Matemática Discreta
2011

Departamento Matemática (FCT/UNL)

Matemática Discreta
2011

Departamento Matemática (FCT/UNL)

Regente da disciplina: Vitor Hugo Fernandes

Teórica 1: Claudio Fernandes http://www.claudiomath.co.cc/

Teórica 2: Vitor Hugo Fernandes

Funcionamento das Teóricas:
O aluno não é obrigado a assistir às aulas teóricas …

Funcionamento das Práticas: Obrigatórias

Avaliação:

1º Obtenção de Frequência:

Assistir a 2/3 das aulas práticas
NT1+NT2≥ 10 com NT1, NT2 ≥ 4

Data Testes	
1º Teste	2011-04-06
2º Teste	2011-06-01

2º Aprovação por Testes:

(NT1+NT2)/2 ≥ 9,5 com NT1, NT2 ≥ 7

3º Aprovação Época Normal ou Recurso

Para quem obteve frequência
Pode ser melhorada a nota do pior teste

MATEMÁTICA DISCRETA

Departamento Matemática (FCT/UNL)
http://www.claudiomath.co.cc/

Objectivos: Conceitos básicos em Teoria de Grafos e Fundamentos da Matemática. Conjuntos e Aplicações. Técnicas de demonstração e algoritmos para a resolução de problemas.

Programa:

1. Parte 1 - Conjuntos e Aplicações
    1. Conjuntos, relações binárias e indução matemática
    2. Funções
    3. Divisibilidade
    4. Congruências lineares
    5. Relações de recorrência

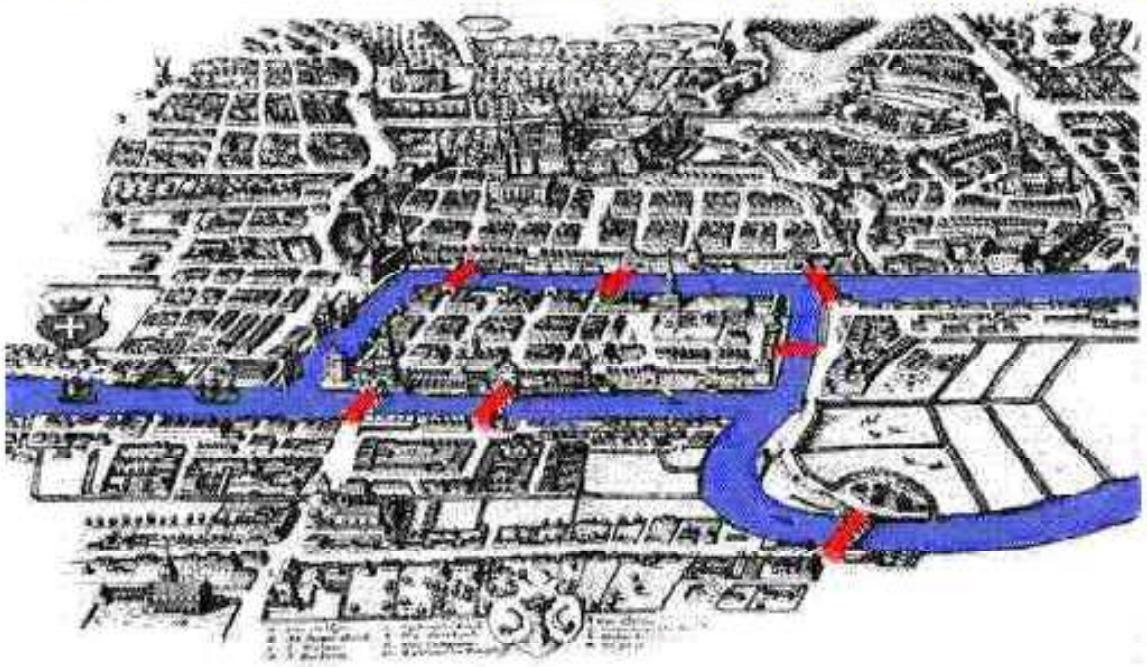
2 Parte 2 - Grafos e Aplicações

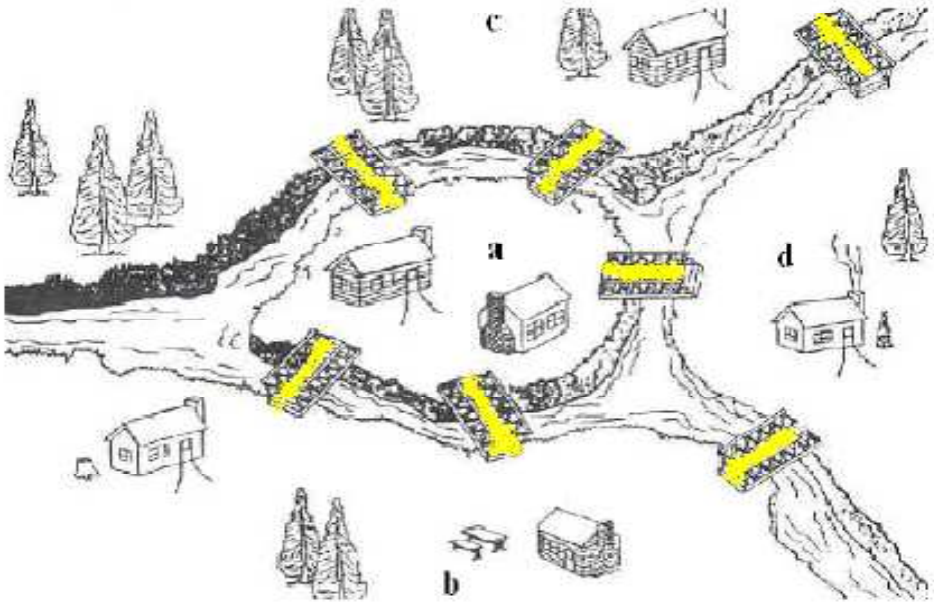
1. Generalidades
2. Conexidade
3. Árvores
4. Grafos Eulerianos
5. Grafos Hamiltonianos
6. Matrizes e Grafos

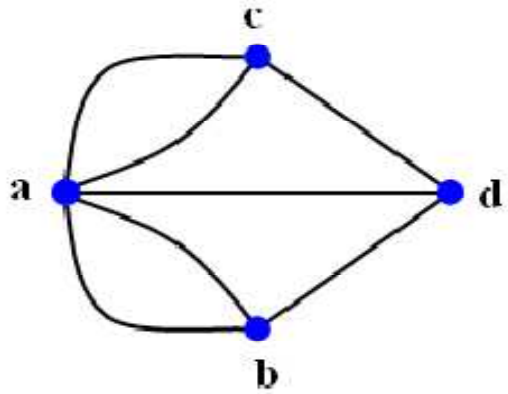
Bibliografia: Indicada no Clip + Material disponibilizado pelos prof.

Motivação:

Pontes de Konigsberg (1736 Euler)



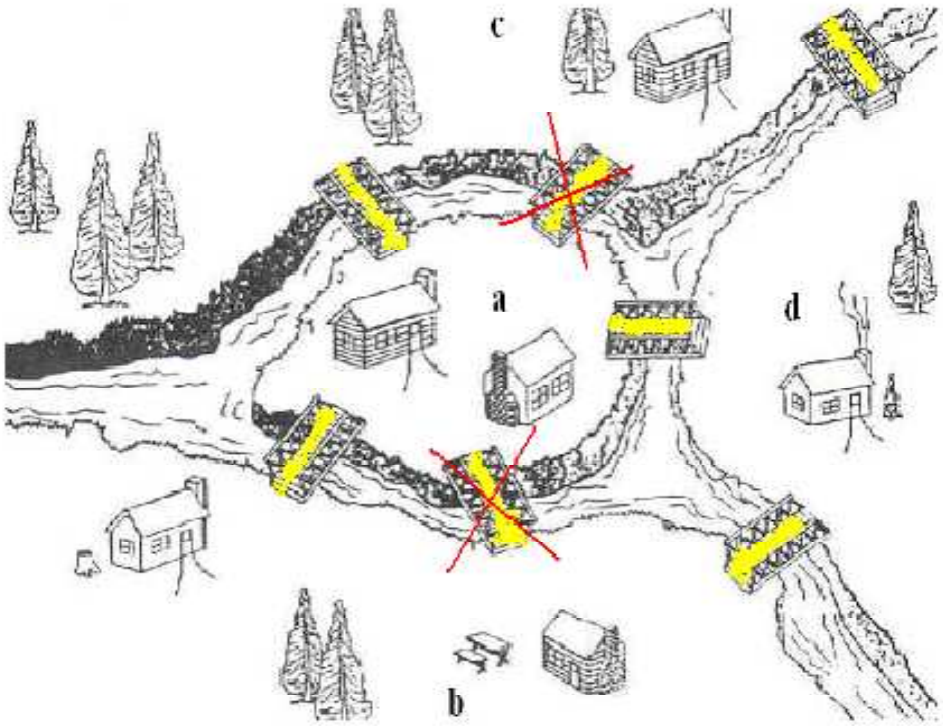


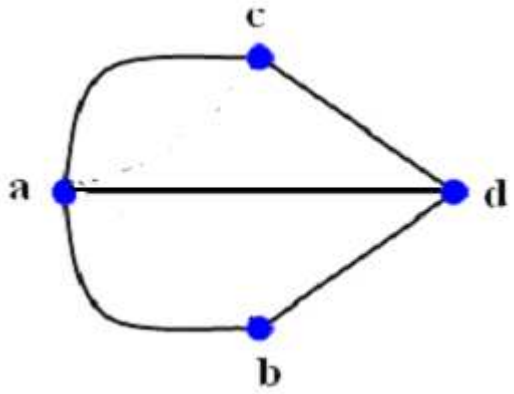


Questão: Será possível percorrer todas as pontes uma e uma só vez, regressando ao ponto de partida?

