FUNDAMENTOS MATEMÁTICOS PARA COMPUTAÇÃO

Prof. Dr. João Carlos de Moraes Morselli Jr.
Departamento de Ciência da Computação

PUC Minas
Poços de Caldas

BIBLIOGRAFIA

Meus agradecimentos ao **Prof. Marcio Leandro Gonçalves** pelo material didático disponibilizado para a realização deste curso.
Viva Lavoisier!!

BIBLIOGRAFIA

Fundamentos Matemáticos para a Ciência da Computação
Autor: GERSTING, Judith L.
Editora: LTC, 2004

Matemática Discreta: uma introdução
Autor: SCHEINERMAN, Edward R.
Editora: Cengage Learning, 2011

Grafos: Teoria, modelos e algoritmos.
Autor: Netto Boaventura
Editora: E Blucher, 2003.

ROTEIRO

Módulo 1
Teoria dos Conjuntos

Módulo 5
Lógica Simbólica

Módulo 3
Teoria dos Números

Módulo 2
Teoria dos Grafos

Módulo 4
Análise Combinatória

PARA QUE ESTUDAR ISSO?

Teoria dos Conjuntos

Na prática qualquer coleção de objetos pode ser considerada um conjunto.
As definições e operações com conjuntos nos ajudam a resolver problemas
do dia a dia através das propriedades e definições estudadas neste módulo.
Ex.: Facebook. Cada perfil possui um conjunto de 'amizades'. Você pode inferir, através
Da teoria dos conjuntos quem é amigo de quem, quais são os amigos em comum entre
dois perfis, etc.

Teoria dos Grafos

Um grafo constitui, na prática, em uma estrutura de dados (para nós) que permite a
modelagem de problemas que outras estruturas não permitiriam.
Ex.: Facebook (de novo!). Apenas através de um grafo poderíamos armazenar
Informações que representem as inter-relações dos perfis.
Ex.: Aplicativos para GPS.

ROTEIRO

5

PARA QUE ESTUDAR ISSO?

Teoria dos Números

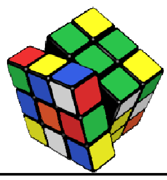
A teoria dos números envolve uma série de conceitos individuais.
Ex.: Indução Matemática (PAA)
Principio da Indução Finita (auxilia na verificação da corretitude de códigos na
engenharia de software)
Congruência (CPF, código de barras, etc.)
Primalidade (criptografia)
Entre outros conceitos

Análise Combinatória

Um estudo realizado na matemática e na lógica, responsável pela análise das
possibilidades e das combinações.
Ex.: Senhas e criptografia

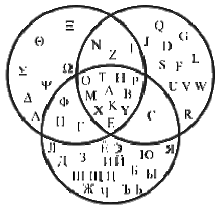
Lógica Simbólica

A lógica examina de forma genérica as formas que a argumentação pode tomar, quais dessas
formas são válidas e quais não são.
Ex.: Linguagens lógicas (Prolog, Lisp, etc.).



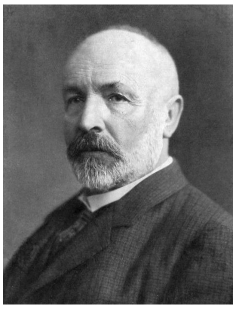
ROTEIRO

6



MÓDULO 1: TEORIA DOS CONJUNTOS

TEORIA DOS CONJUNTOS: INTRODUÇÃO



George Ferdinand Ludwig Philipp Cantor
(1845 / 1918)
Matemático russo de "origem alemã". Conhecido por ter elaborado a moderna teoria dos conjuntos.

Segundo Cantor, conjunto é qualquer coleção, dentro de um todo de objetos definidos e distinguíveis, chamados elementos, de nossa intuição ou pensamento.

NOTAÇÃO DE CONJUNTO

Conjuntos: **A, B, C,..., X, Y, Z**

Elementos dos conjuntos : **a, b, c, ...,x, y, z**

Portanto:

A = {a, b, c, ...}

RELAÇÃO DE PERTINÊNCIA (ELEMENTO X CONJUNTO)

Para indicar que um elemento x pertence ao conjunto A, escreve-se:

$$\boldsymbol{x} \in \boldsymbol{A}$$

e lê-se: "x pertence a A".

Para exprimir que um elemento x **não** pertence ao conjunto A, escreve-se:

$$\boldsymbol{x} \notin \boldsymbol{A}$$

e lê-se: "x não pertence a A".

É importante saber que é bem possível que
os elementos de um conjunto
possam ser também conjuntos.

RELAÇÃO DE INCLUSÃO (CONJUNTO X CONJUNTO)

*Definição: Um conjunto A **está contido** num conjunto B se **todos os elementos de A pertencem** também ao conjunto B.*

$$\mathbf{A} \subset \boldsymbol{B}$$

Portanto, a relação de inclusão entre dois conjuntos A e B pode ser expressa matematicamente como segue:

$$\mathbf{A} \subset \boldsymbol{B} \iff \forall\, \boldsymbol{x},\ \boldsymbol{x} \in \boldsymbol{A} \Rightarrow \boldsymbol{x} \in \boldsymbol{B}$$

A notação $A \not\subset$ B indica que A não está contido em B.

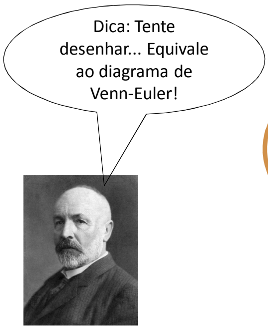
PROPRIEDADES DA RELAÇÃO DE INCLUSÃO

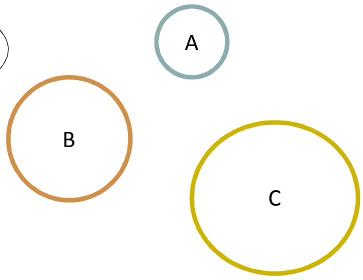
Para quaisquer conjuntos A, B, C, tem-se:

1) $A \subset A$ (reflexiva)

2) $A \subset B$ e $B \subset C \Rightarrow A \subset C$ (transitiva)

3) $A \subset B$ e $B \subset A \Rightarrow A = B$ (antissimétrica)



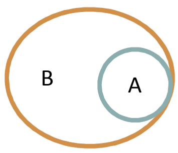


SUBCONJUNTO

A definição de subconjunto está diretamente ligada à relação de inclusão

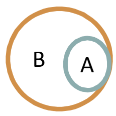
Definição: Se $A \subset B$ então dizemos que A é subconjunto de B (ou que B é superconjunto de A).

Definição: Se B contiver elementos que não estão em A, então A diz-se um subconjunto próprio de B



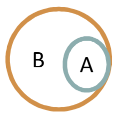
A notação de subconjunto não é padronizada. Existem duas notações para subconjunto:

- $A \subseteq B$ indica, objetivamente, que A é um subconjunto de B.



- $A \subset B$ pode indicar que A é um subconjunto de B,

ou pode indicar



que A é um subconjunto próprio de B, ou seja, que $A \subseteq B$ e $A \neq B$.

MAIS DEFINIÇÕES ...

Conjunto Unitário
Definição: Aquele formado por um único elemento.

Conjunto Vazio (∅)
Definição: Conjunto que não possui elementos.
O conjunto vazio é subconjunto de qualquer conjunto (∅ ⊂ A, ∀ A).

Conjunto das Partes
Definição: Para todo conjunto A, existe um outro conjunto, cujos elementos são subconjuntos de A. Usaremos para esse novo conjunto a notação P(A) e a denominação "conjunto das partes de A".

$$\mathbf{P(A) = \{ X \mid X \subset A \}}$$

Exemplos:
a) A = {a} => P(A) = {∅ , {a} }
b) A = {a,b} => P(A) = {∅, {a}, {b}, {a,b} }

Obs.: O número de elementos de P(A) é sempre igual a 2 elevado ao número de elementos de A.

MÓDULO 1: TEORIA DOS CONJUNTOS

13

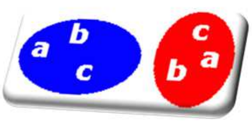
IGUALDADE DE CONJUNTOS

Definição: Dois conjuntos A e B são iguais quando todo elemento de A pertence também a B e, reciprocamente, todo elemento de B pertence a A.

Em símbolos:
A = B ⇔ ∀x, x ∈ A ⇔ x ∈ B

A ordem em que aparecem os elementos num conjunto não tem importância. Assim, o conjunto {a, b, c} é o mesmo que {b, c, a}.

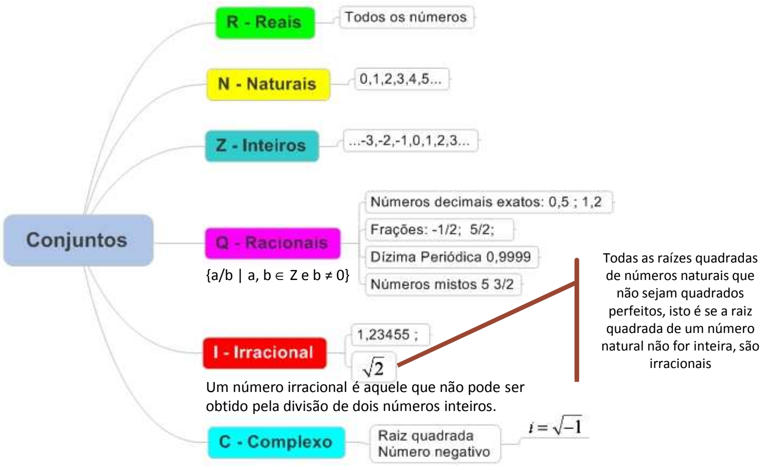
Além disso, se **a** é um elemento de um conjunto, a e {a} são considerados diferentes, isto é, a ≠ {a}. Pois {a} denota o conjunto consistindo do elemento **a** somente, enquanto que **a** é apenas o elemento do conjunto {a}.



MÓDULO 1: TEORIA DOS CONJUNTOS

14

CONJUNTOS NUMÉRICOS

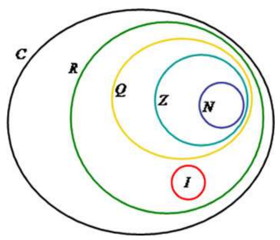


Obs: $x + iy$ é chamada de forma normal de um número complexo. Se y=0, temos um número real x. Por isso todos os conjuntos estão contidos em C.

MÓDULO 1: TEORIA DOS CONJUNTOS

15

CONJUNTOS NUMÉRICOS



É evidente que: $N \subset Z \subset Q \subset R \subset C$.

Quando acrescentamos o símbolo * (estrela) num conjunto numérico, estamos indicando que o zero foi excluído do conjunto.

Exemplo:

$Z^* = \{x \in Z \mid x \neq 0\} = \{\ldots,-4,-3,-2,-1,1,2,3,\ldots\}$

Quando acrescentamos o símbolo + (mais), estamos indicando que foram excluídos todos os números negativos do conjunto.

Exemplo:

$Z_+ = \{x \in Z \mid x \geq 0\} = \{0,1,2,3,\ldots\}$

Quando acrescentamos o símbolo - (menos), estamos indicando que foram excluídos todos os números positivos do conjunto.

Exemplo:

$Z_- = \{x \in Z \mid x \leq 0\} = \{\ldots,-4,-3,-2,-1,0\}$

Por definição o número zero é elemento dos conjuntos Z_+, Z_-, Q_+, Q_-, R_+, R_-.
Para excluirmos o zero destes conjuntos, devemos usar as seguintes representações: Z^*_+, Z^*_-, Q^*_+, Q^*_-, R^*_+, R^*_- .

MÓDULO 1: TEORIA DOS CONJUNTOS

16

INTERVALOS NUMÉRICOS EM $\mathbb{R}$

Sejam a e b dois números reais, com a < b, define-se:

[a,b] = {x ∈ R | a ≤ x ≤ b} (intervalo fechado)
[a,b[= { x ∈ R | a ≤ x < b} (intervalo fechado à esquerda)
]a,b] = { x ∈ R | a < x ≤ b} (intervalo fechado à direita)
]a,b[= { x ∈ R | a < x < b} (intervalo aberto)

]-∞,a] = { x ∈ R | x ≤ a} (intervalo semifechado)
]-∞,a[= { x ∈ R | x < a} (intervalo semiaberto)
[a,+∞[= { x ∈ R | x ≥ a} (intervalo semifechado)
]a,+∞[= { x ∈ R | x > a} (intervalo semiaberto)
]- ∞, +∞[= R

MÓDULO 1: TEORIA DOS CONJUNTOS

17

ESPECIFICAÇÃO DE CONJUNTOS - FORMA SINTÉTICA E TABULAR

Por meio da propriedade P é possível reconhecer se um dado elemento pertence ou não ao conjunto.

{x | x possui a propriedade P}

ou

{x ∈ A | x possui a propriedade P}

Dizemos neste caso, que o conjunto está representado na **forma sintética** ou construtiva.

Exemplos:

a) { x ∈ N | x > 1 }
b) { x ∈ R | x + 4 = 0 }
c) { x | x = 2n e n ∈ Z+}

Forma tabular ou analítica, onde os elementos do conjunto são enumerados individualmente.

Exemplos:

a) { 2, 3, 4, 5, ... }
b) { -4 }
c) { 0, 2, 4, 6, 8, ... }

MÓDULO 1: TEORIA DOS CONJUNTOS

18

Exercícios

1) Dados os conjuntos A = {-1, 2} e B = {1/2, -1}, determinar o conjunto X tal que:

$$X = \{[((A \cap B) \cup \Re) \cap Q\,] \cap Z\} \cap B$$

2) Seja A = {{∅}, ∅}. Verifique quais das seguintes sentenças são verdadeiras ou falsas:

a-) {{∅}} ∈ A

b-) ∅ ∈ A

c-) {∅} ∈ A

d-) {{∅}} ⊂ A

e-) ∅ ⊂ A

f-) {∅} ⊂ A

3) Verificar quais dos seguintes conjuntos são vazios ou unitários:

A = {x ∈ N | x + 8 = 5}

D = {x ∈ Z | x^2 = 4 e x é ímpar}

B = {x ∈ Z* | -1 < x < 1}

E = {x ∈ Z | x^2 = 9 e 2x = 6 }

C = {x ∈ R | | x | < 0}

F = {x ∈ R | $x^2 - 2x + 5 < 0$}

Exercícios

4) Representar com a notação de intervalo os seguintes conjuntos:

a-) {x ∈ R | $-3 \leq x < 1$}

b-) {x ∈ R | $1 \leq x \leq 2$}

c-) {x ∈ R | $-1 < x \leq 3$}

d-) {x ∈ R | $-4 < x$}

e-) {x ∈ R | $3x < 9$}

f-) {x ∈ R | $5x - 7 \geq 8$}

g-) {x ∈ R | $x^2 - 4x + 3 \leq 0$}

5) Verificar se as igualdades abaixo são verdadeiras:

a-) {x ∈ R | x ∈ [0, +∞[e x ∈]- ∞, 0[} = ϕ

b-) {x ∈ R | $x^2 - 4x + 3 \geq 0$} = {x ∈ R | x ∉]1, 3[}

c-) {x ∈ R | $2x^2 - 5x - 3 > 0$} = {x ∈ R | x ∉ [-1/2, 3] }

UNIÃO DE CONJUNTOS

Definição: *Dados dois conjuntos A e B, chama-se união de A e B o conjunto formado pelos elementos que pertencem a A ou a B.*

Simbolicamente:

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

Pode-se concluir também que:

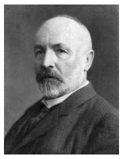
$$x \in A \cup B \Rightarrow \begin{cases} x \in A \text{ e } x \notin B \text{ ou,} \\ x \notin A \text{ e } x \in B \text{ ou ainda,} \\ x \in A \text{ e } x \in B \end{cases}$$

Exemplos:

a) $\{1, 2\} \cup \{3, 4\} = \{1, 2, 3, 4\}$

b) $\varnothing \cup \{3, 4\} = \{3, 4\}$

Na teoria dos conjuntos, a operação de união é análoga à operação de adição na aritmética.



INTERSEÇÃO DE CONJUNTOS

Definição: *Dados dois conjuntos A e B, chama-se interseção de A e B o conjunto formado pelos elementos que pertencem a A e a B.*

Simbolicamente:

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

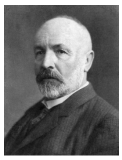
Exemplos:

a) $\{ -2, 4, 7 \} \cap \{-4, 2, 7 \} = \{ 7 \}$

b) $\{ 5, 7 \} \cap \{ 6, 10 \} = \varnothing$

OBS: Quando $A \cap B = \varnothing$ dizemos que A e B são **conjuntos disjuntos**.

Na teoria dos conjuntos, a operação de interseção é análoga à operação de multiplicação na aritmética.



