (10,14) = 2
   (10,0) é uma solução
   $$\left(10 + \frac{14}{2} \cdot t, 0 - \frac{10}{2} \cdot t\right) = (10 + 7 \cdot t, -5 \cdot t)$$
   (10,0) e (3,5), duas maneiras

Seção 4.6

1. $2^5 \cdot 5 = 2 \cdot 2^4 \cdot 5 = 2 \cdot 5 \cdot 2^4 = 10 \cdot 2^4$ que é múltiplo de 10.
2. $3 \cdot x = 5 \cdot k$. Como $5 \nmid 3$, então $5|x$.
3. $x^2 - y^2 = 17$
   $(x+y) \cdot (x-y) = 17$, como 17 é primo então
   $\begin{cases} x+y = 17 \\ x-y = 1 \end{cases}$ ou $\begin{cases} x+y = 1 \\ x-y = 17 \end{cases}$
   $x = 9$ e $y = 8$ ou $x = 9$ e $y = -8 \notin \mathbb{N}$
   Logo a única solução é $x = 8$ e $y = 9$

4. Se $1000|n! \Rightarrow 2^3 \cdot 5^3 | n! \Rightarrow n! = 2^3 \cdot 5^3 \cdot k$ com $k \in \mathbb{N}$
$1 \cdot 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot \ldots \cdot 10 \cdot \ldots \cdot 15$

Ou

15: 2 tem quociente 7 e resto 1
7: 2 tem quociente 3 e resto 1
3: 2 tem quociente 1 e resto 1
1: 2 tem quociente 0 e resto 1
7+3+1+0 = 11, ou seja temos 2^{11} até 15!
E
15: 5 tem quociente 3 e resto 0
3: 5 tem quociente 0 e resto 3
3+0 = 3, ou seja temos 5^3até 15!

Seção 4.7

1. D
$5|x^2 - 1 \Rightarrow 5|(x-1)\cdot(x+1) \Rightarrow 5|x-1$ ou $5|x+1 \Rightarrow x - 1 = 5 \cdot k$ ou $x + 1 = 5 \cdot k$, com $k \in \mathbb{Z} \Rightarrow x = 5 \cdot k + 1$ ou $x = 5 \cdot k - 1 = 5 \cdot k - 1 - 4 + 4 = 5 \cdot (k-1) + 4$, ou seja, $x \equiv 1\ mod\ 5$ ou $x \equiv 4\ mod\ 5$.
2. $1! + 2! + \cdots + 100!$ Dividido por 40
$1! = 1 \quad 1 \equiv 1\ mod\ 40$
$2! = 2 \quad 2 \equiv 2\ mod\ 40$
$3! = 6 \quad 6 \equiv 6\ mod\ 40$
$4! = 24 \quad 24 \equiv 24\ mod\ 40$
$5! = 120 \quad 120 \equiv 0\ mod\ 40$
$6! = 720 \quad 720 \equiv 0\ mod\ 40$
A partir de 5! os números são todos múltiplos de 120, ou seja, todos tem resto 0.
Logo o resto é a soma dos restos
$1 + 2 + 6 + 24 + 0 + 0 + \cdots + 0 = 33$

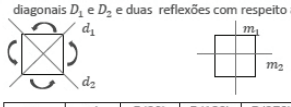
Capítulo 5

Seção 5.1

1. $(\mathbb{N}, +)$
Fechamento $a, b \in \mathbb{N}$, temos que $a + b \in \mathbb{N}$
Associativa $a, b, c \in \mathbb{N}$, temos que $(a + b) + c = a + (b + c)$
Elemento neutro é o 0, temos que $a + 0 = 0 + a = a$
Não possui inverso aditivo pois $a + b = 0$, temos que $b = -a \notin \mathbb{N}$
Logo não é grupo
2. $A = \{-1, 1\}$ e $(A, \cdot)$

·	-1	1
-1	1	-1
1	-1	1

Fechamento
$(-1) \cdot 1 = -1 \in A$
$(-1) \cdot (-1) = 1 \in A$
$1 \cdot 1 = 1 \in A$
Associatividade segue da associatividade da multiplicação de inteiros
$a, b, c \in A$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
Elemento neutro é o elemento neutro dos inteiros
$a \cdot 1 = a$, se $a = 1$ temos que $1 \cdot 1 = 1$ e se $a = -1$ temos que $1 \cdot (-1) = -1$
Elemento inverso – cada elemento possui um inverso único
$1 \cdot 1 = 1$ e $(-1) \cdot (-1) = 1$
A comutatividade vem da comutatividade dos inteiros
Trata-se de um grupo abeliano.
3. Não é grupo abeliano, pois $R(120) o R(1) = R(3)$ e $R(1) o R(120) = R(2)$.
4. Associatividade, comutatividade, elemento neutro e inverso seguem das propriedades dos inteios, ou seja
$$\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$$
$$(\bar{a} + \bar{b}) + \bar{c} = \overline{a+b} + \bar{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \bar{a} + \overline{(b+c)} = \bar{a} + (\bar{b} + \bar{c})$$
$$\bar{a} + \bar{0} = \overline{a+0} = \bar{a} = \bar{0} + \bar{a} = \bar{0} + \bar{a}$$
$$\bar{a} + \overline{-a} = \overline{a + (-a)} = \overline{a - a} = \bar{0}$$
Logo, é grupo abeliano
5. São 8 rotações Id, três rotações $R(90)$, $R(180)$ e $R(270)$, duas reflexões com respeito as diagonais D_1 e D_2 e duas reflexões com respeito as medianas M_1 e M_2.