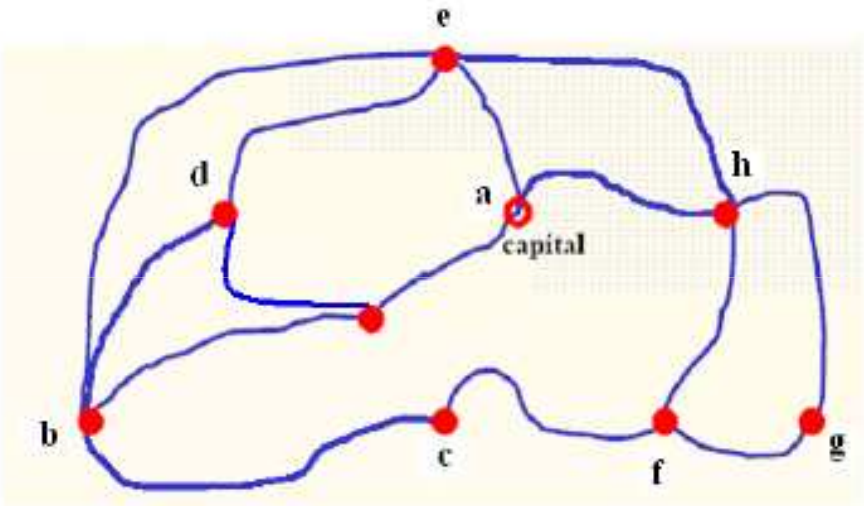
Questão: Será possível percorrer todas as pontes uma e uma só vez, podendo o passeio não finalizar na mesma margem onde começou?

Curiosidade: Konigsberg = Kaliningrado (Hoje)





Problema do caixeiro viajante

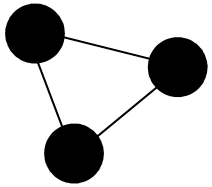


2004

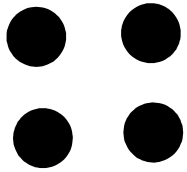
25000 cidades, 7anos(!!!) de tempo computacional

Questão: Será possível saindo da capital visitar todas as outras cidades, uma e uma só vez, e regressar à capital?

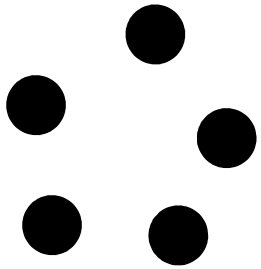
Nº de rotas (se fossem possíveis todas as ligações)



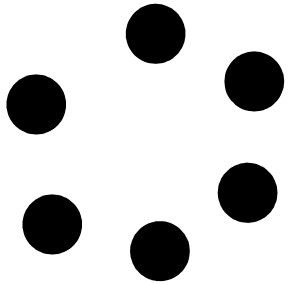
1 rota possível



3 rotas diferentes



12 rotas diferentes



60 rotas diferentes

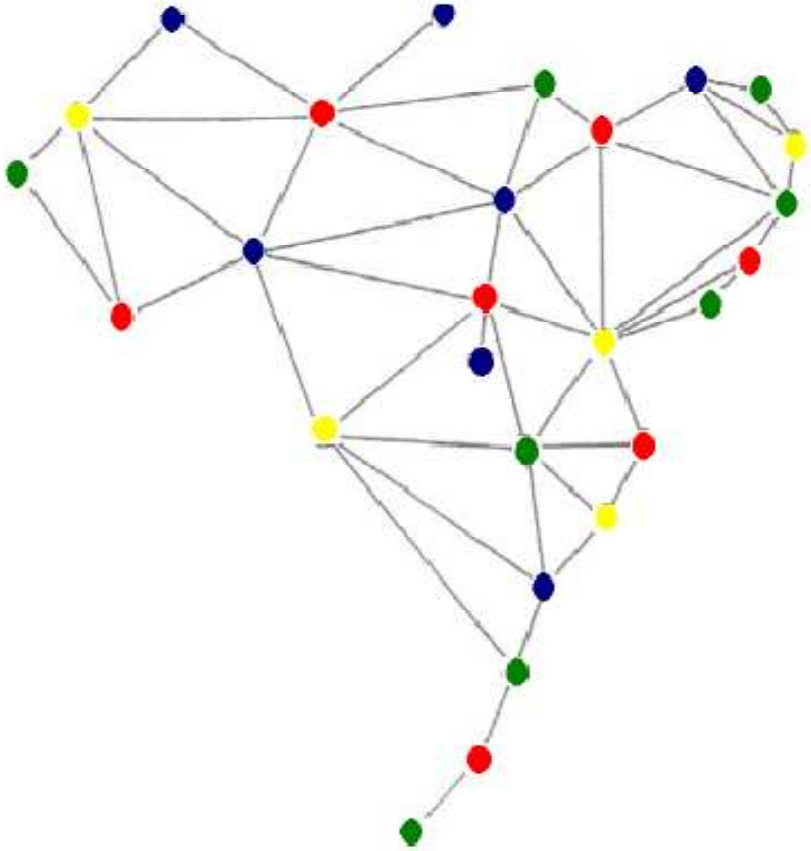
7 - 360 rotas

8 – 2520 rotas

9 – 20160 rotas

10 – 181440 (!)...

Problema da coloração de mapas



Teorema das 4 cores: Qualquer mapa plano, dividido em regiões, necessita no máximo de 4 cores para o colorir, de forma a que regiões vizinhas não tenham a mesma cor.

Primeiro grande resultado
provado com recurso a meios informáticos

Curiosidade:

1852- Problema colocado a De Morgan por um aluno

1976- Primeira demonstração "aceite" pela comunidade Matemática, com recurso ao computador (Appel- americano e Haken- alemão)

Capítulo 1

1.1 Conjuntos, Relações Binária e Indução Matemática

Representação de Conjuntos. Algumas Notações:

- Um conjunto é uma "colecção de objectos".

  $A, B, C, \ldots, X, Y, Z, \ldots$ conjuntos.

  $a, b, c, \ldots, x, y, z, \ldots$ elementos "$a \in A$"

- Em extensão - enumerando os elementos.

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

Em compreensão - através de condições.

$$A = \{x \in \mathbb{N} : |x - 1| < 5\}$$

Por diagrama de Venn - representando elementos dentro de linha fechada

Exemplos:

1. $\mathbb{N} = \{1, 2, 3, \ldots\}$ **Números Naturais**
2. $\mathbb{Z} = \{-2, -1, 0, 1, 2, \ldots\}$ **Números Inteiros**
3. $\mathbb{Q} = \{\frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{Z} \text{ e } q \neq 0\}$ **Números Racionais**
4. $\mathbb{R} = \mathbb{Q} \cup \{\text{dízimas infinitas não periódicas}\}$ **Núm. Reais**
5. $\emptyset$ *o conjunto que não tem nenhum elemento* **conj. Vazio**

Observação: Para qualquer conjunto A, $\emptyset \subseteq A$

- Sejam A e B conjuntos.
  Dizemos que A e B são iguais se têm os mesmos elementos.

“ $A=B$ “

  Dizemos que A está contido em B
  se todo o elemento de A é elemento de B

“ $A \subseteq B$ “

  Dizemos que A é subconjunto próprio de B
  se A está contido em B e A é diferente de B.

$A \subsetneq B$

Observação: $A = B$ se, e só se $A \subseteq B$ e $B \subseteq A$.

Operações sobre conjuntos: Sejam A e B dois conjuntos

- União de conjuntos:

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

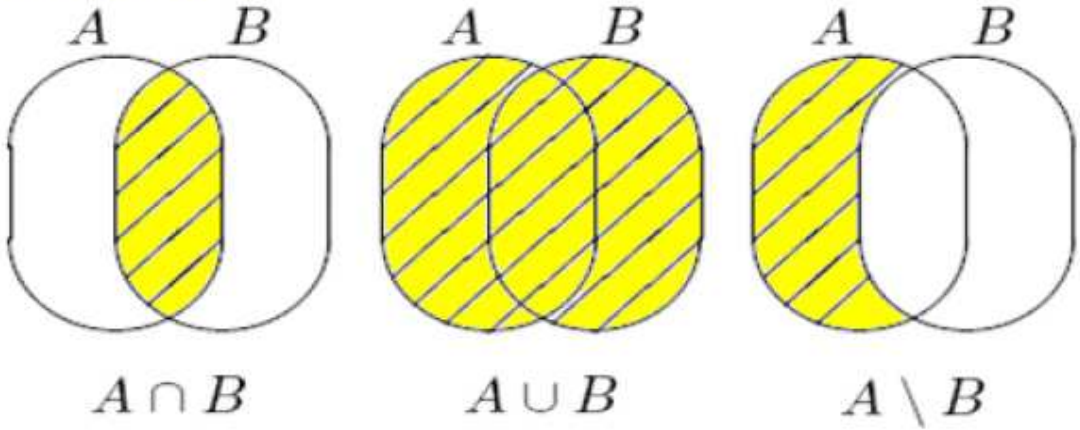
- Intersecção de conjuntos:

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

- Complementar de B em A de um conjunto:

$$A \setminus B = \{x : x \in A \text{ e } x \notin B\}.$$

A excepto B ou complementar de B em A

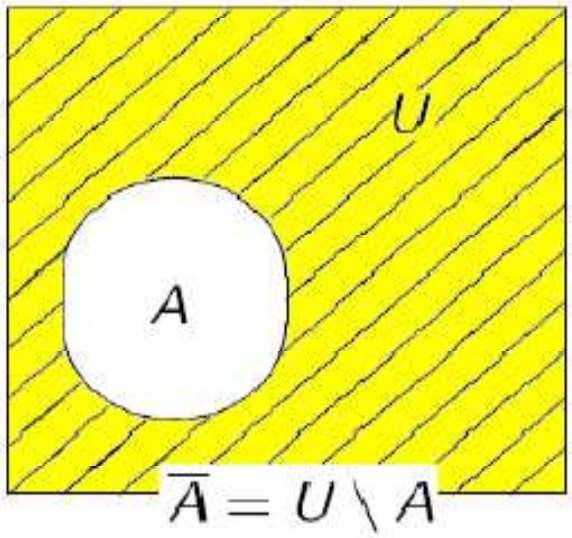


$A \cap B$ $A \cup B$ $A \setminus B$

- Fixado um universo U, o complementar de $A \subseteq U$ é o conjunto

$$\overline{A} = \{x \in U \mid x \notin A\}$$

ou seja, $\overline{A} = U \setminus A$ (o complementar de A em U).