COMPLEMENTO DE UM CONJUNTO

O complemento de um conjunto X, denotado X^c, consiste de todos os elementos em U (conjunto universo) que não estão em X, ou seja:

$$A^c = \{x \in U \mid x \notin A\}$$

Exemplo:

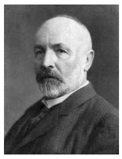
a) Seja A={1,3,5,7,9} e U={1,2,3,4,5,6,7,8,9,10}, então $A^c = \{2,4,6,8,10\}$

b) Seja B = Z+ e U = Z, então $B^c = Z^{*}-$

O complemento de um conjunto também pode ser visto como um caso particular da **diferença entre conjuntos**.

Dados dois conjuntos A e B, a diferença $A - B = \{x \mid x \in A \text{ e } x \notin B\}$.
A – B equivale ao complemento de B em relação ao conjunto A.

...é similar à operação de subtração na aritmética.



PROPRIEDADES FUNDAMENTAIS

P1. Comutativa

(a) $X \cap Y = Y \cap X$
(b) $X \cup Y = Y \cup X$

P2. Associativa

(a) $X \cap (Y \cap Z) = (X \cap Y) \cap Z$
(b) $X \cup (Y \cup Z) = (X \cup Y) \cup Z$

P3. Distributiva

(a) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$
(b) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$

P4. Idempotência

(a) $X \cap X = X$
(b) $X \cup X = X$

P5. Absorção

(a) $X \cap (X \cup Y) = X$
(b) $X \cup (X \cap Y) = X$

P6. Complementação

(a) $X \cap X^c = \varnothing$
(b) $X \cup X^c = U$

P7. Complementação dupla

$(X^c)^c = X$

P8. De Morgan (tente desenhar...)

(a) $(X \cap Y)^c = X^c \cup Y^c$
(b) $(X \cup Y)^c = X^c \cap Y^c$

P9. Operações com ∅ e U

(a) $U \cap X = X$ e $\varnothing \cup X = X$
(b) $\varnothing \cap X = \varnothing$ e $U \cup X = U$
(c) $\varnothing^c = U$ e $U^c = \varnothing$

MÓDULO 1: TEORIA DOS CONJUNTOS

Exercícios

6-) Dados os conjuntos A = {a, b, c}, B = {c, d} e C = {a, b, d}, determinar o conjunto X tal que:

$$A \cup X = \{a, b, c\}, \qquad B \cup X = \{c, d\} \quad \text{e} \quad C \cup X = A \cup B$$

7-) Dado o conjunto A = {1, 2, 3}, achar todos os conjuntos $X \neq A$ tais que $\{1\} \subset X$ e $X \subset A$.

8-) Dados os conjuntos A = {a, b, c, d} e B = {b, d, e}, achar todos os conjuntos X tais que $X \subset A$ e $X \subset B$.

9-) Se A, B e $A \cap B$ são conjuntos com 90, 50 e 30 elementos, respectivamente, então qual o número de elementos do conjunto $A \cup B$?

10-) Em uma escola, 100 alunos praticam vôlei, 150 futebol, 20 os dois esportes e 110 alunos nenhum. Qual o número total de alunos?

11-) Sejam A = {1, 3, 5, 7}, B = {5, 7, 9, 11} e C = {3, 7, 9, 13}. Determinar:

a-) $A - B$ b-) $C - A$ c-) $B - C$ d-) $B - A$ e-) $(A \cup B) - C$

Para entendermos o conceito de Partição vamos rever o Conjunto das Partes

Definição: Para todo conjunto A, existe um outro conjunto, cujos elementos são subconjuntos de A. Usaremos para esse novo conjunto a notação P(A) e a denominação "conjunto das partes de A".

$$P(A) = \{ X \mid X \subset A \}$$

Exemplos:
a) A = {a} => P(A) = {∅ , {a} }
b) A = {a,b} => P(A) = {∅, {a}, {b}, {a,b} }

PARTIÇÃO DE UM CONJUNTO

Definição: *Seja A um conjunto não vazio. Define-se como partição de A, e representa-se por **part(A)**, qualquer subconjunto do conjunto das partes de A (P(A)), que satisfaz simultaneamente, às seguintes condições:*

i-) nenhum dos elementos de part(A) é o conjunto vazio.
ii-) a interseção de quaisquer dois elementos de part(A) é o conjunto vazio.
iii-) a união de todos os elementos de part(A) é igual ao conjunto A.

Exemplo:
A = {a,b} => P(A) = {∅, {a}, {b}, {a,b} }
Part(A) = {{a}, {b}}

EQUIPOTÊNCIA DE CONJUNTOS

Definição: *Dois conjuntos finitos X e Y têm o mesmo número de elementos se e somente se existe uma correspondência um-a-um $f: X \rightarrow Y$.*

Portanto, podemos afirmar que dois conjuntos X e Y são equipotentes, fato denotado por $X \sim Y$, quando existe uma correspondência um-a-um $f: X \rightarrow Y$.

Exemplo:
X = {4,9}

f: $X \rightarrow Y = (f(|\sqrt{x}|) \rightarrow Y)$

Y = {2,3}

CONJUNTO ENUMERÁVEL

Definição: *Um conjunto X é dito ser enumerável quando $X \sim N$ (N é o conjunto dos Naturais). Ou seja, são equipotentes, ou ainda seja, possuem o mesmo número de elementos.*

PRODUTO CARTESIANO

Definição: Sejam A e B dois conjuntos não vazios. O produto cartesiano de A e B, denotado por A x B é definido por:

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

Portanto, o produto de dois conjuntos A e B é o conjunto de todos os pares ordenados cujas primeiras coordenadas pertencem a A e as segundas pertencem a B

PRODUTO CARTESIANO

Generalizando, dados n conjuntos A_1, A_2,...,A_n , o produto cartesiano destes n conjuntos é dado por:

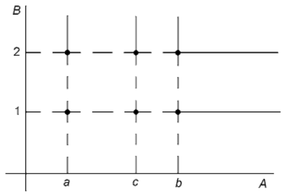
$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1 \text{ e } a_2 \in A_2 \text{ e} \ldots \text{e } a_n \in A_n\}$$

Exemplo:
Seja A = {a,b,c} e B = {1,2}:

A × B = {(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)}
B × A = {(1, a); (1, b); (1, c); (2, a); (2, b); (2, c)}

Nota-se que A × B ≠ B × A.

Pode-se representar geometricamente o produto cartesiano A × B como o conjunto de pontos destacados na seguinte figura:



Módulo 1: Teoria dos Conjuntos

29

RELAÇÃO BINÁRIA (R)

Definição: *Sejam A e B dois conjuntos não vazios. Uma* ***relação binária R*** *sobre A e B é um subconjunto de A × B, isto é, R ⊂ A × B. Ou seja, a relação binária está contida no produto cartesiano.*

Exemplo:
Sejam A = {1, 2, 3} e B = { x, y, z} , e seja R = {(1,y), (1,z), (3,y)}.
Então R é uma relação de A para B, uma vez que R é um subconjunto de A x B

- Dizemos que **y é correspondente de x** pela relação R **se (x, y) ∈ R**, e denotamos **xRy** (lê-se x-erre-y).
- Se **R ⊂ A × A**, dizemos que **R é uma relação binária sobre A**.

OBS: O número de relações binárias distintas entre dois conjuntos finitos A e B, com *m* e *n* elementos, respectivamente, é igual a 2^{mn}.
Porque o produto cartesiano A × B tem *mn* elementos
e, por isso, 2^{mn} subconjuntos.

Módulo 1: Teoria dos Conjuntos

30

RELAÇÃO BINÁRIA (R)

Exemplo:
Seja A = {a,b} e B = {1,2}: // m=2 e n=2
A × B = {(a, 1), (a, 2), (b,1),(b,2)} //m*n=4
//2^{m*n}=16

Subconjuntos de AxB =

{Ø} O conjunto vazio é subconjunto de qualquer conjunto.

{(a, 1)},	{(a,1),(a, 2)},	{(a,1),(a,2),(b, 1)},
{(a, 2)} ,	{(a,1),(b, 1)},	{(a,1),(a,2),(b, 2)},
{(b, 1)},	{(a,1),(b, 2)},	{(a,2),(b,1),(b, 2)},
{(b, 2)},	{(a,2),(b, 1)},	{(a,1),(b,1),(b, 2)},
	{(a,2),(b, 2)},	
	{(b,1),(b, 2)},	{(a,1)(a,2),(b,1),(b, 2)},

MÓDULO 1: TEORIA DOS CONJUNTOS

31

VALE LEMBRAR...

A **Partição** de um conjunto é um subconjunto, com 3 condições específicas, do **Conjunto das partes**:

Part(A) ⊂ P(A)

E a Relação Binária também é um subconjunto do Produto Cartesiano.

aRb ⊂ A x B

MÓDULO 1: TEORIA DOS CONJUNTOS

32

FUNÇÃO

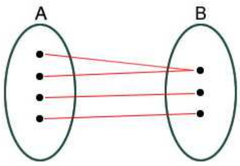
Definição: *Uma relação binária $f \subset A \times B$ é uma **função** de A em B se para todo $x \in A$ existe um único $y \in B$ tal que $(x, y) \in f$.*

A função é denotada **f: A → B** e em vez de **xfy** denotamos **f(x) = y**.
O elemento $y = f(a) \in B$ é a imagem de $a \in A$.

FUNÇÃO Sobrejetora

Definição: *Uma* função f: A → B é dita sobrejetora quando o contradomínio (elementos de B) da função for igual ao conjunto imagem. Em outras palavras, uma função é sobrejetora quando todo elemento de B é imagem de pelo menos um elemento de A.

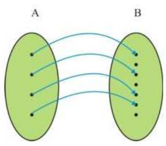
Exemplo:



FUNÇÃO Injetora

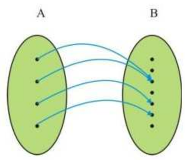
Definição: *Uma função f: A → B é dita injetora se dois elementos distintos de A correspondem sempre a duas imagens distintas em B.*

Exemplo



$a \neq b \Rightarrow f(a) \neq f(b)$

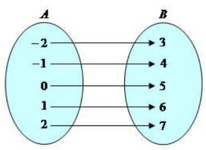
Contraexemplo



FUNÇÃO Bijetora

Definição: *Uma função f: A → B é bijetora se for sobrejetora e injetora, isto é, se todos os elementos do domínio A estão associados a todos os elementos do contradomínio B de forma um para um e exclusiva.*

Exemplo



MÓDULO 1: TEORIA DOS CONJUNTOS

Exercícios

12-) Seja A = {0, {1,2}} determinar P (A), ou seja o conjunto das partes de A.

13-) Sendo E = {a}, determinar P(P(E)).

14-) Determinar P(P(P(ϕ))).

15-) Achar os pares de conjuntos disjuntos entre os seguintes conjuntos:

A = {1, 3, 4}   B = {0, 1, 2, 3}   C = {4, 5, 6}

D = {5, 6, 7}   E = {2, 4, 6, 8}

16-) (ENADE 2008) Considerando o conjunto A = {1, 2, 3, 4, 5, 6}, qual opção corresponde a uma partição desse conjunto?

a-) {{1}, {2}, {3}, {4}, {5}, {6} }
b-) {{1}, {1,2}, {3,4}, {5, 6}}
c-) {{ }, {1, 2, 3}, {4, 5, 6}}
d-) {{1, 2, 3}, {5, 6}}
e-) {{1, 2}, {2, 3}, {3, 4}, {4, 5}, {5, 6}}

Exercícios

17-) (Poscomp 2006)

[MT] Seja o conjunto $A = \{x \in \mathbb{R}, |x| \geq 1\}$. Qual das alternativas é uma partição do conjunto A.

(a) $\{x < -1\},\ \{x > 1\},\ \{1, -1\}$
(b) $\{x \leq 0\},\ \{x \geq 1\},\ \{0\}$
(c) $\{x \leq -1\},\ \{x \geq 3\}, \{1 \leq x \leq 3\}$
(d) $\{x \leq -5\},\ \{-5 < x \leq -3\},\ \{-1\},\ \{x \geq 1\}$
(e) Todas as alternativas são partições de A.

18-) (Poscomp 2002) Para cada n ∈ N seja D_n = (0, 1/n), onde (0, 1/n) representa o intervalo aberto de extremos 0 e 1/n. O conjunto diferença $D_3 - D_{20}$ é igual a:
(a) D_3
(b) D_{20}
(c) (1/20, 1/3)
(d) [1/20, 1/3)
(e) $D_{20} \cup D_3$

19-) (Poscomp 2002) Todos os convidados presentes num jantar tomam chá ou café. Treze convidados bebem café, dez bebem chá e 4 bebem chá e café. Quantas pessoas tem nesse jantar.

(a) 19 (b) 27 (c) 23 (d) 15 (e) 10

Módulo 2: Teoria dos Grafos

INTRODUÇÃO

Para um conjunto de objetos, observamos:

1. O conteúdo dos objetos, e
2. a estrutura do conjunto, ou seja , as relações entre os objetos.

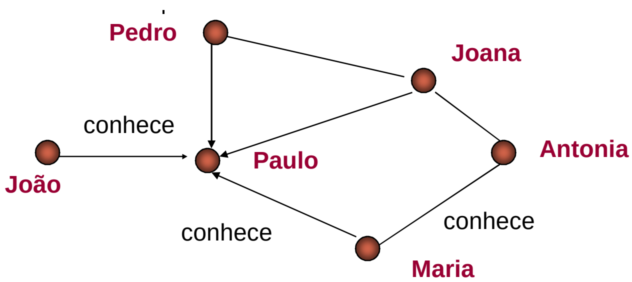
A Teoria dos Grafos (TG) permite que se concentre no segundo ponto, fazendo abstração do primeiro.

Diagramas representam situações reais

nós (vértices): representam objetos

enlaces (arestas): relações entre objetos

Ex.: Seja o Grafo G – *Quem conhece Paulo?*



INTRODUÇÃO

1847 - Kirchhof

Estudo de circuitos elétricos (não eram CI´s!) utilizando grafos

1857 - Cayley

Enumeração de isômeros dos hidrocarbonatos alifáticos saturados, em química orgânica

1869 - Jordan

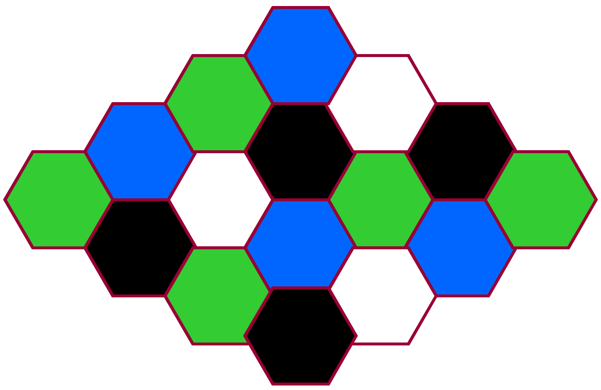
Estudo de Árvores (estritamente matemático)

1879 - Kempe

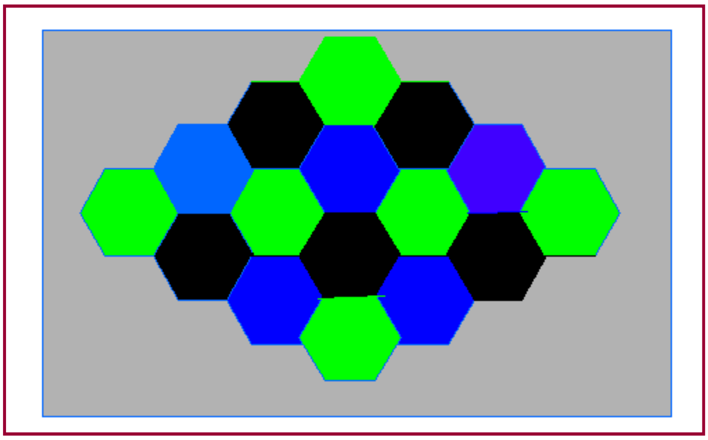
- Apresenta a Conjectura das 4 cores apresentada por Guthrie a De Morgan
- Provar que todo mapa geográfico desenhado no plano e dividido em um número qualquer de regiões pode ser colorido utilizando-se 4 cores, não é necessário mais que isso, sem que duas regiões fronteiriças recebam a mesma cor.
- Foi provado que 5 cores podiam ser usadas(mas todos já sabiam que 4 era possível.
- Quase 100 anos se passaram até que a solução para as 4 cores foi provada.