O	Id	$R(90)$	$R(180)$	$R(270)$	$D(1)$	$D(2)$	$M(1)$	$M(2)$
Id	Id	$R(90)$	$R(180)$	$R(270)$	$D(1)$	$D(2)$	$M(1)$	$M(2)$
$R(90)$	$R(90)$	$R(180)$	$R(270)$	Id	$M(2)$	$M(1)$	$D(1)$	$D(2)$
$R(180)$	$R(180)$	$R(270)$	Id	$R(90)$	$D(2)$	$D(1)$	$M(2)$	$M(1)$
$R(270)$	$R(270)$	Id	$R(90)$	$R(180)$	$M(1)$	$M(2)$	$D(2)$	$D(1)$
$D(1)$	$D(1)$	$M(1)$	$D(2)$	$M(2)$	Id	$R(180)$	$R(90)$	$R(270)$
$D(2)$	$D(2)$	$M(2)$	$D(1)$	$M(1)$	$R(180)$	Id	$R(270)$	$R(90)$
$M(1)$	$M(1)$	$D(2)$	$M(2)$	$D(1)$	$R(270)$	$R(90)$	Id	$R(180)$
$M(2)$	$M(2)$	$D(1)$	$M(1)$	$D(2)$	$R(90)$	$R(270)$	$R(180)$	Id

Seção 5.2

1. Como 0 é par, H é subconjunto de $\mathbb{Z}$ que contém o elemento neutro. Seguem daí as propriedades associativa e elemento neutro de H. O subconjunto H é fechado pois a soma de dois pares é par. Finalmente, se x é par, então –x também é par, o que garante a existência de elementos inversos em H. Concluindo que H é subgrupo.
2. $\{Id\}$
Se tiver $R(90)$ ou $R(270)$ temos $\{Id, R(90), R(180), R(270)\}$ ou tudo.
Se tiver $R(180)$ e não tiver $R(90)$ temos$\{Id, R(180)\}$, $\{Id, R(180), D(1), D(2)\}$, $\{Id, R(180), M(1), M(2)\}$
Se não tiver nenhum R temos $\{Id, D(1)\}$, $\{Id, D(2)\}$, $\{Id, M(1)\}$, $\{Id, M(2)\}$

Seção 5.3

1. É homomorfismo
$$F(x+y) = 5(x+y) = 5x + 5y = F(x) + F(y)$$
2. Não é homomorfismo
$F(x+y) = 3(x+y)^2 = 3x^2 + 6xy + 3y^2 = F(x) + 6xy + F(y) \neq F(x) + F(y)$, se $x \neq 0$ e $y \neq 0$

Seção 5.4

1. Propriedades elementares dos números inteiros
2. É anel por propriedades básicas das operações de matrizes. O elemento neutron da soma é a matriz nula, e da multiplicação é a identidade. Não é domínio pois as propriedades 2 e 3 da definição não são satisfeitas sempre.

$\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}\cdot\begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}=\begin{pmatrix}0 & 0\\0 & 0\end{pmatrix}$ falha propriedade 3

$\begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}\cdot\begin{pmatrix}0 & 0\\1 & 0\end{pmatrix}=\begin{pmatrix}0 & 0\\1 & 0\end{pmatrix}$ falha propriedade 2, são diferentes

$\begin{pmatrix}0 & 0\\1 & 0\end{pmatrix}\cdot\begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}=\begin{pmatrix}0 & 0\\0 & 0\end{pmatrix}$

Seção 5.5

1. Na seção 5.2, atividade 2, vimos que $2\mathbb{Z}$ é subgrupo de $\mathbb{Z}$. Para concluir que é ideal usamos apenas que o produto de um inteiro par por um inteiro qualquer tem como resultado um inteiro par.