Produto Cartesiano (dois conjuntos):

Sejam A e B dois conjuntos. Define-se o produto cartesiano de A por B como o conjunto

$$A \times B = \{(a, b) : a \in A \text{ e } b \in B\}.$$

Par ordenado

Observação:

1. Se $a \in A$ e $b \in B$ então

   $\{a, b\} = \{b, a\}$ mas $\{a, b\} \neq (a, b)$ e $(a, b) \neq (b, a)$

2. $(a,b) = (c,d)$ se e só se $a=c$ e $b=d$

Exemplo:

$A = \{a, b\},\ B = \{1, 2, 3\}$

$$A \times B = \{(a,1), (a,2), (a,3), (b,1), (b,2), (b,3)\}$$

$$B \times B = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3)\}$$

Produto Cartesiano (generalização):

Sejam $A_1, A_2, ..., A_n$, n conjuntos. Define-se o produto cartesiano dos conjuntos $A_1, ..., A_n$ como o conjunto

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

n-uplo ordenado

Se $A = A_1 = A_2 = ... = A_n$ então $A_1 \times A_2 \times \cdots \times A_n = A^n$

Conjunto das partes de um conjunto X:

Seja X um conjunto. Chama-se conjunto das partes de X ao conjunto $P(X)$ cujos elementos são os subconjuntos de X i.e.,

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

Exemplo: $C = \{2, 3, 4\}$

$$\mathcal{P}(C) = \{\emptyset, C, \{2\}, \{3\}, \{4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$$

- $\emptyset \in \mathcal{P}(C)$
- $C \in \mathcal{P}(C)$
- $\{3, 4\} \in P(C)$
- ~~$\{2\} \subseteq P(C)$~~
- $\{2\} \subseteq \{2, 3\}$
- $\emptyset \subseteq \{3, 4\}$

Partição de um conjunto X:

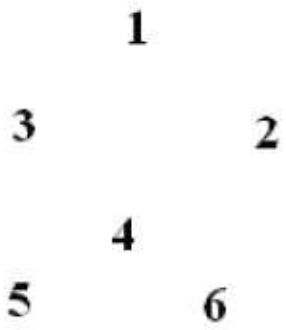
Se X é um conjunto. Chama-se partição de X a qualquer conjunto

$$\{X_i : \ i \in I\}$$

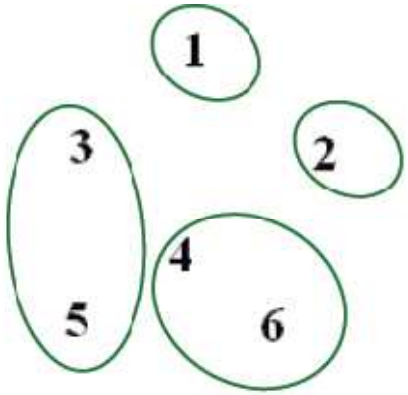
de subconjuntos de X tais que:

(1) $X = \bigcup_{i \in I} X_i$

(2) $i \neq j \Longrightarrow X_i \cap X_j = \emptyset$, *para quaisquer* $i, \ j \in I$.



X



$\{\{2\}, \{1\}, \{3,5\}, \{4,6\}\}$ é partição de X

Partição de um conjunto X:

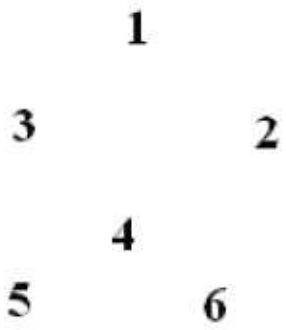
Se X é um conjunto. Chama-se partição de X a qualquer conjunto

$$\{X_i : \ i \in I\}$$

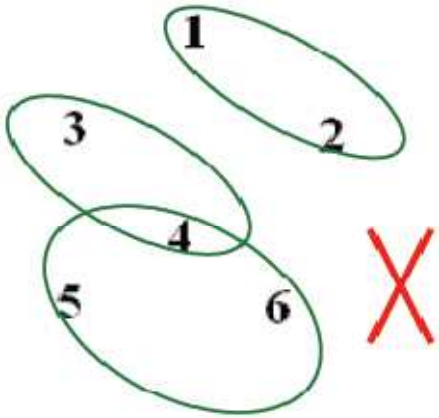
de subconjuntos de X tais que:

(1) $X = \bigcup_{i \in I} X_i$

(2) $i \neq j \Longrightarrow X_i \cap X_j = \emptyset$, *para quaisquer* $i, \ j \in I$.

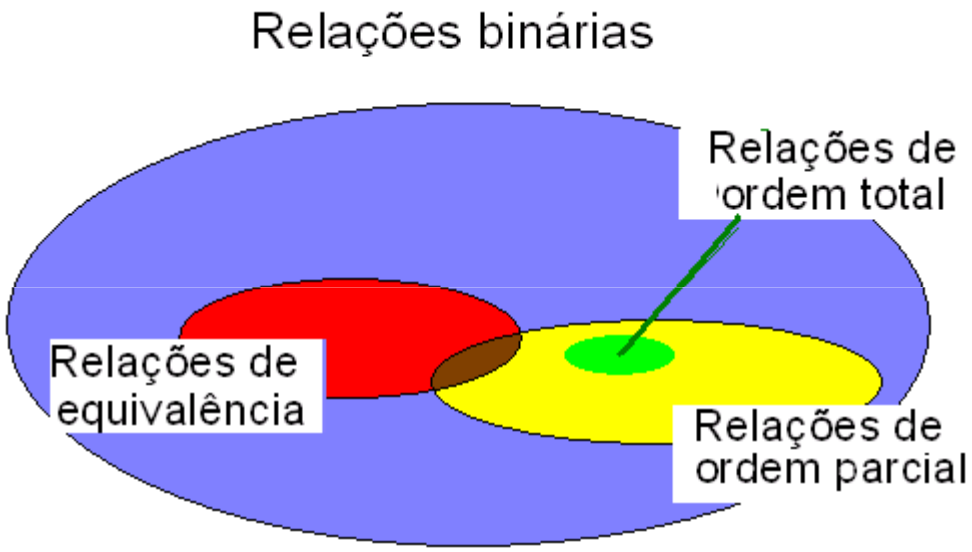


X



$\{\{1,2\},\{3,4\},\{4,5,6\}\}$ não é partição de X

1.1 Relações Binárias



Definição 1.1.1:

Seja X um conjunto. Chama-se relação binária sobre X a todo o subconjunto de $X \times X$.

Uma relação n-ária ($n \in \mathbb{N}, n \geq 2$) sobre X é um subconjunto de X^n.

Exemplos:

1. *Seja* $X = \{1, 2, 3\}$.

$$R = \{(1, 1), (2, 3), (3, 2)\}$$

2. *Seja* $X = \{1, 2, 3, 4\}$.

$$R = \{(x, y) \in X^2 : x + y \leq 5\}$$

Notação: *Sejam X é um conjunto e R é uma relação sobre X.*

Para designar que $(x,y) \in R$ escreve-se também xRy.

x está em relação com y (através da relação R)

Definição 1.1.2:

Sejam X e Y conjuntos. Uma relação de X em Y é um subconjunto de $X \times Y$. No caso particular de $X = Y$, temos uma relação binária sobre X.

Chamamos domínio de uma relação R de X em Y ao conjunto

$$\mathrm{dom}R = \{x \in X : \exists y \in Y \ (x, y) \in R\}$$

Chamamos imagem de uma relação binária R de X em Y ao conjunto

$$\mathrm{im}R = \{y \in Y : \exists x \in X \ (x, y) \in R\}.$$

Definimos relação inversa de R a relação de Y em X dada por

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

Exemplo: $X = \{1, 2, 3\}, Y = \{a, b, c, d\}$ $X \times Y$

$$\sim = \{(1, a), (1, c), (2, c), (2, d), (3, d)\}$$

Relação de X em Y

Exemplo: $X = \{1, 2, 3\}, Y = \{a, b, c, d\}$ $X \times Y$

$$\sim = \{(1, a), (1, c), (2, c), (2, d), (3, d)\}$$

Relação de X em Y

- $(1, c) \in \sim \Leftrightarrow 1 \sim c$ **1 está em relação com c**

Exemplo: $X = \{1, 2, 3\}, Y = \{a, b, c, d\}$ $X \times Y$

$$\sim = \{(1, a), (1, c), (2, c), (2, d), (3, d)\}$$

Relação de X em Y

- $(1, c) \in \sim \Leftrightarrow 1 \sim c$ **1 está em relação com c**

- $\text{dom} \sim = \{1, 2, 3\} \subseteq X,$ $\text{im} \sim = \{a, c, d\} \subseteq Y$ **imagem de ~**

Domínio de ~

Exemplo: $X = \{1, 2, 3\}, Y = \{a, b, c, d\}$ $X \times Y$

$$\sim = \{(1, a), (1, c), (2, c), (2, d), (3, d)\}$$

Relação de X em Y

- $(1, c) \in \sim \Leftrightarrow 1 \sim c$ **1 está em relação com c**

- $\text{dom} \sim = \{1, 2, 3\} \subseteq X, \quad \text{im} \sim = \{a, c, d\} \subseteq Y$

Domínio de ~

- $(\sim)^{-1} = \{(a, 1), (c, 1), (c, 2), (d, 2), (d, 3)\} \subseteq Y \times X$

Relação inversa de ~
Relação de Y em X

- $\text{dom}(\sim)^{-1} = \{a, c, d\} \subseteq Y, \quad \text{im}(\sim)^{-1} = \{1, 2, 3\} \subseteq X$

Relação Composta:

Sejam X, Y, Z conjuntos. Sejam ainda,

R uma relação de X em Y e *S* é uma relação de Y em Z

Define-se a relação composta de R por S como a relação

$S \circ R$ de X em Z,

definida por

$$S \circ R = \{(x, z) : \ (\exists a \in Y)\,(x, a) \in R \text{ e } (a, z) \in S\}$$

Relação Composta:

Sejam X, Y, Z conjuntos. Sejam ainda,

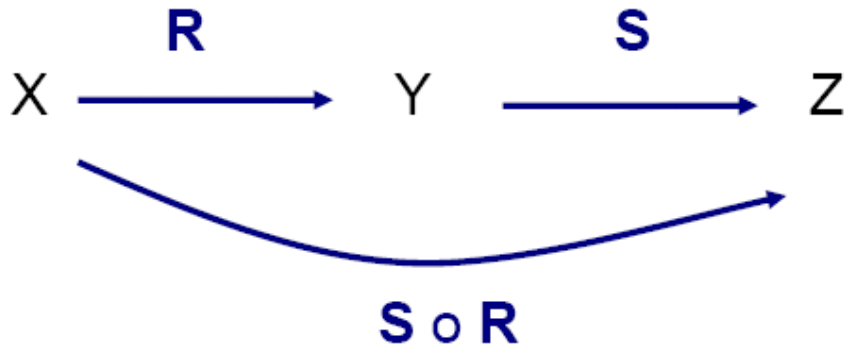
R uma relação de X em Y e *S* é uma relação de Y em Z