1977 - Appel e Haken: Provam matematicamente

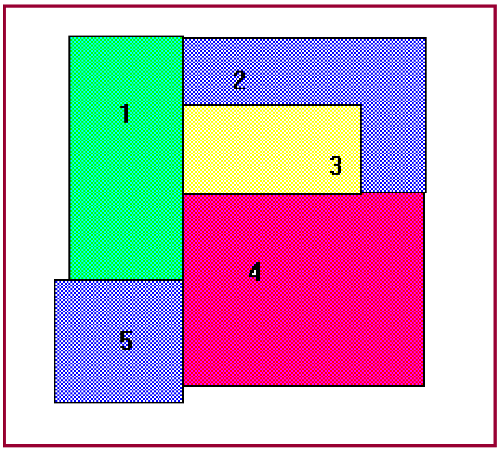
Conjectura das 4 cores



Conjectura das 4 cores

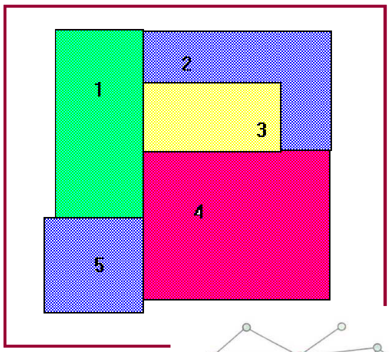


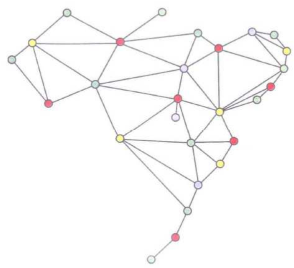
Conjectura das 4 cores

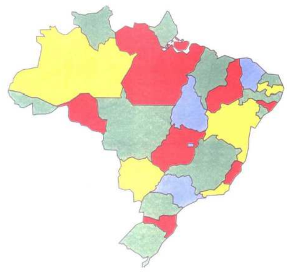


Módulo 2: Teoria dos Grafos

Conjectura das 4 cores







Conjectura das 4 cores

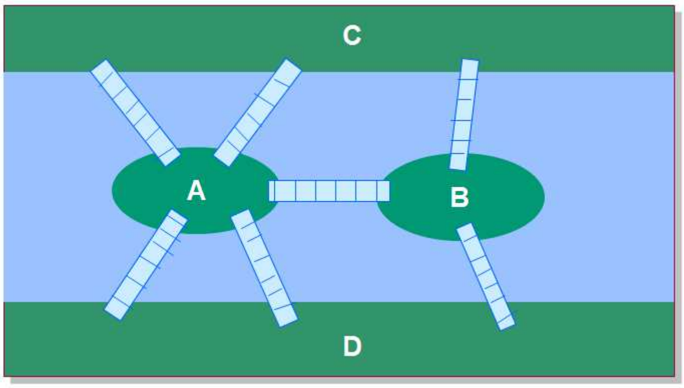
Teorema: *<u>Todo</u> grafo planar (o que é isso?), pode ser colorido com 4 cores (não mais que isso) sem que hajam regiões adjacentes com cores iguais.*

É obvio que pode-se colorir <u>alguns grafos</u>
com 3 cores, 2 cores (ou 1!). Mas estes mapas não possuem características de mapas geográficos.

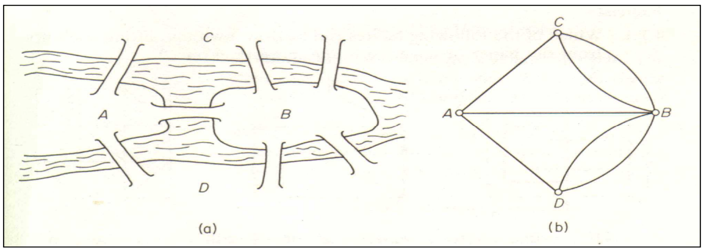
Problema da ponte de Königsberg
(Prússia oriental- hoje a cidade de Kaliningrado)
1736 - Euler

- 2 ilhas no rio Pregel formando 4 regiões distinguíveis de terra (A, B, C e D}
- Há 7 pontes interligando as regiões
- Problema: partindo de uma dessas regiões, determinar um trajeto pelas pontes segundo o qual se possa <u>retornar</u> à região de partida , atravessando <u>cada ponte</u> somente <u>uma</u> vez.

PROBLEMA DA PONTE DE KÖNIGSBERG



GRAFO EULERIANO

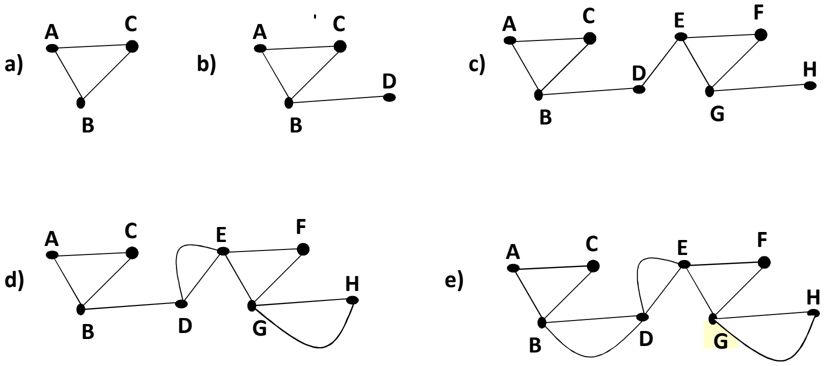


Grafo Euleriano

Teorema: *Um grafo conectado (o que é isso!?) não vazio é euleriano se e somente se ele não possui vértices de grau (nº de arestas adjacentes a ele) ímpar.*

Exercícios

1. Verifique quais grafos abaixo são Eulerianos:



2. Construa 3 grafos Eulerianos e 3 não Eurelianos:

APLICAÇÕES DE TEORIA DOS GRAFOS

Existem funções inúteis no programa?

Considere que funções são vértices e existe aresta de f para g se existe chamada a g no corpo de f:

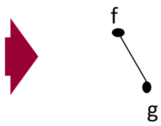
void f (int n)

{ if (n > 5)

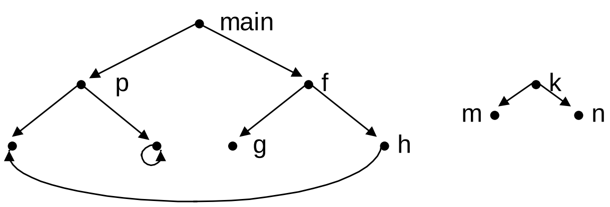
g ( );

...

}



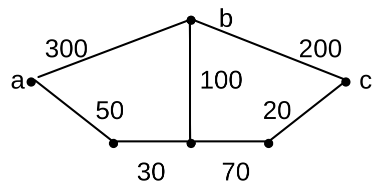
Monta-se um grafo de todo o programa:



APLICAÇÕES DE TEORIA DOS GRAFOS

MÓDULO 2: TEORIA DOS GRAFOS

Um vendedor deve passar por várias cidades e retornar ao ponto inicial. Qual o trajeto de menor distância possível ?



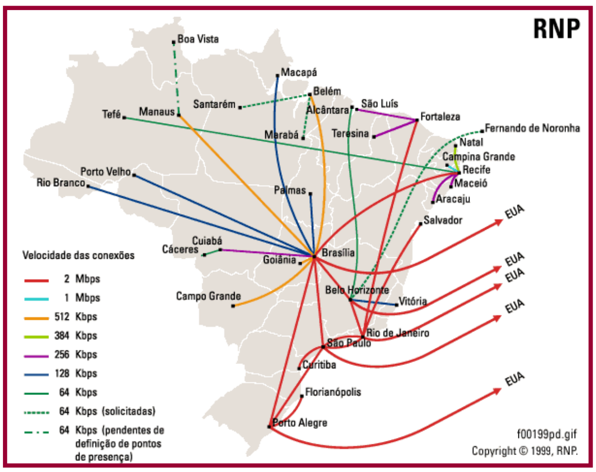
Qual a menor distância entre duas cidades a e c ?

49

APLICAÇÕES DE TEORIA DOS GRAFOS

MÓDULO 2: TEORIA DOS GRAFOS

Como mapear uma "confusão" dessas...



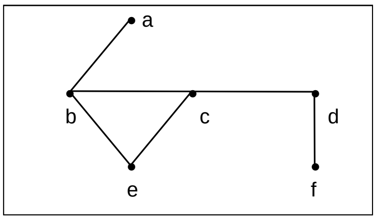
50

APLICAÇÕES DE TEORIA DOS GRAFOS

Ainda:

Engenharias (civil, elétrica, química,...)
Matemática
Economia
Sociologia
Linguística
....

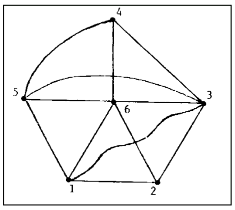
Definição: *Um grafo G = (V, E) é um conjunto V de vértices e um conjunto E de arestas (edges) onde cada aresta é um par de vértices (Ex.: (v, w)). Um grafo é representado graficamente usando círculos para os vértices e retas ou curvas para arestas.*



V = {a, b, c, d, e, f} e E = {(a, b), (b, c), (b, e), (c, e), (c, d), (d, f)} onde (a, b) é uma aresta entre vértice a e b.

CONCEITOS BÁSICOS

- Não há forma única para desenhar um grafo.
- Posições relativas de linhas e arestas nada significam.
- Um diagrama de um grafo somente mostra a relação de incidência entres seus vértices e arestas;
- À uma aresta é associado somente um par de vértices (extremidades);
- Arestas podem se interceptar (não planar).
- Cardinalidades (Notação: n = |V | e m = |E |)
- Duas arestas são adjacentes se possuem um vértice (extremidade) comum.
- Dois vértices são adjacentes se neles incidem uma mesma aresta.
- A visualização de um grafo é feita através de sua representação geométrica (diagrama de um grafo)



V = {1,2,3,4,5,6}

e = {(1,2),(1,3),(3,2),(3,6),(5,3),(5,1), (5,6),(4,6),(4,5),(6,1),(6,2),(3,4)}

CONCEITOS BÁSICOS

Laço

Definição: *Uma aresta e = (v,v), i.e., formada por um par de vértices idênticos.*

Enlace

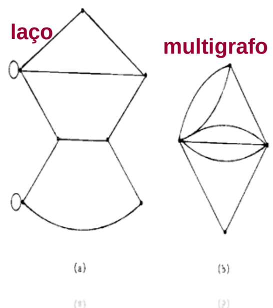
Definição: *Uma aresta e = (v, w), com v ≠ w.*

Multigrafo

Definição: *Grafo que permite arestas paralelas.*

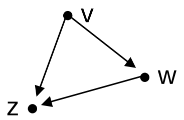
Grafo Simples

Definição: *Grafo que não permite laço nem arestas paralelas.*



CONCEITOS BÁSICOS

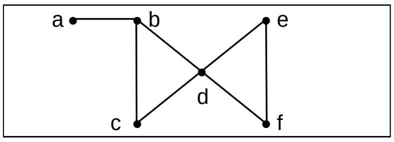
Um grafo pode ser dirigido ou não dirigido. Em um grafo dirigido, a ordem entre os vértices de uma aresta (v, w) é importante. Esta aresta é diferente da aresta (w, v) e é representada com uma flecha de v para w:



V = {v, w, z}   E = {(v, w), (v, z), (w, z)}

Um *circuito* é um caminho onde $v_1 = v_{último}$ como b, c, d, e, f, d, b.

Um circuito será simples se nenhum vértice aparecer mais de uma vez, exceto o primeiro e o último. Um circuito simples é chamado de *ciclo*.

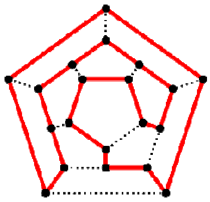


CICLO HAMILTONIANO

Um caminho hamiltoniano é um caminho que permite passar por todos os vértices de um grafo G, não repetindo nenhum, ou, seja, passar por todos uma e uma só vez por cada.

Caso esse caminho seja possível descrever um ciclo, este é denominado ciclo hamiltoniano (ou circuito hamiltoniano) em G. E, um grafo que possua tal circuito é chamado de grafo hamiltoniano

Sir William Rowan Hamilton
1805 – 1865
Matemático, físico e astrônomo



Um problema que envolve caminhos hamiltonianos é o problema do caixeiro viajante, em que um caixeiro deseja visitar um conjunto de N cidades (vértices), passando por cada cidade exatamente uma vez e retornando à cidade de origem, fazendo o caminho de menor tamanho possível

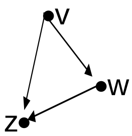
MÓDULO 2: TEORIA DOS GRAFOS

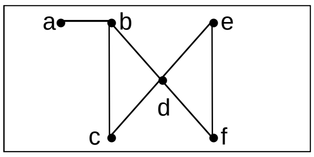
55

MAIS DEFINIÇÕES ...

Definição: *Um grafo é conectado ou conexo se existe um caminho entre dois vértices quaisquer do grafo.*

Definição: *Dígrafo é um grafo dirigido*





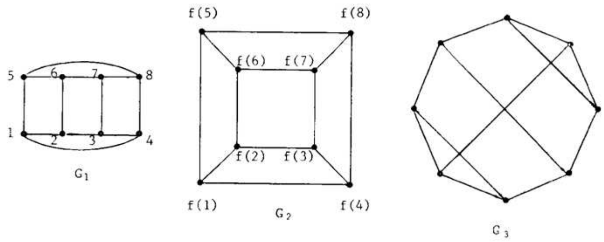
Definição: *O grau de um vértice é o número de arestas adjacentes a ele. Em um grafo dirigido, o grau de entrada de um vértice v é o número de arestas (w, v) e o grau de saída é o número de arestas (v, w).*

MÓDULO 2: TEORIA DOS GRAFOS

56

GRAFO REGULAR DE GRAU (R)

Definição: *Todos os vértices de G possuem o mesmo grau.*



Exemplo: Grafos regulares grau (3) e |V| =8

Observe que para um mesmo número de vértices pode-se ter vários grafos regulares!!

Exercícios

1) Construir uma representação geométrica do grafo G = (V,E), onde:

   V = {1,2,3,4,5,6}
   E = {(1,3), (1,4), (1,5), (2,3),(2,4),(2,5),(3,5),(4,5)}

2) Os amigos João, Pedro, Antônio, Marcelo e Francisco sempre se encontram para botar conversa fora e às vezes jogar dama, xadrez e dominó. As preferências de cada um são as seguintes: João só joga xadrez; Pedro não joga dominó; Antônio joga tudo; Marcelo não joga xadrez e dominó e Francisco não joga nada.

   a) Represente através de um grafo G=(V,E) todas as possibilidades de um amigo jogar com os demais. Defina V e E.

   a) Defina um subgrafo em que todos, menos Francisco, joguem ao mesmo tempo

3) Desenhe 3 grafos regulares com |V| =4.

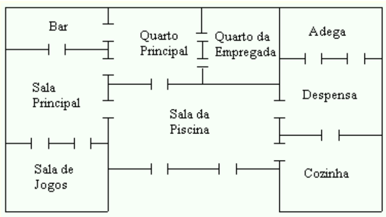
Exercícios

4) "Todo grafo completo é regular". Esta afirmativa é verdadeira? Comente sobre a afirmação e prove.

5) "Toda arvore é um grafo mas nem todo grafo é uma árvore". Esta afirmativa é verdadeira? Comente sobre a afirmação e prove.

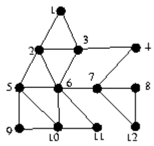
6) O cenário abaixo é a residência do bilionário Count Van Diamond, que acaba de ser assassinado. Sherlock Gomes (um conhecido detetive que nas horas vagas é um estudioso da Teoria dos Grafos) foi chamado para investigar o caso. O mordomo alega ter visto o jardineiro entrar na sala da piscina (lugar onde ocorreu o assassinato) e logo em seguida deixar sair daquela sala pela mesma porta que havia entrado. O jardineiro, contudo, afirma que ele não poderia ser a pessoa vista pelo mordomo, pois ele havia entrado na casa, passado por todas as portas uma única vez e, em seguida, deixado a casa.

Sherlock Gomes avaliou a planta da residência (conforme figura abaixo) e em poucos minutos declarou solucionado o caso. Quem poderia ser o suspeito indicado por Sherlock Gomes? Qual o raciocínio utilizado pelo detetive para apontar o suspeito?



Exercícios

7) Com relação ao grafo ao lado, classifique-o:



8) Desenhe um grafo não planar.

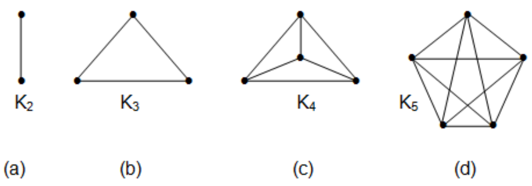
9) Qual o sentido prático da Teoria Cromática sobre Grafos.

10) "Todo grafo Euleriano com um número par de nós é regular." Isso é verdade? Prove.

SUMIDOURO, FONTE E COMPLETO

Definição: Uma fonte é um vértice com grau de entrada 0 e grau de saída ≥ 1. Um sumidouro é um vértice com grau de saída 0 e grau de entrada ≥ 1.

Definição: Um grafo é completo quando existe uma aresta entre dois vértices quaisquer do grafo. O grafo completo de n vértices é denotado por Kn.



$C_{n,2}$ arestas = Cn,2 = n! / (2!(n-2)!) *// combinação de N, 2 a 2*

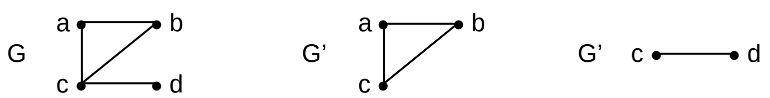
Ex: n = 1: K1 grafo vazio (0 arestas)
n = 2: k2 → 1 aresta
n = 3: K3 → 3 arestas
......