2. A prova é análoga a de que $2\mathbb{Z}$ é ideal de $\mathbb{Z}$. Os elementos do quociente são as classes de restos modulo 6 de inteiros pares. Existem apenas três classes:
   ...
   $-6+6\mathbb{Z}=0+6\mathbb{Z}$
   $-4+6\mathbb{Z}=2+6\mathbb{Z}$
   $-2+6\mathbb{Z}=4+6\mathbb{Z}$
   $0+6\mathbb{Z}$
   $2+6\mathbb{Z}$
   $4+6\mathbb{Z}$
   $6+6\mathbb{Z}=0+6\mathbb{Z}$
   $8+6\mathbb{Z}=2+6\mathbb{Z}$
   $10+6\mathbb{Z}=4+6\mathbb{Z}$
   $12+6\mathbb{Z}=0+6\mathbb{Z}$
   ...
   3 elementos: $0+6\mathbb{Z}$, $2+6\mathbb{Z}$ e $4+6\mathbb{Z}$
3. Para n em $\mathbb{Z}$ diferente de 1, não existe inverso multiplicative em $\mathbb{Z}$. Logo, este domínio não é um corpo.
4. $\mathbb{Z}_9$ não é nem domínio
   Segundo a definição
   $$(a+9\mathbb{Z})\cdot(b+9\mathbb{Z})=a\cdot b+9\mathbb{Z}$$
   temos
   $$(3+9\mathbb{Z})\cdot(3+9\mathbb{Z})=0+9\mathbb{Z}$$
   $$\neq 0$$
   Logo, $\mathbb{Z}_9$ não é domínio.
   Todo corpo é domínio
   $3+9\mathbb{Z}$ não possui inverso multiplicative. Se houvesse, teríamos $a\in\mathbb{Z}$ tal que
   $$(3+9\mathbb{Z})\cdot(a+9\mathbb{Z})=1+9\mathbb{Z}$$
   $$3\cdot a+9\mathbb{Z}=1+9\mathbb{Z}$$
   $$3\cdot a\equiv 1 \bmod 9$$
   O que não é possível!
5. Pelo exemplo 18 sabemos que $\mathbb{Z}_p$ é anel. A comutatividae segue da multiplicação de $\mathbb{Z}$. Resta mostrar a existência de elemento inverso multiplicative.
   Elementos
   $0+p\mathbb{Z}$
   $1+p\mathbb{Z}$
   $2+p\mathbb{Z}$
   ...
   $(p-1)+p\mathbb{Z}$
   $a\in\{0,1,2,\dots,p-1\}$
   Os elementos
   $a+p\mathbb{Z}$, $2\cdot a+p\mathbb{Z}$, ..., $(p-1)\cdot a+p\mathbb{Z}$ são distintos. A prova é por contradição:
   Se $n<m<p$ e $n\cdot a+p\mathbb{Z}=m\cdot a+p\mathbb{Z}$
   $\Rightarrow n\cdot a\equiv m\cdot a \bmod p$
   $\Rightarrow n\equiv m \bmod p$, pois p é primo e $a<p$.
   Além disso, os $(p-1)$ elementos $a+p\mathbb{Z}$, $2\cdot a+p\mathbb{Z}$, ..., $(p-1)\cdot a+p\mathbb{Z}$ são não nulos, pois
   $0<a,n<p\Rightarrow p\nmid an$
   Portanto, algum dos $a\cdot n+p\mathbb{Z}$ é igual a $1+p\mathbb{Z}$, o que mostra a existência de elemento inverso.

Sobre a autora

Raquel Montezuma Pinheiro Cabral: Professora de matemática da rede estadual de ensino do Ceará há 18 anos, trabalhando com educação semi-presencial há 14 anos. Trabalhando na UAB/UECE ministrando as disciplinas de Matemática I, Matemática II, Fundamentos do Cálculo, Probabilidade e Estatística, Informática na Sociedade e Ética, Estágio Supervisionado e na disciplina de TCC. Mestrado profissional de Matemática pela Universidade Federal do Ceará, concluído em 2014. Especialização em ensino da matemática pela Universidade Estadual do Ceará, concluída em 2001. Graduação em Licenciatura Plena em Matemática pela Universidade Estadual do Ceará, concluída em 1987.

Computação

Fiel a sua missão de interiorizar o ensino superior no estado Ceará, a UECE, como uma instituição que participa do Sistema Universidade Aberta do Brasil, vem ampliando a oferta de cursos de graduação e pós-graduação na modalidade de educação a distância, e gerando experiências e possibilidades inovadoras com uso das novas plataformas tecnológicas decorrentes da popularização da internet, funcionamento do cinturão digital e massificação dos computadores pessoais.

Comprometida com a formação de professores em todos os níveis e a qualificação dos servidores públicos para bem servir ao Estado, os cursos da UAB/UECE atendem aos padrões de qualidade estabelecidos pelos normativos legais do Governo Federal e se articulam com as demandas de desenvolvimento das regiões do Ceará.

ISBN 978-85-78265-70-0

Universidade Estadual do Ceará

UAB UNIVERSIDADE ABERTA DO BRASIL

CAPES