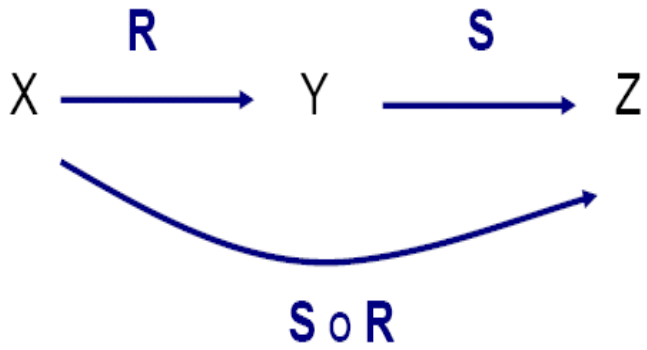
Define-se a relação composta de R por S como a relação

$S \circ R$ de X em Z,

definida por

$$S \circ R = \{(x, z) : \ (\exists a \in Y)\,(x, a) \in R \text{ e } (a, z) \in S\}$$





Exercício: $X = \{1, 2, 3\}$, $Y = \{a, b, c, d\}$, $Z = \{7, 8\}$

$\sim = \{(1, a), (1, c), (2, c), (2, d), (3, d)\}$ relação de X em Y

$S = \{(a, 7), (c, 8), (d, 8)\}$ relação de Y em Z

$S \circ \sim =$?

Representação de relações:

Seja R uma relação binária sobre $X = \{x_1, ..., x_n\}$.

Através de um diagrama:

os elementos de X são representados por pontos e dois pontos do diagrama que representam x_i e x_j estão unidos por uma seta, com orientação de x_i para x_j, se $(x_i, x_j) \in R$.

Através de uma matriz de adjacências:

A matriz de adjacências de R é a matriz $A = [a_{ij}]_{n\times n} \in \mathcal{M}_{n\times n}(\{0,1\})$ definida por:

$$a_{ij} = \begin{cases} 1 & \text{se} \quad (x_i, x_j) \in R \\ 0 & \text{se} \quad (x_i, x_j) \notin R \end{cases}$$

Exemplo: *Seja* $X = \{1, 2, 3, 4\}$.

$$R = \{(x, y) \in X^2 : x + y \leq 5\}$$

Exemplo: *Seja* $X = \{1, 2, 3, 4\}$.

$$R = \{(x, y) \in X^2 : x + y \leq 5\}$$

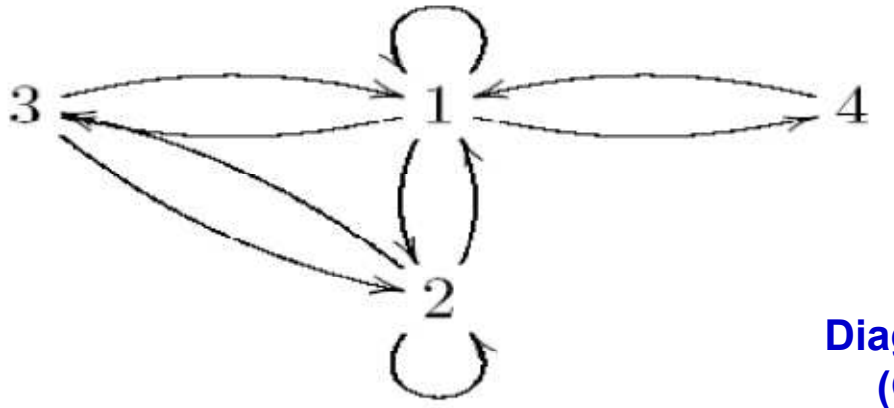


Diagrama da relação (Grafo orientado)

Exemplo: *Seja* $X = \{1, 2, 3, 4\}$.

$$R = \{(x, y) \in X^2 : x + y \leq 5\}$$

$$A = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

Matriz de adjacências de R (Grafo orientado)

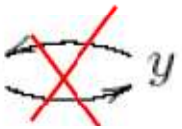
Definição 1.1.3: (Tipos de relações binárias)

Dizemos que uma relação binária R sobre X é:

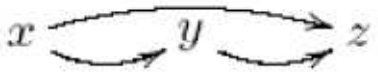
- *reflexiva* se $\forall x \in X \quad xRx$.

- *simétrica* se $\forall x, y \in X \quad xRy \Rightarrow yRx$.

- *anti-simétrica* se $\forall x, y \in X \quad xRy \wedge yRx \Rightarrow x = y$.



- *transitiva* se $\forall x, y, z \in X \quad xRy \wedge yRz \Rightarrow xRz$.



- *irreflexiva* se $\forall x \in X \quad (x, x) \notin R$.

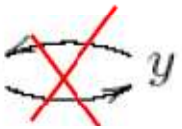
Definição 1.1.3: **(Tipos de relações binárias)**

Dizemos que uma relação binária R sobre X é:

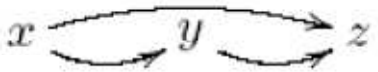
- *reflexiva* se $\forall x \in X \quad xRx$.

- *simétrica* se $\forall x, y \in X \quad xRy \Rightarrow yRx$.

- *anti-simétrica* se $\forall x, y \in X \quad xRy \wedge yRx \Rightarrow x = y$.



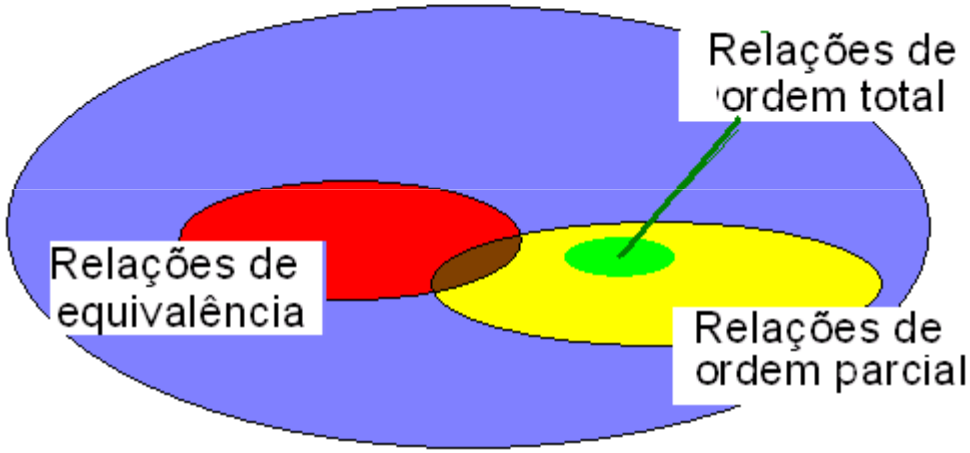
- *transitiva* se $\forall x, y, z \in X \quad xRy \wedge yRz \Rightarrow xRz$.



- *irrefl*

Relação de Equivalência

Relações binárias



Definição 1.1.4: (Relação de equivalência)

Uma relação binária reflexiva, simétrica e transitiva diz-se uma relação de equivalência.

Exemplos:

Sejam X um conjunto.

$\Delta = \{(x, x) : x \in X\}$ é relação de equivalência — "relação identidade"

$\Omega = \{(x, y) : x, y \in X\}$ é relação de equivalência — "relação universal"

Exercício: Quais das seguintes relações binária são relações de equivalência em *X*:

1. Seja $X = \{1, 2, 3, 4\}$.

$$R = \{(1,1), (1,2), (4,1), (2,2), (3,3), (1,4), (2,1), (4,4)\}$$

2. Seja $X = \{1, 2, 3, 4\}$.

$$S = \{(1,1), (1,2), (4,1), (2,2), (3,3), (1,4), (2,1), (4,4), (4,2), (2,4)\}$$

3. Seja *X*=$\mathbb{R}$. Considere em *X* a relação *R* definida por,

$$xRy \Leftrightarrow x^2 = y^2\,, \qquad x, y \in \mathbb{R}$$

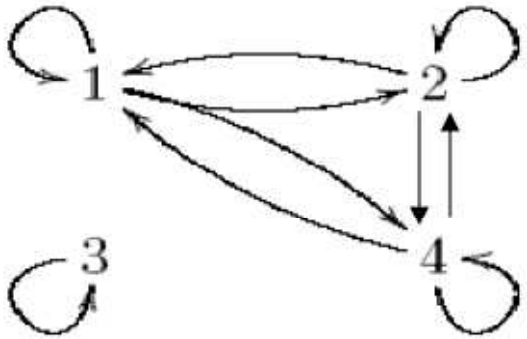
Definição 1.1.5: (Classes de equivalência)

Exemplo:

1. $X = \{1, 2, 3, 4\}$

$$R = \{(1,1), (1,2), (4,1), (2,2), (3,3), (1,4), (2,1), (4,4), (4,2), (2,4)\}$$

Relação equivalência sobre X



$$[1]_R = \{x \in X : \ x\, R\, 1\} \quad ?$$

$$= \{1, 2, 4\}$$

Classe de equivalência de 1

$$[2]_R = \{x \in X : \ x\, R\, 2\}$$

$$= \{1, 2, 4\}$$

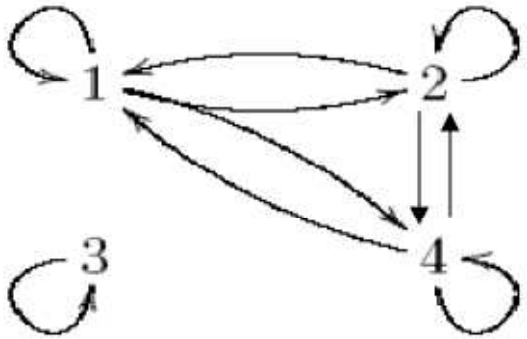
Definição 1.1.5: (Classes de equivalência)

Exemplo:

1. $X = \{1, 2, 3, 4\}$

$$R = \{(1,1), (1,2), (4,1), (2,2), (3,3), (1,4), (2,1), (4,4), (4,2), (2,4)\}$$

Relação equivalência sobre X



$$[1]_R = \{1, 2, 4\}$$
$$[2]_R = \{1, 2, 4\}$$
$$[3]_R = \{3\}$$
$$[4]_R = \{1, 2, 4\}$$

Conjunto quociente de X por R

$$X/R = \{[1]_R, [2]_R, [3]_R, [4]_R\} = \{\{1, 2, 4\}, \{3\}\}$$

Definição 1.1.5: (Classes de equivalência)

Seja X um conjunto e R uma relação de equivalência sobre X.