MÓDULO 2: TEORIA DOS GRAFOS

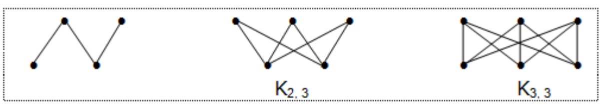
61

SUBGRAFO E GRAFO BIPARTIDO

Definição: Um subgrafo G' = (V', E') de um grafo G = (V, E) é um grafo tal que V' ⊆ V e E' ⊆ E. Exemplos:



Definição: *Um grafo G = (V, E) é bipartido se V pode ser dividido em dois conjuntos V1 e V2 tal que toda aresta de G une um vértice de V1 a outro de V2.*



MÓDULO 2: TEORIA DOS GRAFOS

62

ISOMORFISMO

Problema :

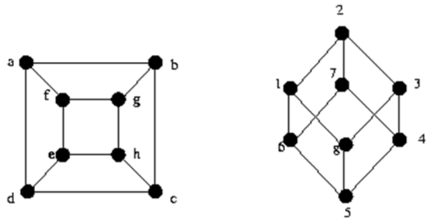
Dados dois grafos :

G1 = (V1, E1) e G2 = (V2, E2)

com |V1| = | V2| = n

$$G1 \approx G2 \ ?$$

Definição: *Dois grafos $G_1(V_1,E_1)$ e $G_2(V_2,E_2)$ são ditos isomorfos entre si se existe uma correspondência entre os seus vértices e arestas de tal maneira que a relação de incidência seja preservada. Em outros termos, temos $|V_1|= |V_2|$ e existe uma função f: $V_1 \rightarrow V_2$, tal que (i,j) é elemento de E_1 se e somente se (f(i),f(j)) é elemento de E_2.*

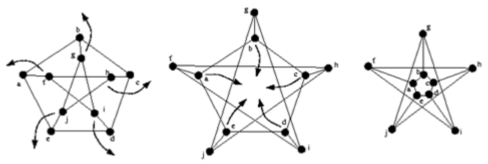


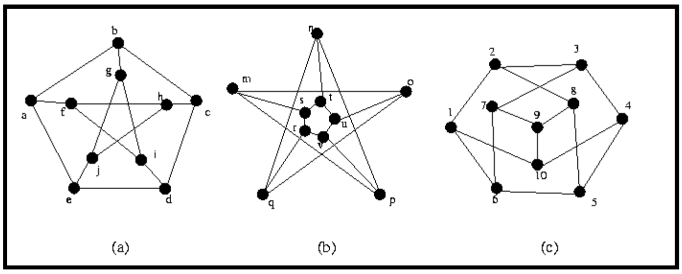
Para ver o isomorfismo dos grafos da figura , podemos utilizar a seguinte função:
f(a) = 1, f(b) = 2, f(c) = 3, f(d) = 8, f(e) = 5, f(f) = 6, f(g) = 7, f(h) = 4.

MÓDULO 2: TEORIA DOS GRAFOS

63

ISOMORFISMO: Técnica da "Movimentação"





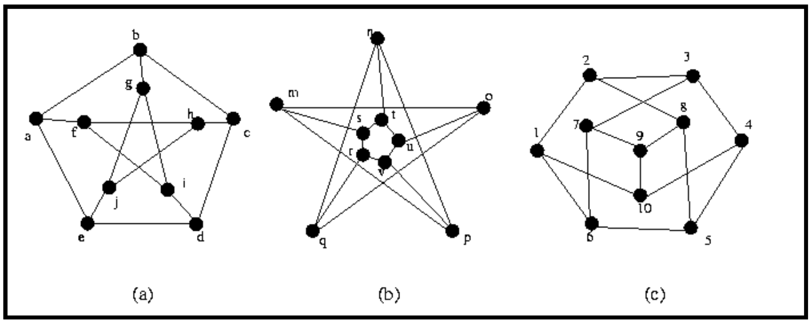
Para ver o isomorfismo dos grafos (a) e (b), utilize a seguinte função:

f(a) = s, f(b) = t, f(c) = u, f(d) = v,
f(e) = r, f(f) = m, f(g) = n, f(h) = o, f(i) = p, f(j) = q

MÓDULO 2: TEORIA DOS GRAFOS

64

ISOMORFISMO: Técnica da "Movimentação"



Para ver o isomorfismo dos grafos (a) e (c), utilize a seguinte função:

f(a) = 1, f(b) = 10, f(c) = 4, f(d) = 5, f(e) = 6

f(f) = 2, f(g) = 9, f(h) = 3, f(i) = 8, f(j) = 7

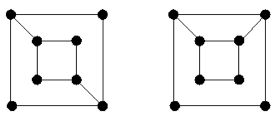
ISOMORFISMO

"Esses exemplos devem ser suficientes para mostrar que não é sempre fácil determinar se dois grafos são isomorfos. Não existe atualmente um algoritmo eficiente para resolver esse problema. Poderiamos tentar todas as permutações possível, mas isso daria um algoritmo de complexidade em O(n!)".

Para que dois grafos sejam isomorfos, no mínimo essas condições tem que ser respeitadas:

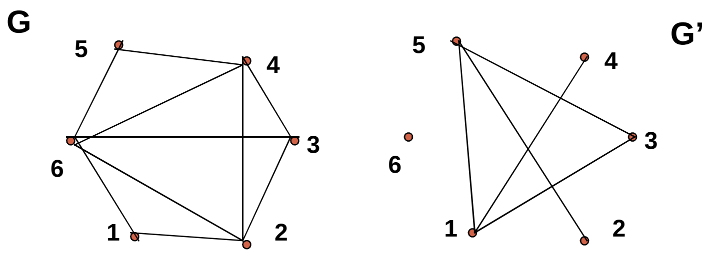
1. Os dois têm o mesmo número de vértices.
2. Os dois têm o mesmo número de arestas.
3. Os dois têm o mesmo número de vértices de grau *n*, para qualquer valor *n* entre 0 e o número de vértices que o grafo contém.

Note que isso não é suficiente para que sejam isomorfos. Por exemplo, os grafos da figura ao lado respeitam essas condições e não são isomorfos.



Complemento de um Gráfico

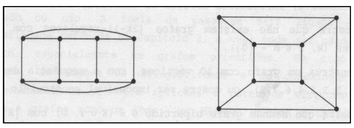
Definição: G’(V’,E’) é complemento de G (V, E) se possui o mesmo conjunto de vértices (V’=V) tal que para todo par de vértices distintos v, w ∈ V tem-se que (v,w) é aresta de G’ se e somente se (v,w) não for aresta de G.

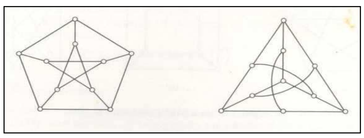


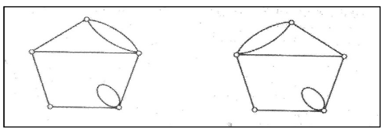
Exercícios

1) Construa representações geométricas de grafos regulares (todos os vértices com mesmo grau) de grau r (r = 1,2,3 e 4).

2) Identifique se os grafos a seguir são isomorfos:

A) 

B) 

C) 

3) Quantos grafos (simples= sem laços e sem paralelas) não isomorfos com 4 vértices existem?
Mostre as representações geométricas desses grafos

4) Exemplifique representações geométricas de grafos completos Kn (n = 1,2,3,4 e 5)

5) Escreva uma situação que possa ser modelada por um grafo bipartido não completo

OPERAÇÕES SOBRE GRAFOS

- A união de dois grafos $G_1 = (V_1,E_1)$ e $G_2= (V_2,E_2)$, denotada $G_1 \cup G_2$, é um grafo $G_3 = (V_3,E_3)$, onde $V_3 = V_1 \cup V_2$ e $E_3 = E_1 \cup E_2$.

- Um grafo é dito decomposto em dois grafos $G_1=(V_1,E_1)$ e $G_2= (V_2,E_2)$ se $G_1 \cup G_2 = G$ e se $E1 \cap E2$ é vazio.

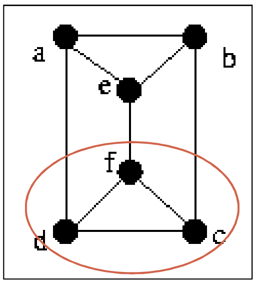
- Remoção: Seja v_i um vértice de G. O grafo $G - v_i$ é um subgrafo de G onde v_i é retirado, com todas as arestas incidentes a v_i.

MÓDULO 2: TEORIA DOS GRAFOS

69

CLIQUE DE UM GRAFO

Definição: *Um subgrafo de G que seja completo. Num(a) clique existe uma aresta entre cada par de vértices distintos.*



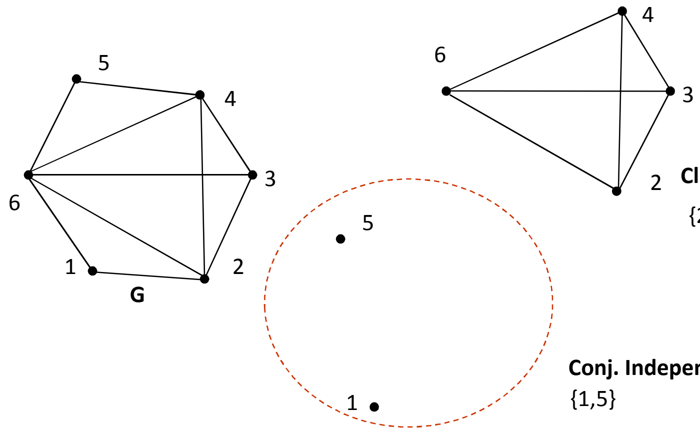
Clique=3

O tamanho de uma clique = cardinalidade do seu conjunto de vértices.

MÓDULO 2: TEORIA DOS GRAFOS

70

CONJUNTO INDEPENDENTE DE VÉRTICES



Clique
{2,3,4,6}

Conj. Independente
{1,5}

REPRESENTAÇÃO DE GRAFOS

Estruturas

Matrizes

- ✓ de Adjacências;
- ✓ de Incidências.

Listas

MATRIZ DE ADJACÊNCIAS

- Dado um grafo G (V, E), a matriz de adjacências R = (rij), é uma matriz de ordem n x n, tal que:

  $r_{ij} = 1 \Leftrightarrow (v_i, v_j) \in E$

  $r_{ij} = 0$ caso contrário

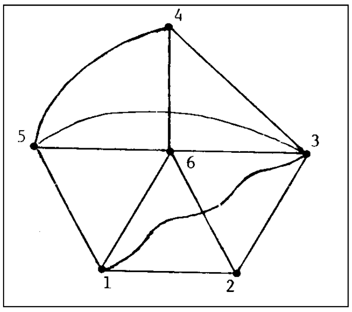
  Ou seja :

  $r_{ij} = 1$ quando os vértices v_i, v_j forem adjacentes;

  $r_{ij} = 0$ caso contrário.

MATRIZ DE ADJACÊNCIAS

G



R

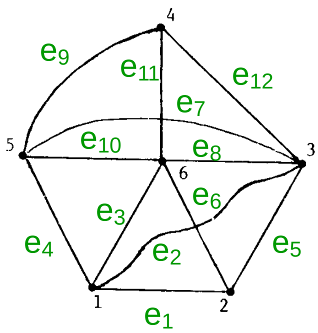
Matriz de Adjacências

	1	2	3	4	5	6
1	0	1	1	0	1	1
2	1	0	1	0	0	1
3	1	1	0	1	1	1
4	0	0	1	0	1	1
5	1	0	1	1	0	1
6	1	1	1	1	1	0

Propriedades da Matriz de Adjacências

- R é simétrica para um grafo não direcionado
- O número de 1's é igual a 2 m (m = número de arestas), pois cada aresta (v_i, v_j) origina dois 1's em R (r_{ij} e r_{ji}).

MATRIZ DE INCIDÊNCIAS



(arestas)

Vértices	1	2	3	4	5	6	7	8	9	10	11	12
1	1	1	1	1	0	0	0	0	0	0	0	0
2	1	0	0	0	1	1	0	0	0	0	0	0
3	0	1	0	0	1	0	1	1	0	0	0	1
4	0	0	0	0	0	0	0	0	1	0	1	1
5	0	0	0	1	0	0	1	0	1	1	0	0
6	0	0	1	0	0	1	0	1	0	1	1	0

- Dado um grafo G (V, E), a matriz de incidências B[bij], de ordem n x m, tal que:

  b_{ij} = 1 ⇔ vértice v_i e aresta e_j forem incidentes,

  b_{ij} = 0 caso contrário.

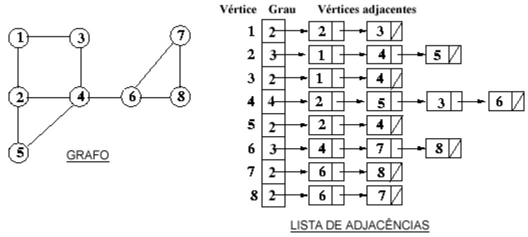
- Ou então:

  b_{ij} = 1 quando o vértice v_i for uma extremidade da aresta e_j.

  b_{ij} = 0 caso contrário.

LISTA DE ADJACÊNCIAS

- Estrutura mais simples e econômica.
- Seja G (V, E) um grafo.
  - ✓ A estrutura de adjacências A de G é um conjunto de n listas A(v), uma para cada v ∈ V.
  - ✓ Cada lista A(v) é denominada Lista de Adjacências do vértice v, e contém os vértices w adjacentes a v em G.

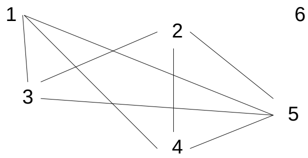


Exercícios

1) Considere o grafo G = (V,E), onde:

V = {1,2,3,4,5,6}
E = {(1,3), (1,4), (1,5), (2,3),(2,4),(2,5),(3,5),(4,5)}

Represente-o através de suas matrizes de adjacência e de incidência.



2) Apresente um exemplo de um grafo qualquer e seu respectivo grafo complemento

Exercícios

3) *Escreva um pseudocódigo que verifique se um grafo G(V,E) é:*

3.1) Regular (utilizando uma matriz de incidência)

3.2) Euleriano (utilizando uma matriz de adjacência)

3.2) Conexo (utilizando uma matriz de adjacência)

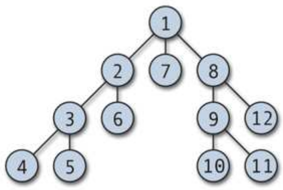
3.2) Possui Laço (utilizando uma matriz de incidência)

MÓDULO 2: TEORIA DOS GRAFOS

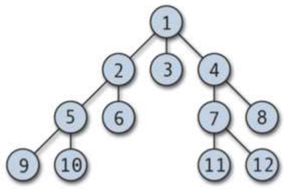
77

BUSCAS EM GRAFOS

BUSCA EM PROFUNDIDADE



BUSCA EM LARGURA



- A busca em profundidade é recursiva (utiliza uma PILHA).
- A busca em largura é, normalmente, iterativa (utiliza uma fila FIFO).

MÓDULO 2: TEORIA DOS GRAFOS

78

BUSCA EM PROFUNDIDADE

```
/* Main*/
desmarcar todos os vertices
definir uma pilha Q
escolher uma raiz s P(s)

dados: G(V,E) conexo

procedimento P(v)
marcar v
colocar v na pilha Q
para w pertencente a A(v) efetuar /* A(v): lista de adj de v */
{           se w  nao é marcado entao
                                        {visitar (v,w)  // arestas de árvore
                                         P(w)}
                                      senao
                                          se w pertence a Q e v,w nao sao consecutivos em Q
                                                  entao
                                                        visitar (v,w) // arestas de retorno
retirar v de Q
}
```

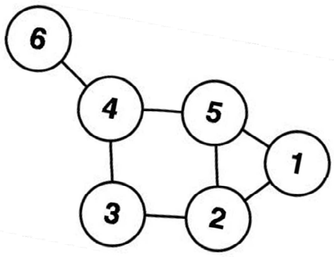

BUSCA EM LARGURA

```
dados: G(V,E)

desmarcar todos os vertices
escolher uma raiz s pertencente a V
definir uma FILA  Q, vazia

procedimento L(v)
marcar s
inserir s em Q
enquanto Q for diferente de 0 efetuar /* diferente de vazio */
  seja v o primeiro elemento de Q
  para w pertencente a A(v) efetuar
     se w e nao marcado
          entao
              visitar (v,w)
              marcar w
              inserir w em Q
          senão
              se w pertence a Q
                 entao    visitar (v,w)
  retirar v de Q
```

Exercícios

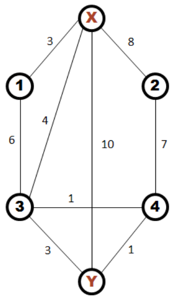
1) *Faça o rastreamento, partindo do vértice 1, e imprima a ordem de visitas aos vértices do grafo abaixo seguindo as buscas:*

   A) Por profundidade
   B) Por Largura



CAMINHO MÍNIMO – ALGORITMO DE DIJKSTRA

O algoritmo de Dijkstra considera um conjunto S de menores caminhos, iniciado com um vértice inicial . A cada passo do algoritmo busca-se nas adjacências dos vértices pertencentes a S aquele vértice com menor distância relativa a I e adiciona-o a S e, então, repetindo os passos até que todos os vértices alcançáveis por I estejam em S. As arestas que ligam vértices já pertencentes a S são desconsideradas (Algoritmo Guloso).