Chama-se classe de equivalência (módulo R) de um elemento $a \in X$, *ao conjunto*

$$[a]_R = \{x \in X : xRa\}.$$

O conjunto das classes de equivalência $[a]_R$ com $a \in X$ é chamado de conjunto quociente de X por R,

$$X/R = \{[\mathrm{a}]_R : \ \mathrm{a} \in X\}$$

Exemplo:

2. $X = \{1, 2, 3, 4, 5\}$

$R=$

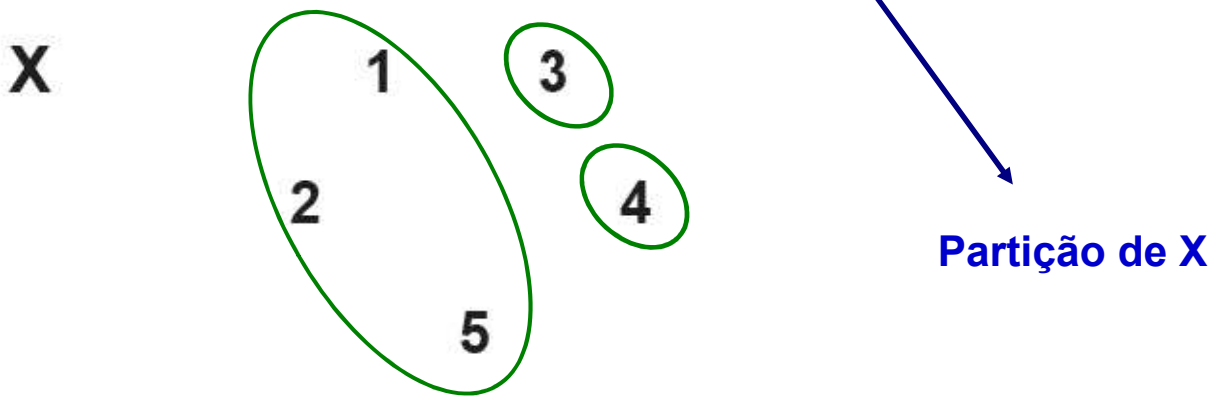
$\{(1,1),(2,2),(3,3),(4,4),(5,5),(1,2),(2,1),(1,5),(5,1),(2,5),(5,2)\}$

Relação equivalência sobre X

Tem-se:

$[1] = \{1, 2, 5\} = [2] = [5], \quad [3] = \{3\}, \quad [4] = \{4\}$

$$X/R = \{\{1, 2, 5\}, \{3\}, \{4\}\}$$



Partição de X

Não esquecer:

R é relação de equivalência em X

Tem-se:

- $[a]_R \neq \emptyset$ pois $a \in [a]_R$
- $aRb \Rightarrow [a]_R = [b]_R$
- $a\not{R}b \Rightarrow [a]_R \cap [b]_R = \emptyset$
- $X/R = \{[x]_R : x \in X\}$ é uma partição de X

$$X = \bigcup_{x \in X} [x]_R$$

Proposição 1.1.6: **Teorema 1.1.7:** **Teorema 1.1.8:**

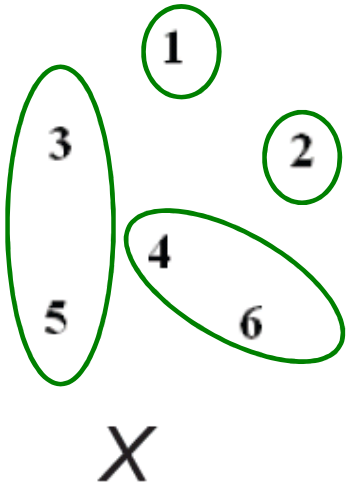
Teorema 1.1.8: Dá-nos resposta à seguinte questão.

Questão: Considere o conjunto $X = \{1, 2, 3, 4, 5, 6\}$

e a partição de X dada por

$$\mathcal{P} = \{\{2\}, \{1\}, \{3, 5\}, \{4, 6\}\}$$

Existe uma relação de equivalência cujas classes sejam os elementos da partição?



$$R = \{(1,1), (2,2), (3,3), (4,4), (5,5), (6,6), (3,5), (5,3), (4,6), (6,4)\}$$

Congruência módulo 3

n=3

Define-se em $\mathbb{Z}$ uma relação binária $\equiv_3$ do seguinte modo: para quaisquer $x, y \in \mathbb{Z}$

$$x \equiv_3 y \iff x - y = 3k, \quad \text{para algum } k \in \mathbb{Z}$$

X-Y é múltiplo de 3

Congruência módulo 3

n=3

Define-se em $\mathbb{Z}$ uma relação binária $\equiv_3$ do seguinte modo: para quaisquer $x, y \in \mathbb{Z}$

$$x \equiv_3 y \Leftrightarrow x - y = 3k, \text{ para algum } k \in \mathbb{Z}$$

X-Y é múltiplo de 3

Observação:

$9 \equiv_3 0$ pois $9-0 = 3x2$

$0 \equiv_3 9$ pois $0 - 9 = 3x(-2)$

$10 \equiv_3 1$ pois $10-1 = 9 = 3x3$

$100 \equiv_3 10$ pois $100-10=90=3x30$

É relação de equivalência

Classes de equivalência para $\equiv_3$

- $[0]_3 = \{x \in \mathbb{Z} : x \equiv_3 0\}$

  $= \{..., -15, -12, -9, -6, -3, 0, 3, 6, 9, 12, 15, ...\}$

- $[1]_3 = \{x \in \mathbb{Z} : x \equiv_3 1\}$

  $= \{..., -14, -11, -8, -5, -2, 1, 4, 7, 10, 13, 16, ...\}$

- $[2]_3 = \{x \in \mathbb{Z} : x \equiv_3 2\}$

  $= \{..., -13, -10, -7, -4, -1, 2, 5, 8, 11, 14, 17, ...\}$

$[3]_3 = [0]_3,\ [4]_3 = [1]_3,\ [5]_3 = [2]_3, ...$

$$\mathbb{Z}/\equiv_3 = \{[0]_3, [1]_3, [2]_3\}$$

Obs: Se $x \equiv_3 y$ então diz-se que x=y (mod 3)

Congruência módulo n

nº fixo

3. Em $\mathbb{Z}$ define-se uma relação de equivalência $\equiv_n$ por: para quaisquer $x, y \in \mathbb{Z}$,

$$x \equiv_n y \Leftrightarrow \exists k \in \mathbb{Z} : x - y = kn,$$

designada por relação de congruência módulo n.

Tem-se:

$$\begin{aligned} \overline{0} &= \{\ldots, -2n, -n, 0, n, 2n, \ldots\} \\ \overline{1} &= \{\ldots, -2n+1, -n+1, 1, n+1, 2n+1, \ldots\} \\ &\ldots \\ \overline{n-1} &= \{\ldots, -n-1, -1, n-1, 2n-1, 3n-1, \ldots\} \end{aligned}$$

$$\mathbb{Z}/R = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Não esquecer

Proposição 1.1.6:

Sejam X um conjunto e R uma relação de equivalência sobre X. Para quaisquer $a,\ b \in X$, as seguintes afirmações são equivalentes:

(1) bRa;

(2) $b \in [a]_R$;

(3) $[b]_R = [a]_R$.

Teorema 1.1.7:

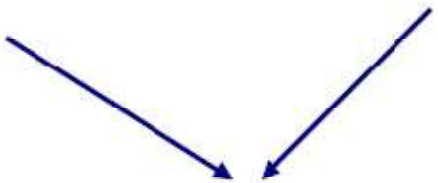
Sejam X um conjunto e R uma relação de equivalência sobre X.

Temos:

(1) *Para qualquer $x \in X$, $[x]_R \neq \emptyset$;*

(2) *Para quaisquer $x,\ y \in X$, $[x]_R = [y]_R$ ou $[x]_R \cap [y]_R = \emptyset$;*

(3) $X = \bigcup_{x \in X} [x]_R$;



X/R **é partição de** X

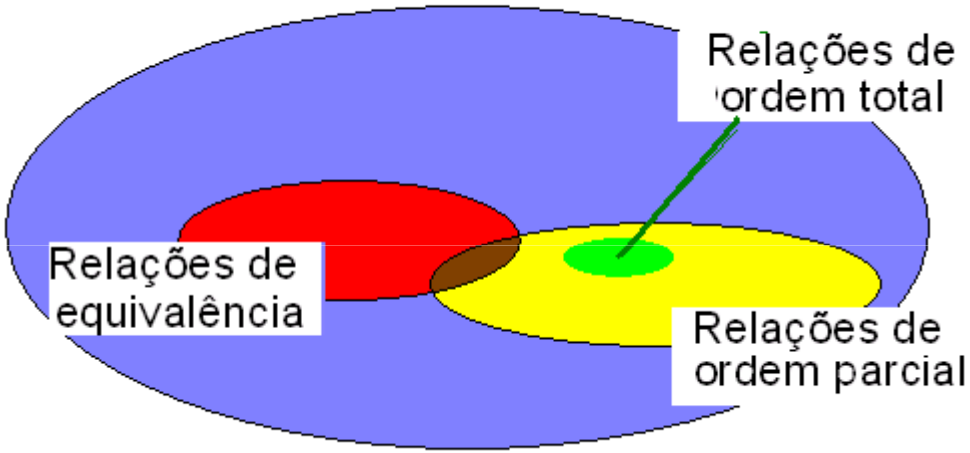
Teorema 1.1.8:

1. *Se R é uma relação de equivalência sobre X, então X/R é uma partição de X.*
2. *Se $\mathcal{P} = \{X_i : \ i \in I\}$ é uma partição de X e R é a relação*

$$xRy \iff (\exists i \in I) \qquad x,\ y \in X_i,$$

(i) *R é relação de equivalência sobre X*
(ii) $\mathcal{P} = X/R$.