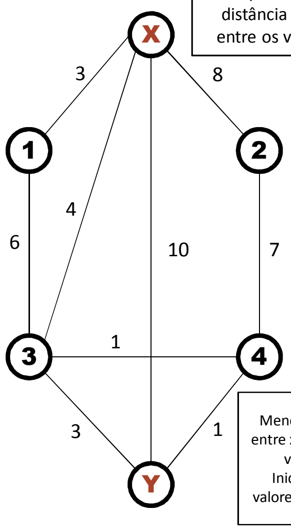


Edsger Wybe Dijkstra

Ciência da computação

Nacionalidade	Neerlandês
Nascimento	11 de Maio de 1930
Local	Roterdã, Países Baixos
Morte	6 de Agosto de 2002 (72 anos)
Local	Nuenen, Países Baixos
Atividade	
Campo(s)	Ciência da computação
Orientador(es)	Adriaan van Wijngaarden
Orientado(s)	Nico Habermann, Jan L. A. van de Snepscheut
Conhecido(a) por	Algoritmo de Dijkstra, Semáforo, THE
Prêmio(s)	Prêmio Turing (1972)

CAMINHO MÍNIMO – ALGORITMO DE DIJKSTRA



Representa a distância direta entre os vértices

A = Matriz de Adjacência

	x	1	2	3	4	y
x	∞	3	8	4	∞	10
1	3	∞	∞	6	∞	∞
2	8	∞	∞	∞	7	∞
3	4	6	∞	∞	1	3
4	∞	∞	7	1	∞	1
y	10	∞	∞	3	1	∞

IN = {x}

Contem os vértices onde já foram determinados os menores caminhos até estes vértices

P = vértice em análise, sempre o com menor valor em d

Menor distância entre x e os outros vértices. Inicialmente valores saem de A

	x	1	2	3	4	y
d	0	3	8	4	∞	10
s	-	x	x	x	x	x

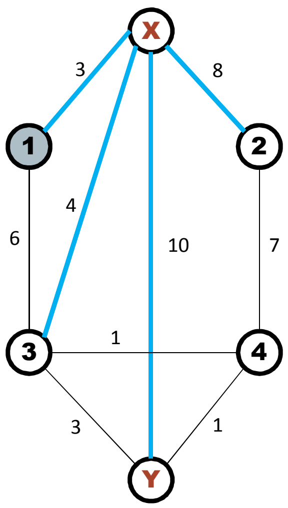
M

Contém o caminho resposta.

Módulo 2: Teoria dos Grafos

83

CAMINHO MÍNIMO – ALGORITMO DE DIJKSTRA



A = Matriz de Adjacência

	x	1	2	3	4	y
x	∞	3	8	4	∞	10
1	3	∞	∞	6	∞	∞
2	8	∞	∞	∞	7	∞
3	4	6	∞	∞	1	3
4	∞	∞	7	1	∞	1
y	10	∞	∞	3	1	∞

P=1 (pela matriz M identificamos o vértice não visitado com menor distância de X , i. e. = 3)

IN = {x, 1}

*Recalcular os valores de d[] para os vértices restantes 2,3,4 e y. Ou seja, menor distância de x a estes vértices em **d** ou seguindo por **A** **apenas pelos vértices de IN**.*

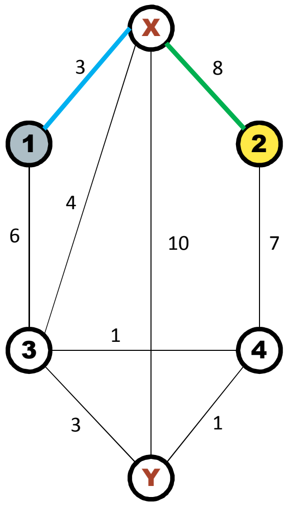
M

	x	1	2	3	4	y
d	0	3	8	4	∞	10
s	-	x	x	x	x	x

Módulo 2: Teoria dos Grafos

84

CAMINHO MÍNIMO – ALGORITMO DE DIJKSTRA



Min entre x e 2.
1º Direto (x->2)
2º Passando por 1.

A = Matriz de Adjacência

	x	1	2	3	4	y
x	∞	3	8	4	∞	10
1	3	∞	∞	6	∞	∞
2	8	∞	∞	∞	7	∞
3	4	6	∞	∞	1	3
4	∞	∞	7	1	∞	1
y	10	∞	∞	3	1	∞

P=1

IN = {x, 1}

d[2] = min(8, 3+ A[1,2]) = min(8, ∞) = 8

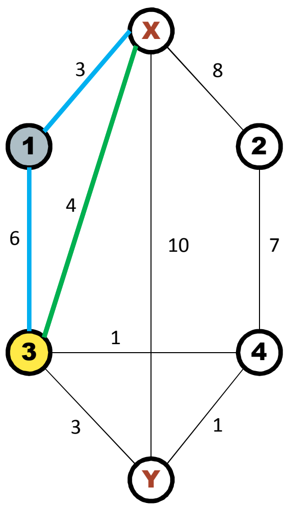
M

	x	1	2	3	4	y
d	0	3	8	4	∞	10
S	-	x	x	x	x	x

Módulo 2: Teoria dos Grafos

85

CAMINHO MÍNIMO – ALGORITMO DE DIJKSTRA



A = Matriz de Adjacência

	x	1	2	3	4	y
x	∞	3	8	4	∞	10
1	3	∞	∞	6	∞	∞
2	8	∞	∞	∞	7	∞
3	4	6	∞	∞	1	3
4	∞	∞	7	1	∞	1
y	10	∞	∞	3	1	∞

P=1

IN = {x, 1}

d[2] = min(8, 3+ A[1,2]) = min(8, ∞) = 8
d[3] = min(4, 3+ A[1,3] = min(4,9) = 4

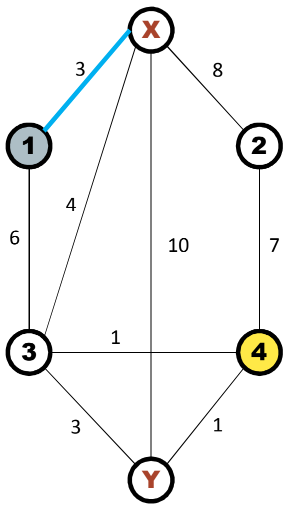
M

	x	1	2	3	4	y
d	0	3	8	4	∞	10
S	-	x	x	x	x	x

Módulo 2: Teoria dos Grafos

86

CAMINHO MÍNIMO – ALGORITMO DE DIJKSTRA



A = Matriz de Adjacência

	x	1	2	3	4	y
x	∞	3	8	4	∞	10
1	3	∞	∞	6	∞	∞
2	8	∞	∞	∞	7	∞
3	4	6	∞	∞	1	3
4	∞	∞	7	1	∞	1
y	10	∞	∞	3	1	∞

P=1

IN = {x, 1}

d[2] = min(8, 3+ A[1,2]) = min(8, ∞) = 8
d[3] = min(4, 3+ A[1,3] = min(4,9) = 4
d[4] = min(∞, 3 + A[1,4]) = min (∞, ∞) = ∞

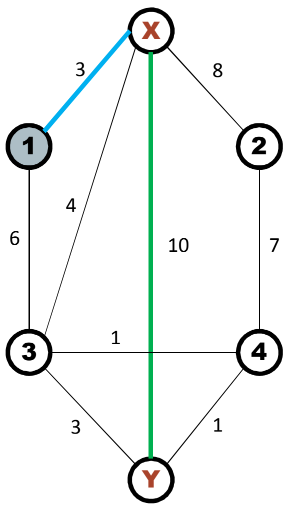
M

	x	1	2	3	4	y
d	0	3	8	4	∞	10
S	-	x	x	x	x	x

Módulo 2: Teoria dos Grafos

87

CAMINHO MÍNIMO – ALGORITMO DE DIJKSTRA



A = Matriz de Adjacência

	x	1	2	3	4	y
x	∞	3	8	4	∞	10
1	3	∞	∞	6	∞	∞
2	8	∞	∞	∞	7	∞
3	4	6	∞	∞	1	3
4	∞	∞	7	1	∞	1
y	10	∞	∞	3	1	∞

P=1

IN = {x, 1}

d[2] = min(8, 3+ A[1,2]) = min(8, ∞) = 8
d[3] = min(4, 3+ A[1,3] = min(4,9) = 4
d[4] = min(∞, 3 + A[1,4]) = min (∞, ∞) = ∞
d[y] = min(10, 3+ A[1,y]) = min(10, ∞) = 10

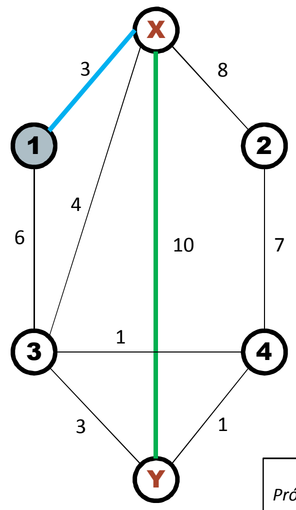
M

	x	1	2	3	4	y
d	0	3	8	4	∞	10
S	-	x	x	x	x	x

Módulo 2: Teoria dos Grafos

88

CAMINHO MÍNIMO – ALGORITMO DE DIJKSTRA



Não há alterações nos valores de d, logo não alteramos S. Isso significa que não existe nenhum caminho a partir de x, passando por 1, que seja menor do que ir diretamente aos vértices que não estão em IN.

A = Matriz de Adjacência

	x	1	2	3	4	y
x	∞	3	8	4	∞	10
1	3	∞	∞	6	∞	∞
2	8	∞	∞	∞	7	∞
3	4	6	∞	∞	1	3
4	∞	∞	7	1	∞	1
y	10	∞	∞	3	1	∞

P=1

IN = {x, 1}

d[2] = min(8, 3+ A[1,2]) = min(8, ∞) = 8

d[3] = min(4, 3+ A[1,3] = min(4,9) = 4

d[4] = min(∞, 3 + A[1,4]) = min (∞, ∞) = ∞

d[y] = min(10, 3+ A[1,y]) = min(10, ∞) = 10

Próximo p, pois tem a menor distancia.

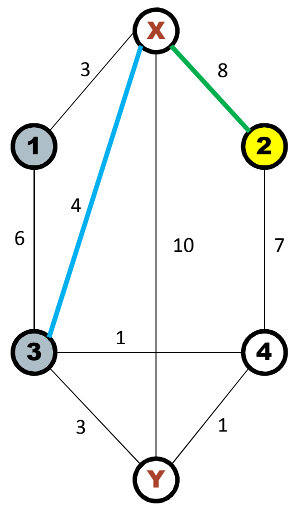
M

	x	1	2	3	4	y
d	0	3	8	4	∞	10
S	-	x	x	x	x	x

Módulo 2: Teoria dos Grafos

89

CAMINHO MÍNIMO – ALGORITMO DE DIJKSTRA



A = Matriz de Adjacência

	x	1	2	3	4	y
x	∞	3	8	4	∞	10
1	3	∞	∞	6	∞	∞
2	8	∞	∞	∞	7	∞
3	4	6	∞	∞	1	3
4	∞	∞	7	1	∞	1
y	10	∞	∞	3	1	∞

P=3 (pois possui menor d em M)

IN = {x, 1,3}

d[2] = min(8, 4+ ∞) = 8

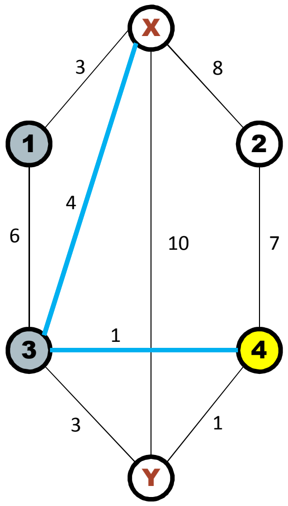
M

	x	1	2	3	4	y
d	0	3	8	4	∞	10
S	-	x	x	x	x	x

Módulo 2: Teoria dos Grafos

90

CAMINHO MÍNIMO – ALGORITMO DE DIJKSTRA



A = Matriz de Adjacência

	x	1	2	3	4	y
x	∞	3	8	4	∞	10
1	3	∞	∞	6	∞	∞
2	8	∞	∞	∞	7	∞
3	4	6	∞	∞	1	3
4	∞	∞	7	1	∞	1
y	10	∞	∞	3	1	∞

P=3

IN = {x, 1,3}

d[2] = min(8, 4+ ∞) = 8

d[4] = min(∞, 4+1) = 5 (alterou!)

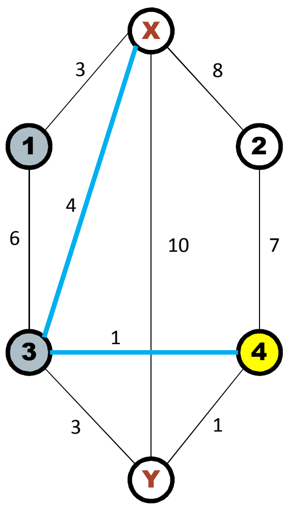
M

	x	1	2	3	4	y
d	0	3	8	4	∞	10
S	-	x	x	x	x	x

Módulo 2: Teoria dos Grafos

91

CAMINHO MÍNIMO – ALGORITMO DE DIJKSTRA



A = Matriz de Adjacência

	x	1	2	3	4	y
x	∞	3	8	4	∞	10
1	3	∞	∞	6	∞	∞
2	8	∞	∞	∞	7	∞
3	4	6	∞	∞	1	3
4	∞	∞	7	1	∞	1
y	10	∞	∞	3	1	∞

P=3

IN = {x, 1,3}

d[2] = min(8, 4+ ∞) = 8

d[4] = min(∞, 4+1) = 5 (alterou!)

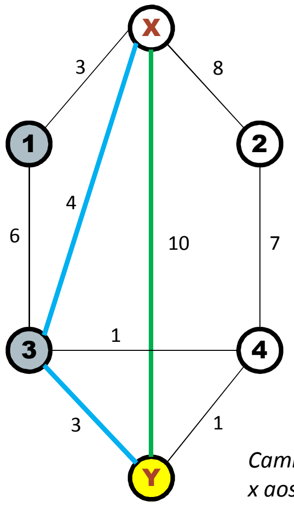
M

	x	1	2	3	4	y
d	0	3	8	4	5	10
S	-	x	x	x	3	x

Módulo 2: Teoria dos Grafos

92

CAMINHO MÍNIMO – ALGORITMO DE DIJKSTRA



A = Matriz de Adjacência

	x	1	2	3	4	y
x	∞	3	8	4	∞	10
1	3	∞	∞	6	∞	∞
2	8	∞	∞	∞	7	∞
3	4	6	∞	∞	1	3
4	∞	∞	7	1	∞	1
y	10	∞	∞	3	1	∞

P=3

IN = {x, 1,3}

d[2] = min(8, 4+ ∞) = 8
d[4] = min(∞, 4+1) = 5
d[y] = min(10, 4+3) = 7 (alterou!)

Caminhos menores de x aos vértices 4 e y foram encontrados passando por 3

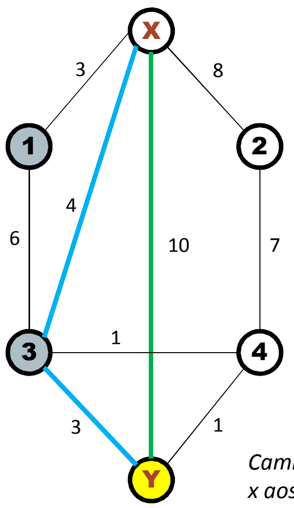
M

	x	1	2	3	4	y
d	0	3	8	4	5	10
s	-	x	x	x	3	x

Módulo 2: Teoria dos Grafos

93

CAMINHO MÍNIMO – ALGORITMO DE DIJKSTRA



A = Matriz de Adjacência

	x	1	2	3	4	y
x	∞	3	8	4	∞	10
1	3	∞	∞	6	∞	∞
2	8	∞	∞	∞	7	∞
3	4	6	∞	∞	1	3
4	∞	∞	7	1	∞	1
y	10	∞	∞	3	1	∞

P=3

IN = {x, 1,3}

d[2] = min(8, 4+ ∞) = 8
d[4] = min(∞, 4+1) = 5
d[y] = min(10, 4+3) = 7 (alterou!)