Relações binárias



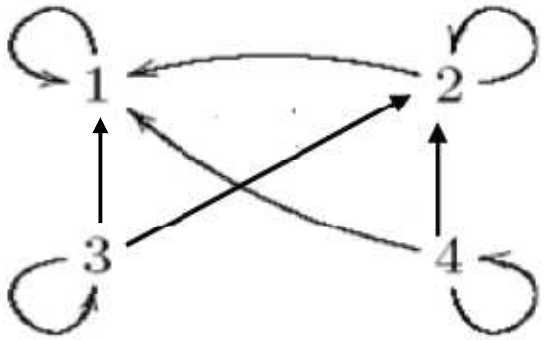
Definição 1.1.9: (Relação de ordem parcial)

Uma relação binária reflexiva, anti-simétrica e transitiva diz-se uma relação de ordem parcial. **"r.o.p."**

Exemplo:

1. $X = \{1, 2, 3, 4\}$

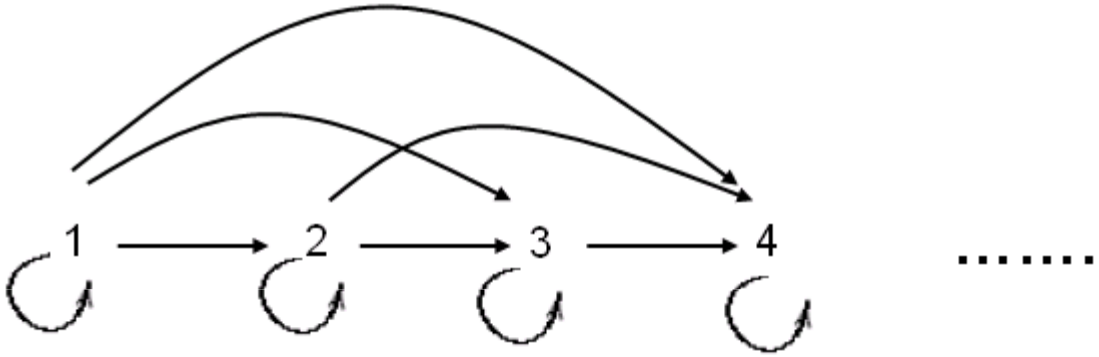
$R = \{(1,1), (2,2), (3,3), (4,4), (4,2)(2,1), (4,1), (3,2), (3,1)\}$



´É relação de ordem parcial

2. $\mathbb{N}$ com a relação $\leq$ definida por,

$n \leq m$ se e só se n é menor ou igual a m, $\quad n, m \in \mathbb{N}$



´É relação de ordem parcial

Notação:

- As relações de ordem parcial são usualmente designadas por $\leq$

$$x \leq y \quad \Leftrightarrow \quad (x, y) \in \leq$$

(x está em relação com y)

(x é "menor ou igual" a y)

(x está abaixo do y)

(y está acima do x)

- Se $\leq$ é uma r.o.p em X. Dois elementos x e $y \in X$ dizem-se comparáveis se

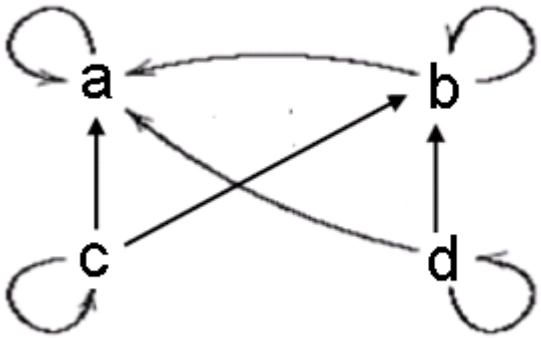
$$x \leq y \text{ ou } y \leq x.$$

- Sejam $\leq$ uma r.o.p. sobre X e $x, y \in X$. Escrevemos $x < y$ para significar $x \leq y$ e $x \neq y$.

Exemplo:

1. $X = \{a, b, c, d\}$

$\leq$ → relação de ordem parcial representada no diagrama



Os elementos **d** e **a** são comparáveis? Sim, pois $(d, a) \in \leq \Leftrightarrow d \leq a$

Como $d \neq a$ então $d < a$

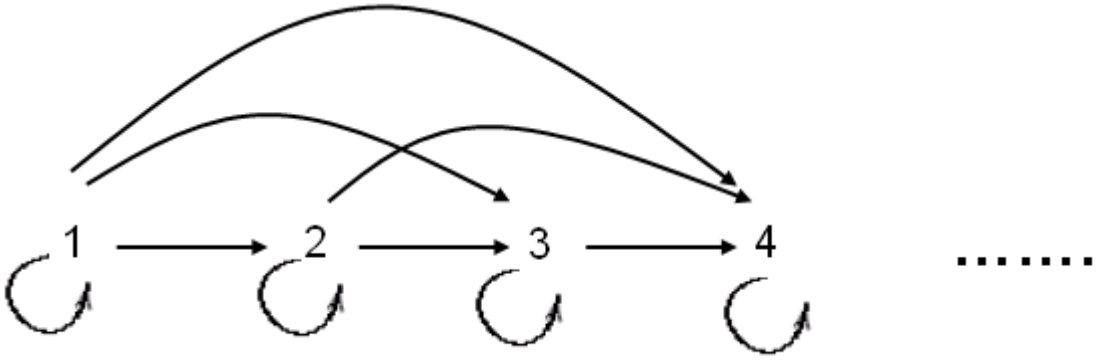
Os elementos **c** e **d** são comparáveis? Não, pois $(c, d) \notin \leq$ c $(d,c) \notin \leq$

Os elementos **d** e **b** são comparáveis? Sim, pois $d \leq b$

❷ $\mathbb{N}$ com a relação $\leq$ definida por,

$n \leq m$ se e só se n é menor ou igual a m, $\quad n, m \in \mathbb{N}$

relação de ordem parcial



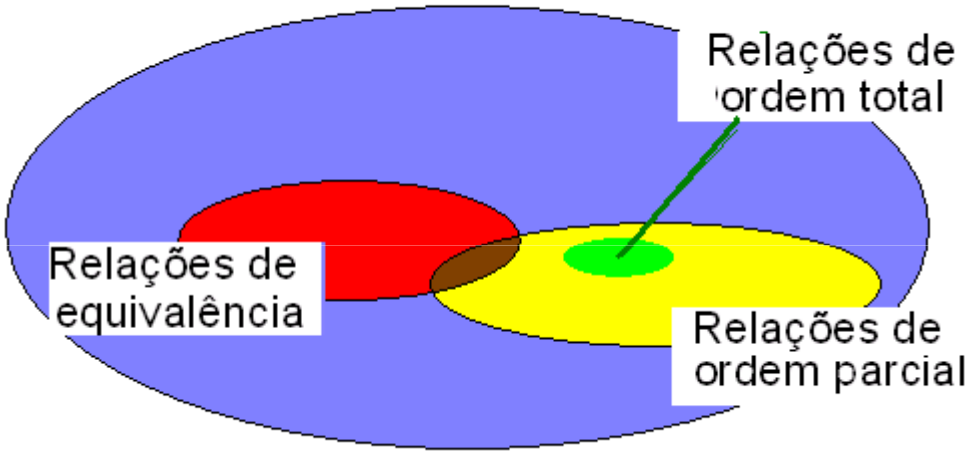
Se X é um conjunto,

$\leq$ é relação de ordem parcial em X
onde
todos os elementos são comparáveis

"r.o.t."

$\leq$ **diz-se uma relação de ordem total**

Relações binárias



Definição 1.1.10: (Conjunto parcialmente /totalmente ordenado)

Se X é um conjunto e $\leq$ é uma r.o.p. em X. Então:

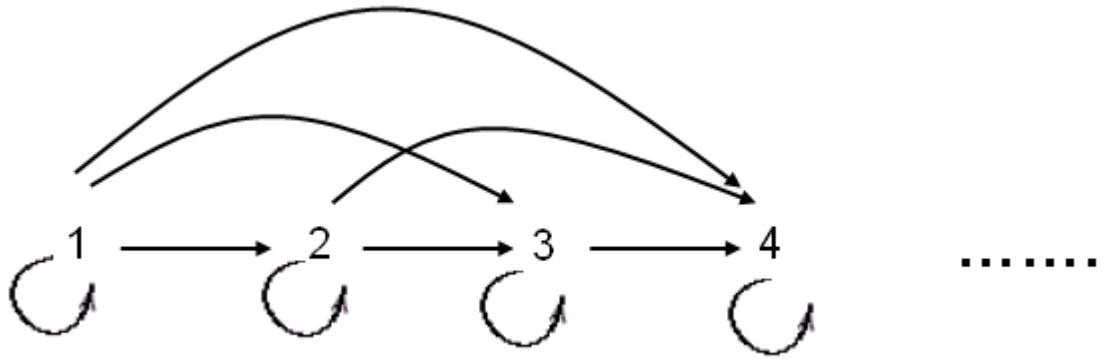
(1) O par $(X, \leq)$ diz-se um conjunto parcialmente ordenado (c.p.o.)

(2) Se a relação $\leq$ for de ordem total então $(X, \leq)$ diz-se um conjunto totalmente ordenado (c.t.o.) ou uma cadeia

Exemplos:

1

Seja $\leq$ a relação de ordem usual em $\mathbb{R}$. Então $(\mathbb{R}, \leq)$ é uma cadeia.
$(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$ são cadeias (para a ordem usual).



2. $X = \{1, 2, 3\}$

$$P(X) = \{\emptyset, X, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}$$

Defina-se em $P(X)$ a relação binária dada por: Para A, B em $P(X)$

$$A \leq B \iff A \subseteq B$$

Refexiva? $A \in \mathcal{P}(X)$

Ora, $A \leq A$ pois $A \subseteq A$

Anti-simétrica? $A, B \in \mathcal{P}(X)$

Suponha-se que $A \leq B$ e $B \leq A$.

$\Updownarrow$ $\Updownarrow$

$A \subseteq B$ $B \subseteq A$ Assim, $A = B$

Transitiva?

2. $X = \{1, 2, 3\}$

$$P(X) = \{\emptyset, X, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}$$

Defina-se em $P(X)$ a relação binária dada por: Para A, B em $P(X)$

$$A \leq B \iff A \subseteq B$$

Transitiva? $A, B, C \in \mathcal{P}(X)$

Suponha-se que $A \leq B$ e $B \leq C$.

$$\Updownarrow \qquad \Updownarrow$$

$$A \subseteq B \qquad B \subseteq C$$

Assim,

$$A \subseteq B \subseteq C, \quad \text{logo}$$

$$A \subseteq C \Leftrightarrow A \leq C.$$

$(P(X), \leq)$

é um c.p.o.

$(P(X), \leq)$

não é c.t.o.

2

Seja X um conjunto. A relação $\leq$ definida em $\mathcal{P}(X)$ por:

$$A \leq B \iff A \subseteq B$$

é uma relação de ordem parcial em $\mathcal{P}(X)$, logo $(\mathcal{P}(X), \leq)$ é um c.p.o. (não é c.t.o.)

Diagramas de Hasse

Forma mais eficaz de representar c.p.o.

Definição 1.1.11: Seja $(X, \leq)$ um c.p.o..

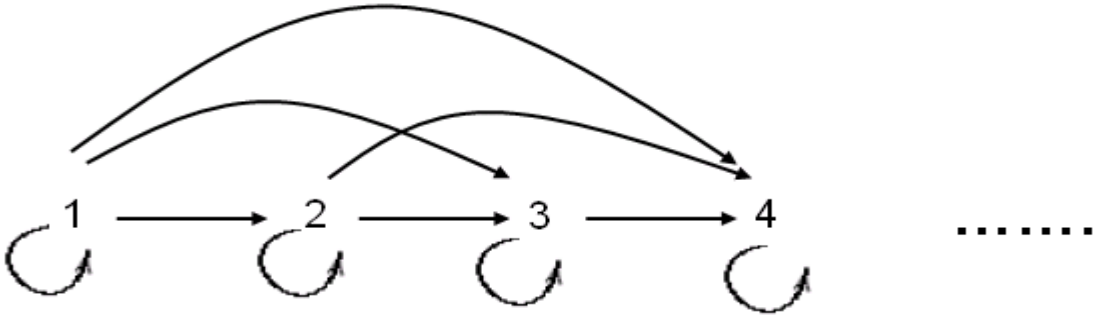
$x, y \in X$

Diz-se que y cobre x se (i) $x \leq y$

(ii) Não existe $z \in X$ tal que $x < z < y$

Exemplo

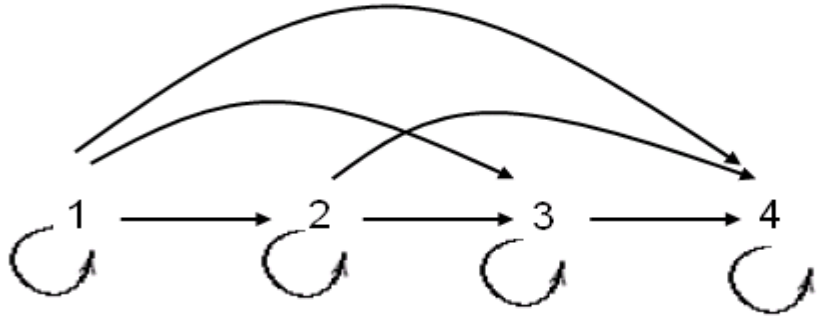
- $(\mathbb{N}, \leq)$ onde $\leq$ a relação de ordem usual



3 cobre 3 e 3 cobre 2

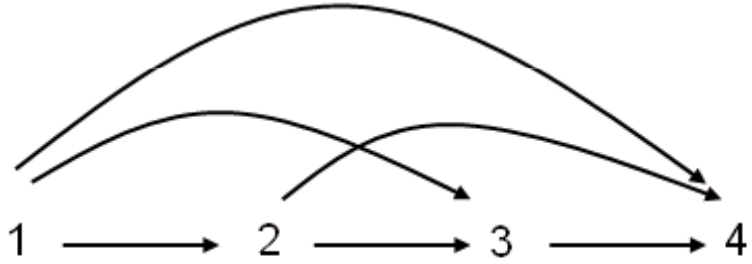
Considere em $\mathbb{N}$ uma relação de ordem parcial tenha o diagrama em baixo

(1)



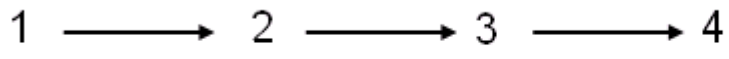
.....

(2)



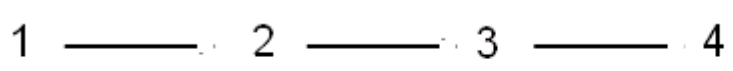
.....

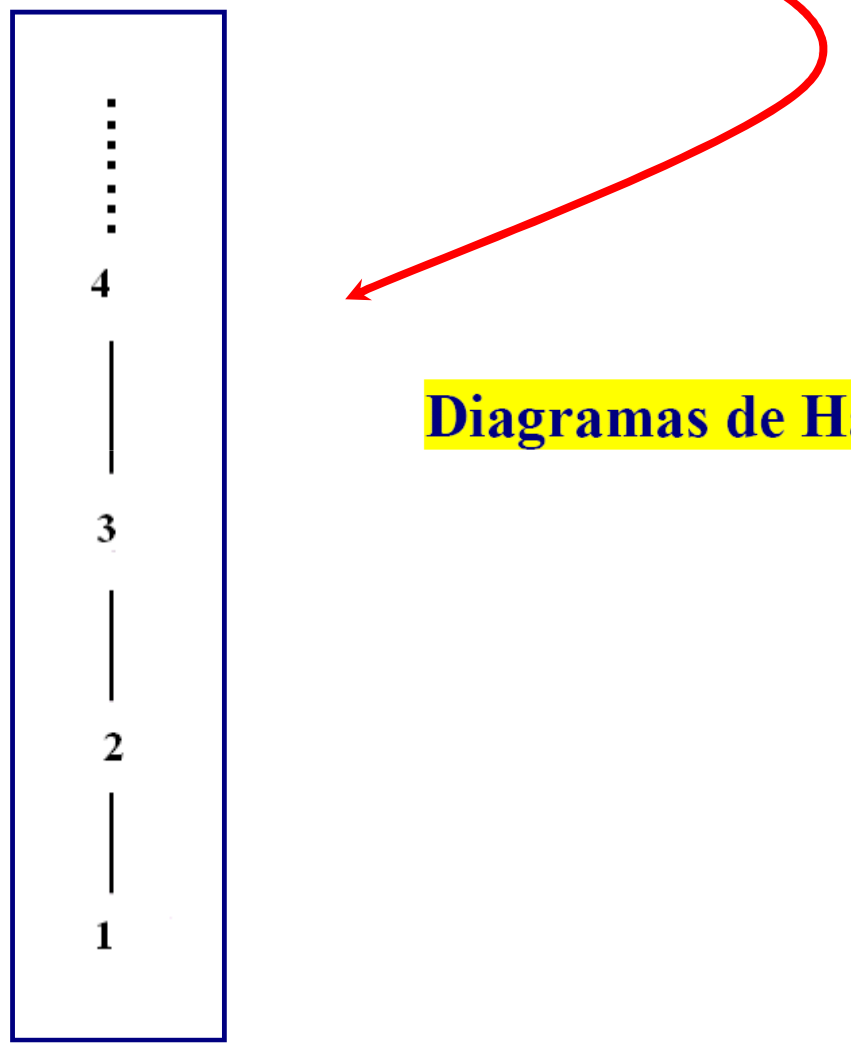
(3)



.....

(4)