Caminhos menores de x aos vértices 4 e y foram encontrados passando por 3

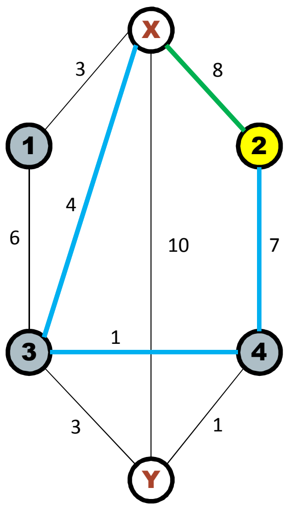
M

	x	1	2	3	4	y
d	0	3	8	4	5	7
s	-	x	x	x	3	3

Módulo 2: Teoria dos Grafos

94

CAMINHO MÍNIMO – ALGORITMO DE DIJKSTRA



A = Matriz de Adjacência

	x	1	2	3	4	y
x	∞	3	8	4	∞	10
1	3	∞	∞	6	∞	∞
2	8	∞	∞	∞	7	∞
3	4	6	∞	∞	1	3
4	∞	∞	7	1	∞	1
y	10	∞	∞	3	1	∞

P=4 (pois possui menor d em M)

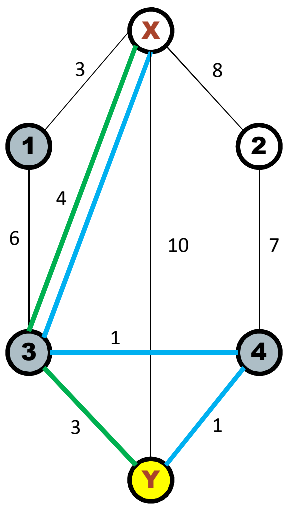
IN = {x, 1,3,4}

d[2] = min(8, 5+7) = 8

M

	x	1	2	3	4	y
d	0	3	8	4	5	7
S	-	x	x	x	3	3

CAMINHO MÍNIMO – ALGORITMO DE DIJKSTRA



A = Matriz de Adjacência

	x	1	2	3	4	y
x	∞	3	8	4	∞	10
1	3	∞	∞	6	∞	∞
2	8	∞	∞	∞	7	∞
3	4	6	∞	∞	1	3
4	∞	∞	7	1	∞	1
y	10	∞	∞	3	1	∞

P=4

IN = {x, 1,3,4}

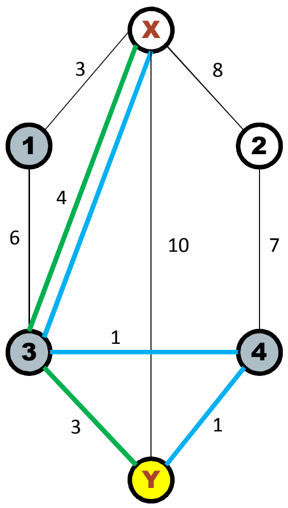
d[2] = min(8, 5+7) = 8

d[y] = min(7, 5+1) = 6 (alterou!)

M

	x	1	2	3	4	y
d	0	3	8	4	5	7
S	-	x	x	x	3	3

CAMINHO MÍNIMO – ALGORITMO DE DIJKSTRA



A = Matriz de Adjacência

	x	1	2	3	4	y
x	∞	3	8	4	∞	10
1	3	∞	∞	6	∞	∞
2	8	∞	∞	∞	7	∞
3	4	6	∞	∞	1	3
4	∞	∞	7	1	∞	1
y	10	∞	∞	3	1	∞

P=4

IN = {x, 1,3,4}

d[2] = min(8, 5+7) = 8

d[y] = min(7, 5+1) = 6 (alterou!)

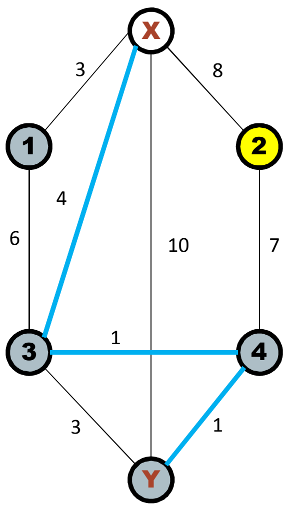
M

	x	1	2	3	4	y
d	0	3	8	4	5	6
S	-	x	x	x	3	4

Módulo 2: Teoria dos Grafos

97

CAMINHO MÍNIMO – ALGORITMO DE DIJKSTRA



A = Matriz de Adjacência

	x	1	2	3	4	y
x	∞	3	8	4	∞	10
1	3	∞	∞	6	∞	∞
2	8	∞	∞	∞	7	∞
3	4	6	∞	∞	1	3
4	∞	∞	7	1	∞	1
y	10	∞	∞	3	1	∞

P=Y (pois possui menor d em M)

IN = {x, 1,3,4, Y}

Termina, pois Y (destino) pertence à IN.

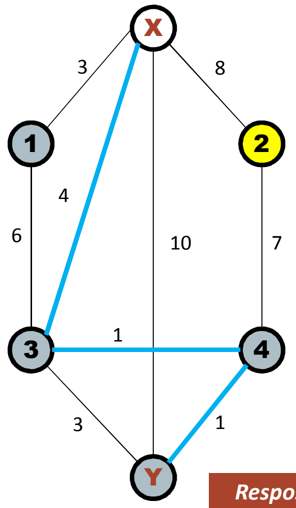
M

	x	1	2	3	4	y
d	0	3	8	4	5	6
S	-	x	x	x	3	4

Módulo 2: Teoria dos Grafos

98

CAMINHO MÍNIMO – ALGORITMO DE DIJKSTRA



A = Matriz de Adjacência

	x	1	2	3	4	y
x	∞	3	8	4	∞	10
1	3	∞	∞	6	∞	∞
2	8	∞	∞	∞	7	∞
3	4	6	∞	∞	1	3
4	∞	∞	7	1	∞	1
y	10	∞	∞	3	1	∞

P=Y (pois possui menor d em M)

IN = {x, 1,3,4, Y}

Termina, pois Y (destino) pertence à IN.

Resposta = X → 3 → 4 → Y
(o algoritmo retorna ao contrário)

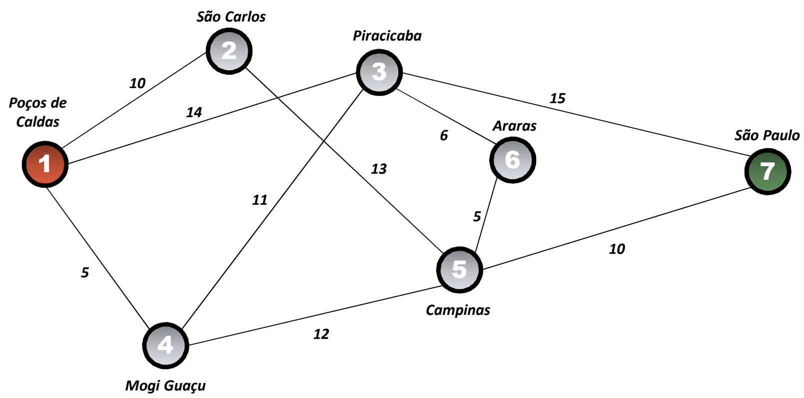
	x	1	2	3	4	y
d	0	3	8	4	5	6
s	-	x	x	x	3	4

Módulo 2: Teoria dos Grafos

99

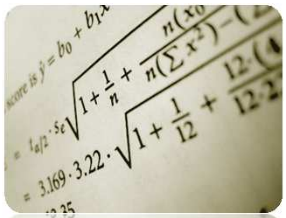
Exercícios

1) *Aplique o algoritmo de Dijkstra para encontrar o menor caminho em (A,F) no grafo abaixo:*



Módulo 2: Teoria dos Grafos

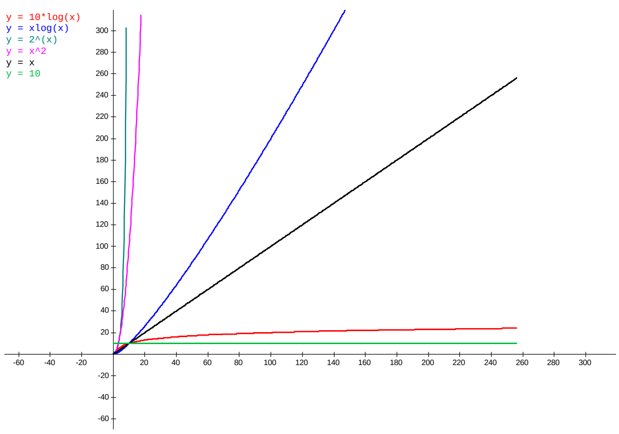
100



MÓDULO 3: TEORIA DOS NÚMEROS

TEORIA DOS NÚMEROS

A Teoria dos Números possui diversas aplicações na Ciência da Computação, entre elas se destacam: análise de programas (PAA), verificação de relações de recorrência, prova de teoremas, criptografia de dados, etc.



INDUÇÃO MATEMÁTICA

A Indução Matemática é uma técnica usada para demonstrar propriedades de números inteiros positivos (em qualquer domínio de aplicação).

Por exemplo, considere o que segue abaixo:

$2^0 = 1 = 2^1 - 1$

$2^0 + 2^1 = 1 + 2 = 3 = 2^2 - 1$

$2^0 + 2^1 + 2^2 = 1 + 2 + 4 = 7 = 2^3 - 1$

$2^0 + 2^1 + 2^2 + 2^3 = 1 + 2 + 4 + 8 = 15 = 2^4 - 1$

$$\mathbf{2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1}$$

SERÁ?

No entanto, não se pode afirmar que este padrão será sempre verdadeiro para todos os valores de *n* a menos que provemos.

Para provar que alguma coisa é verdadeira para todo inteiro n ≥ que algum valor, **pense em indução**.

MÓDULO 3: TEORIA DOS NÚMEROS

103

ELEMENTO MÍNIMO DE UM CONJUNTO DE INTEIROS

Seja A um conjunto de números inteiros. Chama-se elemento mínimo de A um elemento $a \in A$ tal que $a \leq x$ para todo $x \in A$.

$$\mathbf{minA = a \Leftrightarrow (a \in A \text{ e } \forall x \in A, a \leq x)}$$

Teorema: Se a é elemento mínimo de A, então este elemento é único.

Exemplos:

a) $N^* = \{1, 2, 3, \ldots\}$ $\quad minN^* = 1$

b) $Z^- = \{0, -1, -2, -3, \ldots\}$ $\quad$ não existe mínimo.

MÓDULO 3: TEORIA DOS NÚMEROS

104

Princípio da Boa Ordenação (P. B. O.)

Teorema: Todo conjunto não vazio A de inteiros não negativos possui o elemento mínimo.

Em outras palavras, todo subconjunto não vazio do conjunto:

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

possui o elemento mínimo.

Simbolicamente:

$$\forall A \subset Z+, A \neq \varnothing \Rightarrow \exists \min A$$

Exemplos:

a) $A = \{1, 3, 5, 7, ...\}$
$A \neq \varnothing$ e $A \subset Z+ \Rightarrow \exists \min A = 1$

b) $P = \{2, 3, 5, 7, 11, ...\}$
$P \neq \varnothing$ e $P \subset Z+ \Rightarrow \exists \min P = 2$

PRINCÍPIO DE INDUÇÃO FINITA

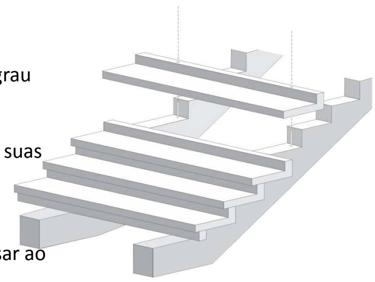
Seja S um subconjunto de N* que satisfaça as duas seguintes condições:

1. 1 pertence a S ($1 \in S$);
2. para todo inteiro positivo k, se $k \in S$, então $k + 1 \in S$.

Nestas condições e utilizando o P.B.O., conclui-se que S é o conjunto N* (S = N*).

Ilustração do Princípio de Indução Finita

Imagine que você está subindo em uma escada sem fim. Como você pode saber se será capaz de alcançar um degrau arbitrariamente alto?



Suponha que você faça as seguintes afirmações sobre as suas habilidades de subir escadas:

1. Você pode alcançar o primeiro degrau;
2. Se você alcançar um degrau, você pode sempre passar ao degrau seguinte (note que isso é uma implicação);

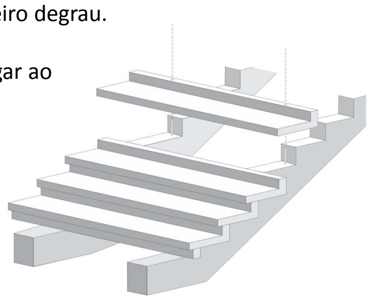
... Ilustração do Princípio de Indução Finita

Tanto (1) como (2) são sentenças verdadeiras; então pela sentença (1) você pode chegar ao primeiro degrau e pela sentença (2) você pode chegar ao segundo; novamente pela (2) você pode chegar ao terceiro; pela sentença (2) novamente você pode chegar ao quarto degrau, e assim sucessivamente. Você pode então subir tão alto quanto você queira.

Neste caso, ambas as sentenças (1) e (2) são necessárias.

Se apenas a (1) é verdadeira, você não sai do primeiro degrau.

Se apenas a (2) é verdadeira, você poderá não chegar ao primeiro degrau a fim de iniciar o processo de subida da escada.



MATEMATICAMENTE ....

Vamos considerar agora que os degraus da escada são números inteiros positivos 1, 2, 3, ...
Considere também uma propriedade específica que um número pode ter. Ao invés de "alcançar um degrau arbitrário" podemos mencionar que um inteiro positivo tem essa propriedade.

Usaremos a notação P(n) para indicar que o inteiro positivo n tem a propriedade P. Como podemos usar a técnica de subir escadas para provar que para todos inteiros positivos n nós temos P(n)?

As duas afirmações que precisamos para demonstração são:

1. P(1) (1 tem a propriedade P)

2. $P(k) \Rightarrow P(k + 1), \forall k$ (se algum número tem a propriedade P, então o número seguinte também a tem)

Se pudermos demonstrar (1) e (2) , então P(n) vale para qualquer inteiro positivo n, da mesma maneira que podemos subir até um degrau arbitrário na escada.

Teorema de Indução Matemática (T.I.M.)

(1) P(1) verdadeira
(2) $\forall$ k, P(k) $\Rightarrow$ P(k + 1) verdadeira
} $\Rightarrow$ P(n) é verdadeira p/ $\forall$ n $\in$ Z

Indução Matemática para Verificação de Programas

Considere a função recursiva abaixo:

```
function funcao(n,p)
    begin
      if n=0 then p
      else funcao(n-1, n*p);
    end
```

Sua execução gera:

funcao(n,p) = n(n-1)(n-2)...1*p
= n!*p

(p é uma constante qualquer)

Como provar que *$\forall n \geq 0$, funcao(n,p) = n!*p* ?

INDUÇÃO MATEMÁTICA

Usando indução matemática:

(1) P(1) verdadeira
(2) $\forall$ k, P(k) $\Rightarrow$ P(k + 1) verdadeira
} $\Rightarrow$ P(n) é verdadeira p/ $\forall$ n $\in$ Z

```
function funcao(n,p)
    begin
      if n=0 then p
      else funcao(n-1, n*p);
    end
```

(1) P(0) = p (trivial!)

P(k) = k! * p (n=k, Hipótese)

(2) P(k + 1) = (k+1)! * p (n=k+1, Tese)

Demonstração da tese:

funcao(k+1,p) = funcao(k, ((k+1)*p)) (chamada recursão)
= k! * ((k+1)*p) (uso da hipótese)
= (k! * (k+1)) * p (associatividade)
= (k+1)! * p (definição de n!)

Para P(k), todo este termo = p

MÓDULO 3: TEORIA DOS NÚMEROS

Exercícios

1) Aplique o Teorema de Indução Matemática para demonstrar as proposições abaixo:

$a-)1+2+2^2+...+2^n=2^{n+1}-1, \forall n \geq 1.$

$b-)1+2+3+...+n=\dfrac{n(n+1)}{2}, \forall n > 0.$

$c-)n^2 > 3n, \forall n \geq 4.$

$d-)2^{n+1} < 3^n, \forall n > 1.$

Afinal, a série mostrada no início deste módulo, é verdadeira?
$2^0 + 2^1 + 2^2 + ... + 2^n = 2^{n+1} - 1$

2-) Considere a função abaixo:

```
function facit(n)
begin
  if n=0 then 1
  else n*facit(n-1);
end
```

Prove usando indução matemática que: $\forall n \geq 0$, facit(n) = n!

DIVISIBILIDADE

Considerando a, b e c números inteiros, dizemos que

a divide c ou que **c é divisível por a**

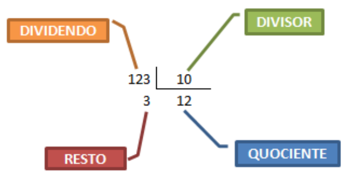
quando se tem a igualdade: **c = a.b**.

Notação: a | c (a divide c).

Propriedades:

(1) a|0, 1|a e a|a;
(2) Se a|1, então a = 1 ou a = -1;
(3) Se a|b e se c|d, então ac|bd;
(4) Se a|b e se b|c, então a|c;
(5) Se a|b e se b|a, então a = b ou a = -b;

"Dividir" neste contexto significa ter resto zero, pois c = a.b + r onde r é o resto.
Ex.: 6 = 2.3+0
Lembre-se:



ALGORITMO DA DIVISÃO

Se a e b são dois inteiros, com b > 0, então existem e são únicos os inteiros q e r que satisfazem às condições:

$$\boxed{a = bq + r \quad e \quad 0 \leq r \leq b}$$

Obviamente r = 0 quando a é múltiplo de b.

Exemplo:
a = 60 e b = 7 => 60 = 7.8 + 4, onde q = 8 e r = 4.

PARIDADE DE UM INTEIRO

Na divisão de um inteiro qualquer **a** por **b**=2, os possíveis restos são r = 0 e r = 1.

Se r = 0, então a = 2.q e é denominado **par**.

Se r = 1, então a = 2.q +1 e é denominado **ímpar**

Exercícios

3) Mostrar que, se a | (2x - 3y) e se a | (4x - 5y), então a | y.

4) Demonstrar:

a) se a é um inteiro ímpar, então 4 | a (a^2 - 1);

b) se a e b são inteiros ímpares, então 4 | (a^2 - b^2).

5) Na divisão de dois inteiros positivos o quociente é 16 e o resto é o maior possível. Achar os dois inteiros, sabendo que a soma dos dois é 341.

6) Verificar (e provar quando verdadeiro):

a) A soma de dois pares é par;

b) O produto de dois pares é par;

c) A soma de dois ímpares é par;

d) O produto de dois ímpares é ímpar;

e) A soma de um par com um ímpar é ímpar;

f) O produto de um par com um ímpar é par.

MÁXIMO DIVISOR COMUM (MDC)

Sejam a e b dois inteiros não conjuntamente nulos ($a \neq 0$ e $b \neq 0$). Chama-se máximo divisor comum de a e b o inteiro positivo **d** ($d > 0$) que satisfaz as condições:

(1) $d \mid a$ e $d \mid b$;

(2) se $c \mid a$ e se $c \mid b$, então $c \leq d$.

Nota-se que, pela condição (1), d é divisor comum de a e b, e pela condição (2), d é o maior dentre todos os divisores comuns de a e b.

Notação: mdc (a,b) = máximo divisor comum de a e b.

Propriedades:

(a) mdc (a,b) = mdc (b,a);

(b) mdc(a,1) =1;

(c) mdc(0,0) não existe;

(d) se $a \neq 0$, então mdc(a,0) = $|a|$;

(e) se $a \mid b$, então o mdc(a,b) = $|a|$.

MDC pelo Algoritmo de Euclides

"Para se achar o MDC de dois inteiros positivos divide-se o maior pelo menor, este pelo primeiro resto obtido, o segundo resto pelo primeiro, e assim sucessivamente até se obter um resto nulo. O último resto não nulo é o máximo divisor comum procurado."

	q1	q2	q3	...	qn	qn+1
a	b	r1	r2	...	rn-1	rn
r1	r2	r3	r4	...	0	

a = bq1 + r1

$$\begin{array}{l|l} a & b \\ \cline{2-2} r1 & q1 \end{array}$$

MDC pelo Algoritmo de Euclides

"Para se achar o MDC de dois inteiros positivos divide-se o maior pelo menor, este pelo primeiro resto obtido, o segundo resto pelo primeiro, e assim sucessivamente até se obter um resto nulo. O último resto não nulo é o máximo divisor comum procurado."

	q1	q2	q3	...	qn	qn+1
a	b	r1	r2	...	rn-1	rn
r1	r2	r3	r4	...	0	

a = bq1 + r1   b = r1q2 + r2

$\begin{array}{l|l} a & b \\ \hline r1 & q1 \end{array}$ $\begin{array}{l|l} b & r1 \\ \hline r2 & q2 \end{array}$

MDC pelo Algoritmo de Euclides

"Para se achar o MDC de dois inteiros positivos divide-se o maior pelo menor, este pelo primeiro resto obtido, o segundo resto pelo primeiro, e assim sucessivamente até se obter um resto nulo. **O último resto não nulo é o máximo divisor comum procurado**."

	q1	q2	q3	...	qn	qn+1
a	b	r1	r2	...	rn-1	rn
r1	r2	r3	r4	...	0	

a = bq1 + r1   b = r1q2 + r2   r1 = r2q3 + r3

$\begin{array}{l|l} a & b \\ \hline r1 & q1 \end{array}$ $\begin{array}{l|l} b & r1 \\ \hline r2 & q2 \end{array}$ $\begin{array}{l|l} r1 & r2 \\ \hline r3 & q3 \end{array}$

MDC pelo Algoritmo de Euclides

"Para se achar o MDC de dois inteiros positivos divide-se o maior pelo menor, este pelo primeiro resto obtido, o segundo resto pelo primeiro, e assim sucessivamente até se obter um resto nulo. **O último resto não nulo é o máximo divisor comum procurado**."

	q1	q2	q3	...	qn	qn+1
a	b	r1	r2	...	rn-1	rn
r1	r2	r3	r4	...	0	

a = bq1 + r1   b = r1q2 + r2   r1 = r2q3 + r3

a	b	b	r1	r1	r2	r_n	r_{n+1}
r1	q1	r2	q2	r3	q3	0	q_{n+1}

MDC

MDC pelo Algoritmo de Euclides

Exemplo: mdc(963, 657) = ?

	1				
963	657				
306					

963	657
306	1

MDC pelo Algoritmo de Euclides

Exemplo: mdc(963, 657) = ?

	1	2			
963	657	306			
306	45				

963	657		657	306
306	1		45	2

MDC pelo Algoritmo de Euclides

Exemplo: mdc(963, 657) = ?

	1	2	6		
963	657	306	45		
306	45	36			

963	657		657	306		306	45
306	1		45	2		36	6

MÓDULO 3: TEORIA DOS NÚMEROS

MDC pelo Algoritmo de Euclides

Exemplo: mdc(963, 657) = ?

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

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

MDC pelo Algoritmo de Euclides

Exemplo: mdc(963, 657) = ?

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

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

MÓDULO 3: TEORIA DOS NÚMEROS

MDC pelo Algoritmo de Euclides

Exemplo: mdc(963, 657) = 9

	1	2	6	1	4
963	657	306	45	36	9
306	45	36	$\boxed{9}$	0	

963 | 657   657 | 306   306 | 45   45 | 36   36 | 9

306   1   45   2   36   6   9   1   0   4

Resto zero. Penúltimo resto é o MDC.

mdc(963, 657) = 9

Exercícios

7) Ache, utilizando o algoritmo de Euclides, o ***mdc*** entre:

a) mdc(252,105)

b) mdc(82,46)

8) O mdc de dois inteiros positivos a e b é 8 e na sua determinação pelo algoritmo de Euclides os quocientes sucessivamente obtidos foram 2, 1, 1 e 4. Calcular a e b.

NÚMEROS PRIMOS E COMPOSTOS

Diz-se que um inteiro positivo $p > 1$ é um número **primo** se e somente se 1 e p são os seus únicos divisores. Um número $p > 1$ que não é primo é chamado de **composto**.

Exemplos: 2, 3, 5 e 7 são primos e 4, 6, 8 e 10 são compostos

Observações:

(1) O inteiro 1 não é nem primo nem composto;

(2) O número 2 é o único inteiro positivo par que é primo.

TEOREMA FUNDAMENTAL DA ARITMÉTICA

"Todo inteiro positivo n > 1 é igual a um produto de fatores primos."

Exemplo: 360 = 2.2.2.3.3.5

Decomposição Canônica:

Todo inteiro positivo $n > 1$ admite uma única decomposição da forma:

$$n = p^{k1}.q^{k2}....r^{kr}$$

onde, cada k_i é um inteiro positivo e p,q, ..., r são primos, com $p < q < ...<r$, denominada decomposição canônica do inteiro positivo n.

Exemplo: $360 = 2^3.3^2.5$

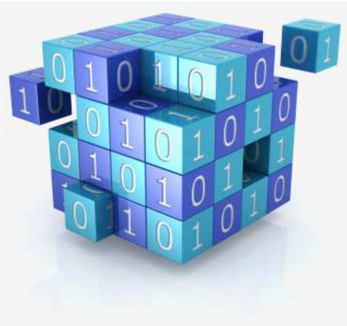
MÓDULO 3: TEORIA DOS NÚMEROS

Números primos e Criptografia de dados

Algoritmo RSA (Rivest, Chamir e Adleman) é um dos algoritmos de chave criptográfica mais utilizados.

Seu funcionamento consiste na multiplicação de 2 números primos *MUITO grandes* para a geração de um terceiro número.

Para quebrar essa criptografia, seria necessário a fatoração (decomposição) desse número para encontrar os 2 números primos que o geraram, porém, para isso é necessário um poder muito alto de processamento, o que acaba inviabilizando a tarefa.



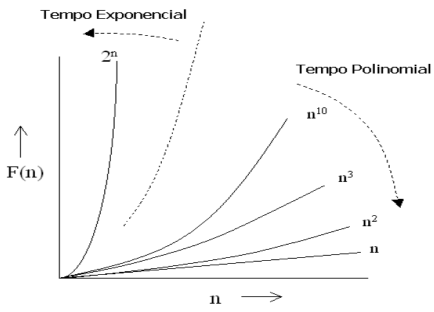
MÓDULO 3: TEORIA DOS NÚMEROS

Primalidade e Fatoração

Algumas pessoas confundem o problema de fatoração com o problema de verificar se o número é primo ou não.

O problema de fatoração (decomposição) é: dado um inteiro N, tente achar os números primos que quando multiplicados dão N.

A primalidade é a constatação de que determinado número é primo.



MÓDULO 3: TEORIA DOS NÚMEROS

ARITMÉTICA MODULAR - CONGRUÊNCIAS

Uma **congruência** é a relação entre dois números que, divididos por um terceiro - chamado *módulo de congruência* - deixam o mesmo resto.

Exemplo: 9 é congruente ao 2, módulo 7, pois ambos deixam resto 2, ao serem divididos por 7.

Definição Formal: Sejam a e b dois inteiros quaisquer e seja m um inteiro positivo fixo. Diz-se que **a é congruente a b módulo m** se e somente se m divide a diferença a – b. Ou seja, m | a – b.
(pois: a = mk+r e b=mk´+r, subtraindo um lado pelo outro temos m | a-b que é igual a a-b = m(k-k´) com resto zero)
Em outros termos, a é congruente a b módulo m se e somente se existe um inteiro k tal que a-b = m*k.

Notação: $a \equiv b \pmod{m}$ => a é congruente a b módulo m

$a \equiv b \pmod{m} \Leftrightarrow m \mid (a-b)$

Exemplos:
$3 \equiv 24 \pmod{7}$, porque $7 \mid (3 - 24)$
$-31 \equiv 11 \pmod{6}$, porque $6 \mid (-31 - 11)$

MÓDULO 3: TEORIA DOS NÚMEROS

ARITMÉTICA MODULAR - CONGRUÊNCIAS

Propriedades:

(a) a ≡ a (mod. m)

(b) a ≡ b (mod. m) => b ≡ a (mod. m)

(c) a ≡ b (mod. m) e b ≡ c (mod. m) => a ≡ c (mod. m)

(d) a ≡ b (mod. m) e c ≡ d (mod. m) => a + c ≡ b +d (mod. m)

(e) a ≡ b (mod. m) => ac ≡ bc (mod. m)

ARITMÉTICA MODULAR - CONGRUÊNCIAS

Aplicações de congruência e aritmética modular

Aritmética do Relógio

Trata-se de um caso de congruência módulo 12. Note que 13 horas é congruente a 1 hora, no módulo 12. Ambos divididos por 12, deixam resto 1. 17 horas é congruente a 5 horas, módulo 12. Tanto 17, como 5, divididos por 12, deixam resto 5...e assim, sucessivamente.

(Tem que achar legal senão eu fico chateado... – Fala aí, ahhh que legal!)

MÓDULO 3: TEORIA DOS NÚMEROS

Exercícios

8) Escrever cada inteiro abaixo como um produto de números primos:

a) 5040 b) 480 c) 560 d) 980

9) Verificar a validade (V ou F):

a) $91 \equiv 0 \pmod 7$ b) $-2 \equiv 2 \pmod 8$

c) $17 \equiv 9 \pmod 2$ d) $3 + 5 + 7 \equiv 5 \pmod{10}$

e) $112 \equiv 1 \pmod 3$ f) $42 \equiv 8 \pmod{10}$

ARITMÉTICA MODULAR - CONGRUÊNCIAS

Aplicações de congruência e aritmética modular

Número do CPF

11 dígitos, primeiro bloco com 9 algarismos e um segundo com mais 2 dígitos de controle .

O décimo dígito (que é o primeiro dígito de controle) é o resultado de uma congruência, **módulo 11** de um número obtido por uma operação dos primeiros nove algarismos.

Qual operação?

Se a1 a2 a3 a4 a5 a6 a7 a8 a9 é a sequência formada pelos 9 primeiros dígitos, devemos multiplicá-los, nessa ordem, por {1, 2, 3, 4, 5, 6, 7, 8, 9} e somar os produtos obtidos. Esta soma, dividida por 11 gerará como resto o primeiro dígito de controle.

A determinação do segundo dígito de controle é feita de modo similar, sendo que agora acrescenta-se o décimo dígito e utiliza-se uma base de multiplicação de 0 a 9.

ARITMÉTICA MODULAR - CONGRUÊNCIAS

Exemplo: CPF 235 343 104 – XY
O primeiro dígito de controle será obtido da seguinte maneira:

CPF 2 3 5 3 4 3 1 0 4 X Y
1 2 3 4 5 6 7 8 9

2 x 1 + 3 x 2 + 5 x 3 + 3 x 4 + 4 x 5 + 3 x 6 + 1 x 7 + 0 x 8 + 4 x 9 = 116

$$\begin{array}{r|l} 116 & 11 \\ \hline 6 & 10 \end{array}$$

X = 6

CPF 2 3 5 3 4 3 1 0 4 6 Y
0 1 2 3 4 5 6 7 8 9

2 x 0 + 3 x 1 + 5 x 2 + 3 x 3 + 4 x 4 + 3 x 5 + 1 x 6 + 0 x 7 + 4 x 8 + 6 x 9 = 145

$$\begin{array}{r|l} 145 & 11 \\ \hline 2 & 13 \end{array}$$

Y = 2

CPF 235343104 - 62

MÓDULO 3: TEORIA DOS NÚMEROS

ARITMÉTICA MODULAR - CONGRUÊNCIAS

Aplicações de congruência e aritmética modular

Gerador de Números Pseudo-aleatórios

Na maioria das linguagens de programação existe uma função predefinida geradora de números aleatórios (geralmente chamada de *rand() ou random()).* A geração de números aleatórios é muito útil em simulações computacionais. Diversos métodos têm sido criados para gerar uma sequência de números aleatórios. Em rigor, nenhum destes métodos gera números perfeitamente aleatórios, por isso é habitual chamá-los de números ***pseudo-aleatórios***.

O método mais comum é o chamado **Método das Congruências Lineares**. Escolhe-se quatro inteiros: o módulo **m**, o multiplicador **a**, o incremento **c** e a semente x_0, com $2 \le a < m$, $0 \le c < m$ e $0 \le x_0 < m$. Gera-se uma sequência de números pseudo-aleatórios $\{x_n\}$, com $0 \le x_n < m$ para qualquer n, usando sucessivamente a relação de congruência:

$$x_{n+1} = (a.x_n + c) \bmod m$$

Na linguagem C:

```
srand(NULL(time))
ale = rand()%6 + 1      // 0 a 5 mais 1
```

MÓDULO 3: TEORIA DOS NÚMEROS

ARITMÉTICA MODULAR - CONGRUÊNCIAS

Aplicações de congruência e aritmética modular

Gerador de Números Pseudo-aleatórios

Exemplo: m = 9, a = 7,c = 4 e x_0 = 3 é a seguinte:

$x_1 = (7x_0 + 4) \bmod 9 = 25 \bmod 9 = 7$
$x_2 = (7x_1 + 4) \bmod 9 = 53 \bmod 9 = 8$
$x_3 = (7x_2 + 4) \bmod 9 = 60 \bmod 9 = 6$
$x_4 = (7x_3 + 4) \bmod 9 = 46 \bmod 9 = 1$
$x_5 = (7x_4 + 4) \bmod 9 = 11 \bmod 9 = 2$
$x_6 = (7x_5 + 4) \bmod 9 = 18 \bmod 9 = 0$
$x_7 = (7x_6 + 4) \bmod 9 = 4 \bmod 9 = 4$
$x_8 = (7x_7 + 4) \bmod 9 = 32 \bmod 9 = 5$
$x_9 = (7x_8 + 4) \bmod 9 = 39 \bmod 9 = 3$

$$x_{n+1} = (a.x_n + c) \bmod m$$

Como $x_9 = x_0$ e cada termo na sequência só depende do anterior, a sequência terá nove números diferentes antes de começar a repetir:

3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, . . .

SEQUÊNCIAS RECORRENTES

MÓDULO 3: TEORIA DOS NÚMEROS

Consideremos a sequência de inteiros:

$$U_1, U_2, U_3, \ldots, U_{n-1}, U_n, \ldots$$

Na qual cada termo, a partir do terceiro, é a soma dos dois termos precedentes, isto é, para n ≥3:

$$u_n = u_{n-1} + u_{n-2}$$

Tal sequência recebe o nome de sequência recorrente.

Exemplo: **Sequência de Fibonacci**

$f_1 = f_2 = 1$ e $f_n = f_{n-1} = f_{n-2}$ (n >= 3)

1, 1, 2, 3, 5, 8, 13, 21, ...

Exercícios

10) Determine quais são os dois dígitos de controle do número de CPF igual a 347.873.254.

11) Usando o método das congruências lineares (utilizado no exemplo de gerador de números aleatórios), determine qual será a sequência de números aleatórios usando: m = 5, a = 6,c = 3 e x_0 = 2.

12) As congruências são também muito utilizadas na criptografia de dados. O exemplo mais simples (e muito antigo, remonta a Júlio César) é a chamada **cifra de César**. Ele usava um método de escrita de mensagens secretas transladando cada letra do alfabeto para três casas mais à frente.
Utilizando o método das congruências lineares (dado no exemplo de gerador de números aleatórios) e associando cada letra do alfabeto conforme segue:

A = 0, B = 1, C = 2, D = 3, E = 4, F = 5, G = 6, H = 7, I = 8, J = 9, K = 10,
L = 11, M = 12, N = 13, O = 14, P = 15, Q = 16, R = 17, S = 18, T = 19,
U = 20, V = 21, X = 22, Y = 23, W = 24, Z = 25

Determine como ficaria criptografada a seguinte mensagem utilizando a cifra de césar.
"DESCOBRI A SOLUCAO"

13) Retomando a sequência de Fibonacci (último tópico da teoria), para qual número converge a seguinte razão?

f_{n+1}/f_n

MÓDULO 4: ANÁLISE COMBINATÓRIA

FATORIAL

*Para podermos rever o conceito de **Análise Combinatória** torna-se prudente revisarmos também o conceito sobre cálculo de expressões fatoriais.*

Dado um número inteiro positivo n > 1, definimos:

$$n! = n.(n-1).(n-2)...3.2.1$$

Nos casos particulares n = 1 e n = 0, definimos:

$$1! = 1 \text{ e } 0! = 1$$

Deve-se notar que:

0! = 1
1! = 1
2! = 2.1 = 2
3! = 3.2! = 3.2 = 6
4! = 4.3! = 4.6 = 24 , ...

DEFINIÇÃO

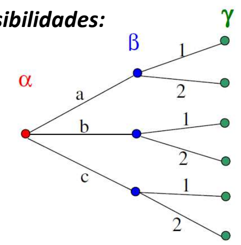
A Análise Combinatória é a parte da Matemática onde estudamos as técnicas de **contagem de agrupamentos** que podem ser feitos com elementos de um dado conjunto.

PRINCÍPIO FUNDAMENTAL DA CONTAGEM

"Se uma ação é composta de duas etapas sucessivas, sendo que a primeira pode ser feita de m modos e, para cada um destes, a segunda pode ser feita de n modos, então, o número de maneiras diferentes de realizar esta ação é **m*n**."

Exemplo: Imagine que para ir de uma cidade **α** para uma cidade **β** existam três estradas: a, b e c, e de **β** para **Υ** existam duas: 1 e 2.

Árvore de possibilidades:



Portanto, a realização das duas etapas (**α** → **β** → **Υ**) pode ser feita de 3*2 modos, que correspondem aos 6 caminhos de **α** para **Υ**.

MÓDULO 4: ANÁLISE COMBINATÓRIA

Exercícios

1-) Calcule o valor de cada expressão:

a) 6! + 5! c-) 0! - 3.1!
b) 4.5! - 6.3! d-) 6 + 6! - (4!)2

2-) Simplifique e calcule o valor de:

a) 6! / 8! b) 9! / 6! c) 14! / 12!
d) 10! / (4! 6!) e) 12! / (10! 2!) f) (5! 15!) / (13! 7!)
g) 20! / (18! 2!) h) (50! 39!) / (40! 48!)

3-) Simplifique:

a) n! / (n -1)!
b) (n + 1)! / n!
c) n! / (n -2)!
d) (n + 2)! / (n + 1)!

Exercícios

4) Calcule *n* na equação
a) n! = 12 . (n - 2)! b) n! / (2! (n - 2)!) =21

5) Glorinha deseja formar um conjunto calça-blusa para vestir-se. Se ela dispõe de 6 calças e 10 blusas para escolher, de quantos modos pode formar o conjunto ?

6) Com os algarismos 1, 2, 3, 4 e 5 quantos números naturais de três algarismos podem ser escritos ? Destes números, quantos são formados por algarismos distintos?

7) Quantas placas de licença de automóveis podem ser formadas por 3 letras e 4 algarismos sendo as letras apenas vogais e sendo os algarismos distintos ?

8) Uma sorveteria oferece uma taça de sorvete que pode vir coberto com calda de chocolate ou de morango ou de caramelo. Se o sorvete pode ser escolhido entre 10 sabores diferentes, quantas são as opções para um cliente escolher a taça com cobertura ?

PERMUTAÇÕES

Def.: *Denominamos* ***permutação*** *de n elementos a toda sucessão de n termos formada com os n elementos.*

Ela deve ser utilizada quando você quiser contar quantas possibilidades existem de se organizar um número de objetos de forma distinta.

Por exemplo:

1) Permutações dos algarismos 1, 2 e 3:
(1,2,3) (1,3,2) (2,1,3) (2,3,1) (3,2,1) (3,1,2)

2) Anagramas da palavra LIA:
LIA, LAI, ALI, AIL, IAL, ILA

O número de filas que podem ser formadas com 25 pessoas é 25.24.23. ... . 3.2.1, pois para o primeiro lugar da fila temos 25 possibilidades, para o segundo 24 e assim por diante.

Obs.: Normalmente em permutação utilizamos todos os elementos!

QUANTIDADE DE PERMUTAÇÕES

PERMUTAÇÕES DE ELEMENTOS DISTINTOS (Permutação Simples)

O número de permutações de n elementos distintos é dado por:

$$\boxed{P_n = n!}$$

Exemplo:
a) Quantas permutações podem ser formadas com as letras a, b, c, d, e:

P5 = 5! = 120

(a,b,c,d,e) (a,b,c,e,d) (a,b,e,c,d) ...

b) Quantos anagramas podemos formar com a palavra GATO?

Podemos variar as letras de lugar e formar vários anagramas, formulando um caso de permutação simples.

P = 4! = 24

QUANTIDADE DE PERMUTAÇÕES

PERMUTAÇÕES COM ELEMENTOS REPETIDOS

Quando temos n elementos dos quais n1 são repetidos de um tipo, n2 são repetidos de outro tipo, n3 são repetidos de outro tipo e assim por diante, o número de permutações que podemos formar é dado por:

$$\boxed{P_n^{n_1, n_2, n_3 ..., n_k} = \frac{n!}{n_1!n_2!n_3!...n_k!}}$$

Exemplos:

a) Quantas permutações podem ser formadas com os símbolos: +,+,+,-,x

$$P_5^3 = \frac{5!}{3!} = \frac{5.4.3!}{3!} = 20$$

b) Quantas permutações podem ser formadas com os símbolos: +,+,+,-,-,x.

$$P_5^{3,2} = \frac{6!}{3!2!} = \frac{6.5.4.3!}{3!2!} = 60$$

MÓDULO 4: ANÁLISE COMBINATÓRIA

147

ARRANJOS

Def.: *Denominamos **arranjos** de n elementos distintos tomados k a k às sucessões formadas de k termos distintos escolhidos entre os n elementos dados.*

Os arranjos serão representados colocando os elementos entre parênteses ( ).

Um **arranjo** de n elementos dispostos k a k, com k menor ou igual a n, é uma **ESCOLHA** de k entre esses n objetos na qual **a ordem IMPORTA!**

Exemplo:

a) Considerando os elementos: A, C, V, P, escrever os arranjos destes 4 elementos 2 a 2 da seguinte forma:

(A,C) , (A,V) , (A,P) , (C,V) , (C,P) , (V,P)
(C,A) , (V,A) , (P,A) , (V,C) , (P,C) , (P,V)

MÓDULO 4: ANÁLISE COMBINATÓRIA

148

QUANTIDADE DE ARRANJOS

Representamos pelo símbolo $A_{n,k}$ o número de arranjos de n elementos tomados k a k, cuja fórmula é:

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

Obs.: Existem diferentes tipos de arranjos (com repetição, condicional,...), neste curso revisaremos apenas os arranjos simples.

Dois arranjos são diferentes se tiverem elementos diferentes, ou se tiverem os mesmos elementos porém em ordem diferentes.

Exemplo 1: Seja Z={A,B,C,D}. Os arranjos simples desses 4 elementos tomados 2 a 2 são 12 grupos que não podem ter a repetição de qualquer elemento mas que podem aparecer na ordem trocada. Todos os agrupamentos estão no conjunto:

As={AB,AC,AD,BA,BC,BD,CA,CB,CD,DA,DB,DC}

Exemplo 2: Considerando os elementos: A, C, V, P. O número de arranjos dos 4 elementos tomados 2 a 2 é calculado como segue:

$$A_{4,2} = \frac{4!}{(4-2)!} = \frac{4!}{2!} = \frac{4.3.2!}{2!} = 12$$

MÓDULO 4: ANÁLISE COMBINATÓRIA

149

COMBINAÇÕES

Def.: *Denominamos **combinações** de n elementos distintos tomados k a k aos conjuntos formados de k termos distintos escolhidos entre os n elementos dados.*

As combinações serão representadas colocando os elementos entre chaves { }.

Duas combinações são diferentes apenas quando têm elementos diferentes. Aqui NÃO IMPORTA a ordem em que os elementos são colocados.

Exemplo 1: Considerando os elementos: A, C, V, P, escreve-se as combinações destes 4 elementos 2 a 2 da seguinte forma:

{A,C} , {A,V} , {A,P} , {C,V} , {C,P} , {V,P}

Exemplo 2: Seja C={A,B,C,D}, m=4 e p=2. As combinações simples desses 4 elementos tomados 2 a 2 são 6 grupos que não podem ter a repetição de qualquer elemento nem podem aparecer na ordem trocada. Todos os agrupamentos estão no conjunto:

C_s={AB,AC,AD,BC,BD,CD}

MÓDULO 4: ANÁLISE COMBINATÓRIA

QUANTIDADE DE COMBINAÇÕES

Representamos pelo símbolo $C_{n,k}$ o número de combinações de n elementos tomados k a k, cuja fórmula é:

$$\boxed{C_{n,k} = \frac{n!}{k!(n-k)!}}$$

OBS:

$$C_{n,k} = \frac{A_{n,k}}{k!}$$

Exemplo: Considerando os elementos: A, C, V, P. O número de combinações dos 4 elementos tomados 2 a 2 é calculado como segue:

$$C_{4,2} = \frac{4!}{2!(4-2)!} = \frac{4!}{2!2!} = \frac{4.3.2!}{2!2!} = 6$$

SIMPLIFICANDO

Permutações são agrupamentos que diferem apenas pela **ORDEM** de seus elementos

Combinações são os agrupamentos que diferem pela **NATUREZA**

Arranjos são agrupamentos que diferem pela **ORDEM** e pela **NATUREZA** de seus elementos

IDENTIFICANDO QUAL UTILIZAR ...

PERMUTAÇÕES

- Na palavra NORTE, quantos anagramas podem ser formados? Quantos começam com vogal?
- Os resultados do último sorteio da Mega-Sena foram os números 04, 10, 26, 37, 47 e 57. De quantas maneiras distintas pode ter ocorrido essa sequência de resultados?
- Considere todos os números formados por seis algarismos distintos obtidos permutando-se, de todas as formas possíveis, os algarismos 1, 2, 3, 4, 5 e 6. Determine quantos números é possível formar (no total) e quantos números se iniciam com o algarismo 1.
- Utilizando o nome COPACABANA, calcule o número de anagramas formados desconsiderando aqueles em que ocorrem repetições consecutivas de letras.
- Em um torneio de futsal um time obteve 8 vitórias, 5 empates e 2 derrotas, nas 15 partidas disputadas. De quantas maneiras distintas esses resultados podem ter ocorrido?

IDENTIFICANDO QUAL UTILIZAR ...

COMBINAÇÕES

- Em uma sala de aula existem 12 alunas, onde uma delas chama-se Carla, e 8 alunos, onde um deles atende pelo nome de Luiz. Deseja-se formar comissões de 5 alunas e 4 alunos. Determine o número de comissões, onde simultaneamente participam Carla e Luiz.
- Um time de futebol é composto de 11 jogadores, sendo 1 goleiro, 4 zagueiros, 4 meio campistas e 2 atacantes. Considerando-se que o técnico dispõe de 3 goleiros, 8 zagueiros, 10 meio campistas e 6 atacantes, determine o número de maneiras possíveis que esse time pode ser formado.
- Um pesquisador científico precisa escolher três cobaias, num grupo de oito cobaias. Determine o número de maneiras que ele pode realizar a escolha.
- No jogo de basquetebol, cada time entra em quadra com cinco jogadores. Considerando-se que um time para disputar um campeonato necessita de pelo menos 12 jogadores, e que desses, 2 são titulares absolutos, determine o número de equipes que o técnico poderá formar com o restante dos jogadores, sendo que eles atuam em qualquer posição.

IDENTIFICANDO QUAL UTILIZAR ...

ARRANJOS

- Um número de telefone é formado por 8 algarismos. Determine quantos números de telefone podemos formar com algarismos diferentes, que comecem com 2 e terminem com 8.
- Em uma urna de sorteio de prêmios existem dez bolas enumeradas de 0 a 9. Determine o número de possibilidades existentes num sorteio cujo prêmio é formado por uma sequência de 6 algarismos.
- Em uma escola está sendo realizado um torneio de futebol de salão, no qual dez times estão participando. Quantos jogos podem ser realizados entre os times participantes em turno e returno?
- Otávio, João, Mário, Luís, Pedro, Roberto e Fábio estão apostando corrida. Quantos são os agrupamentos possíveis para os três primeiros colocados?

Exercícios

4) Na palavra NORTE, quantos anagramas podem ser formados? Quantos começam com vogal?

5) Os resultados do último sorteio da Mega-Sena foram os números 04, 10, 26, 37, 47 e 57. De quantas maneiras distintas pode ter ocorrido essa sequência de resultados?

6) Considere todos os números formados por seis algarismos distintos obtidos permutando-se, de todas as formas possíveis, os algarismos 1, 2, 3, 4, 5 e 6. Determine quantos números é possível formar (no total) e quantos números se iniciam com o algarismo 1.

7) Utilizando o nome COPACABANA, calcule o número de anagramas formados desconsiderando aqueles em que ocorrem repetições consecutivas de letras.

8) Em um torneio de futsal um time obteve 8 vitórias, 5 empates e 2 derrotas, nas 15 partidas disputadas. De quantas maneiras distintas esses resultados podem ter ocorrido?

9) Em uma sala de aula existem 12 alunas, onde uma delas chama-se Carla, e 8 alunos, onde um deles atende pelo nome de Luiz. Deseja-se formar comissões de 5 alunas e 4 alunos. Determine o número de comissões, onde simultaneamente participam Carla e Luiz.

Exercícios

10) Um time de futebol é composto de 11 jogadores, sendo 1 goleiro, 4 zagueiros, 4 meio campistas e 2 atacantes. Considerando-se que o técnico dispõe de 3 goleiros, 8 zagueiros, 10 meio campistas e 6 atacantes, determine o número de maneiras possíveis que esse time pode ser formado.

11) Um pesquisador científico precisa escolher pelo menos três cobaias, num grupo de oito cobaias. Determine o número de maneiras que ele pode realizar a escolha.

12) No jogo de basquetebol, cada time entra em quadra com cinco jogadores. Considerando-se que um time para disputar um campeonato necessita de pelo menos 12 jogadores, e que desses, 2 são titulares absolutos, determine o número de equipes que o técnico poderá formar com o restante dos jogadores, sendo que eles atuam em qualquer posição.

13) Um número de telefone é formado por 8 algarismos. Determine quantos números de telefone podemos formar com algarismos diferentes, que comecem com 2 e terminem com 8.

14) Em uma urna de sorteio de prêmios existem dez bolas enumeradas de 0 a 9. Determine o número de possibilidades existentes num sorteio cujo prêmio é formado por uma sequência de 6 algarismos.

15) Em uma escola está sendo realizado um torneio de futebol de salão, no qual dez times estão participando. Quantos jogos podem ser realizados entre os times participantes em turno e returno?

16) Otávio, João, Mário, Luís, Pedro, Roberto e Fábio estão apostando corrida. Quantos são os agrupamentos possíveis para os três primeiros colocados?

CHECK LIST TRABALHO GRAFOS