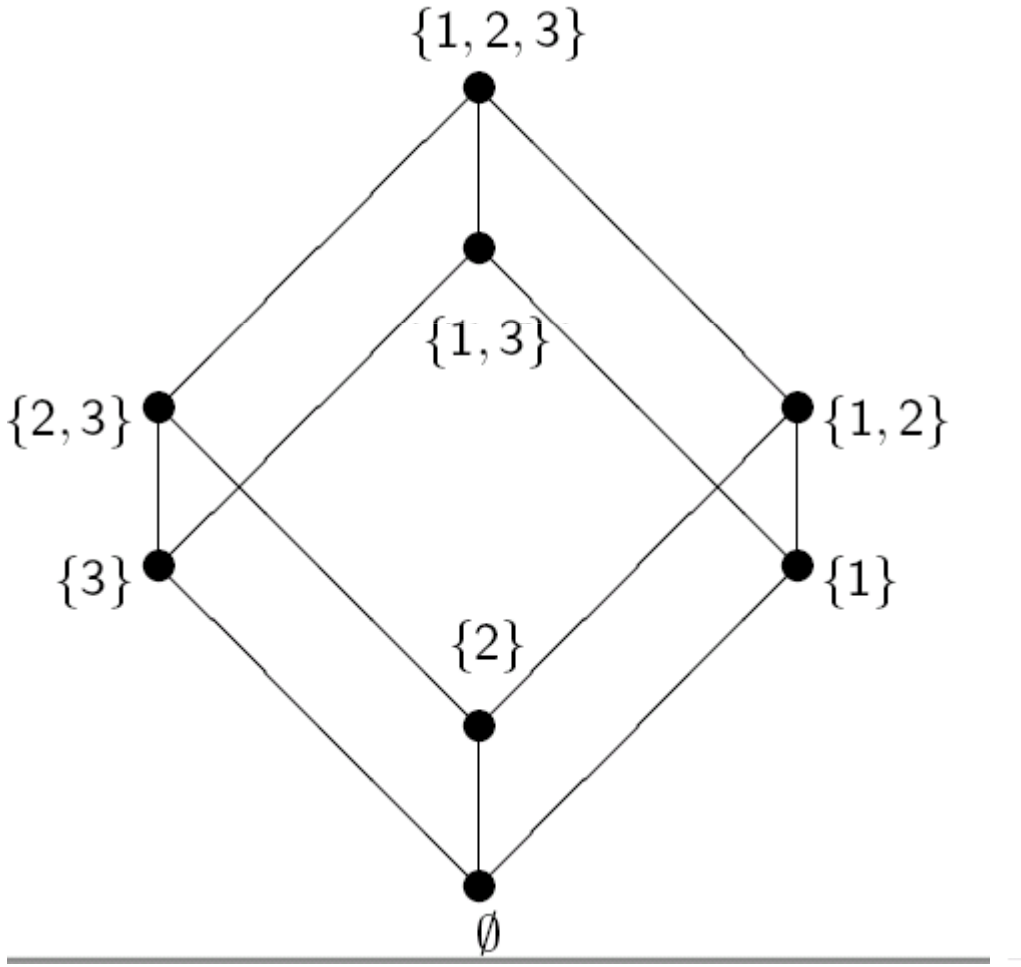
Diagramas de Hasse

Exemplo $X = \{1, 2, 3\}$

$$P(X) = \{\emptyset, X, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}$$

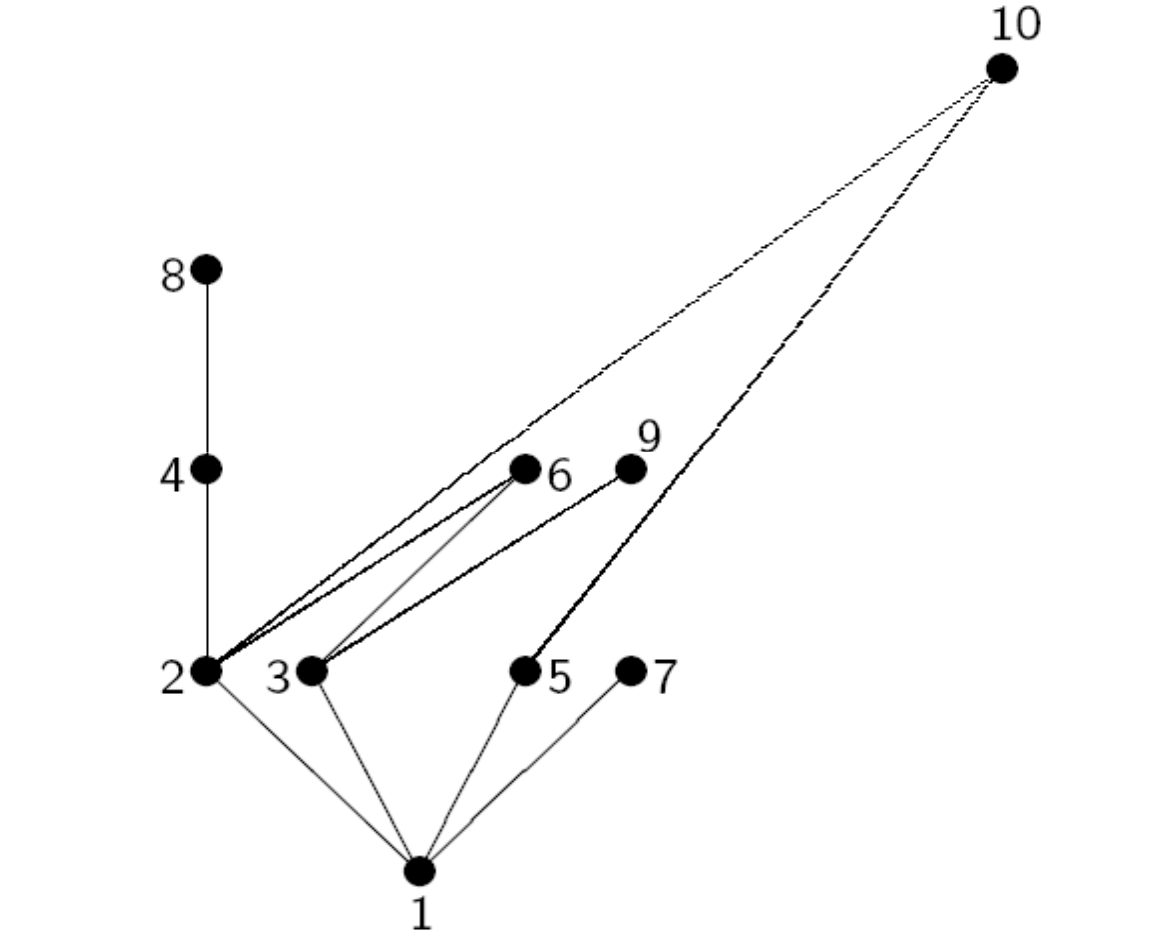
$$A \leq B \iff A \subseteq B$$

´É relação de ordem parcial



Exemplo

Considere X={1,2,3,4,5,6,7,8,9,10} e | uma relação de ordem parcial com o seguinte diagrama de Hasse



Relação de Divisibilidade

X={1,2,3,4,5,6,7,8,9,10}. Considere a relação | definida por: a, b$\in$X

$$a|b \text{ (a divide b)} \iff (\exists k \in \mathbb{N}) \;\; b = ak$$

b é múltiplo de a

Observação:

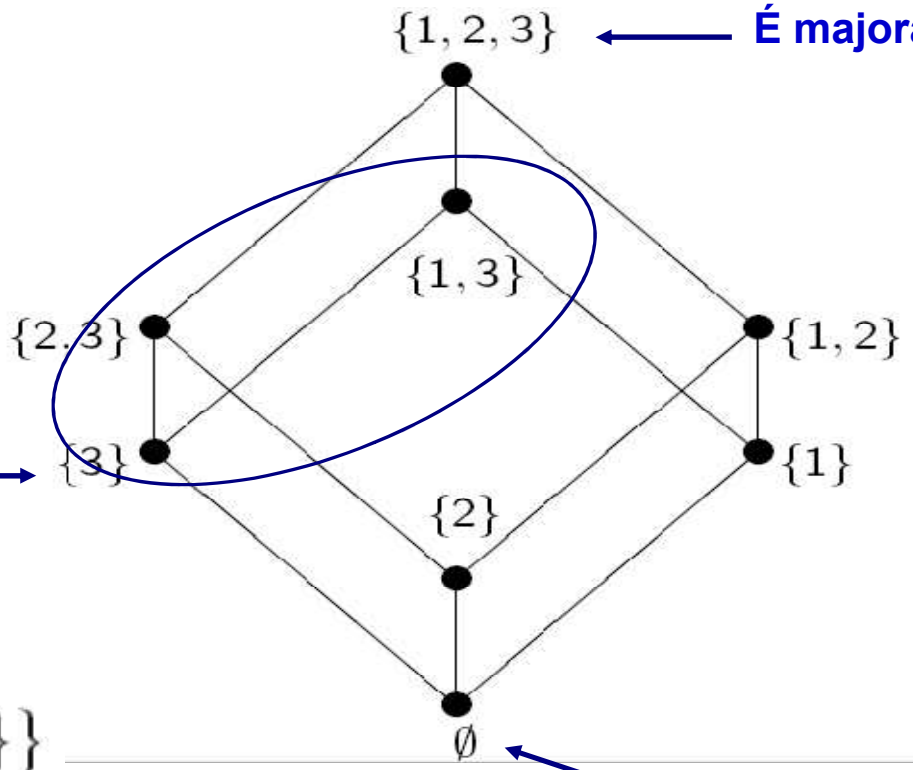
- $3|9 \qquad 3|3 \qquad 2|10$ 7 é comparável com 8?
- $a|a$ pois $a = a \times 1$ (reflexiva)
- $a|b$ e $b|a$ então $a = b$ (anti-simétrica)
- $a|b$ e $b|c$ então $a|c$ (transitiva)

(X, |) é c.p.o.
não é c.t.o.

Definição 1.1.12:

Sejam $(X, \leq)$ um c.p.o. e $Y \subseteq X$.

- O c.p.o. $(\mathcal{P}(\{1,2,3\}), \subseteq)$ possui o seguinte diagrama de Hasse:



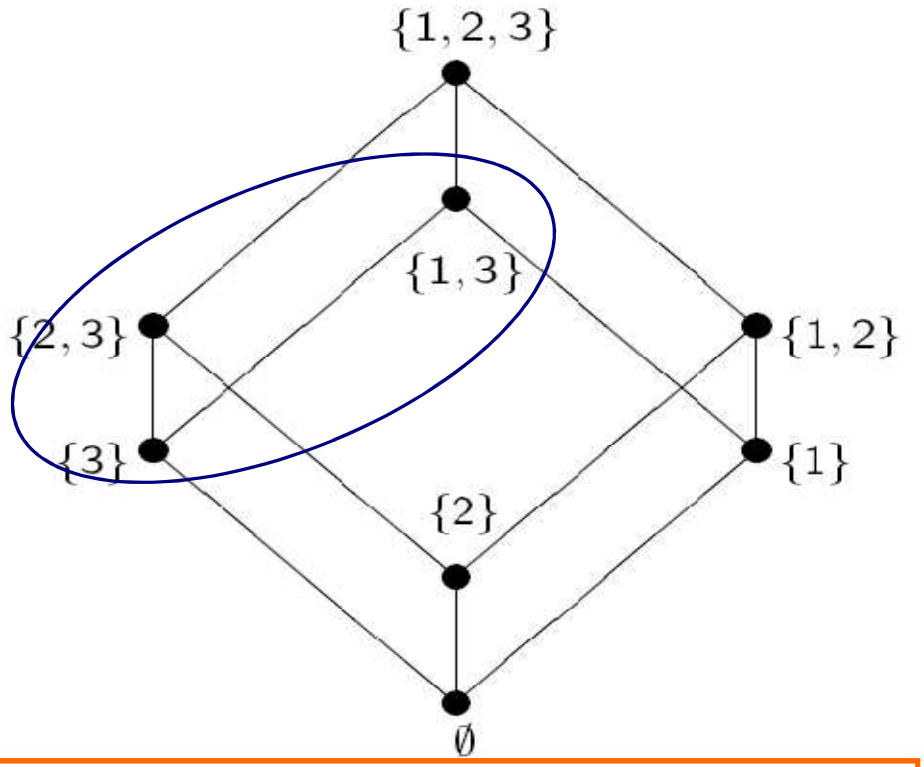
$$X = P(\{1,2,3\})$$

$$Y = \{\{3\}, \{1,3\}, \{2,3\}\}$$

- O c.p.o. $(\mathcal{P}(\{1,2,3\}), \subseteq)$ possui o seguinte diagrama de Hasse:

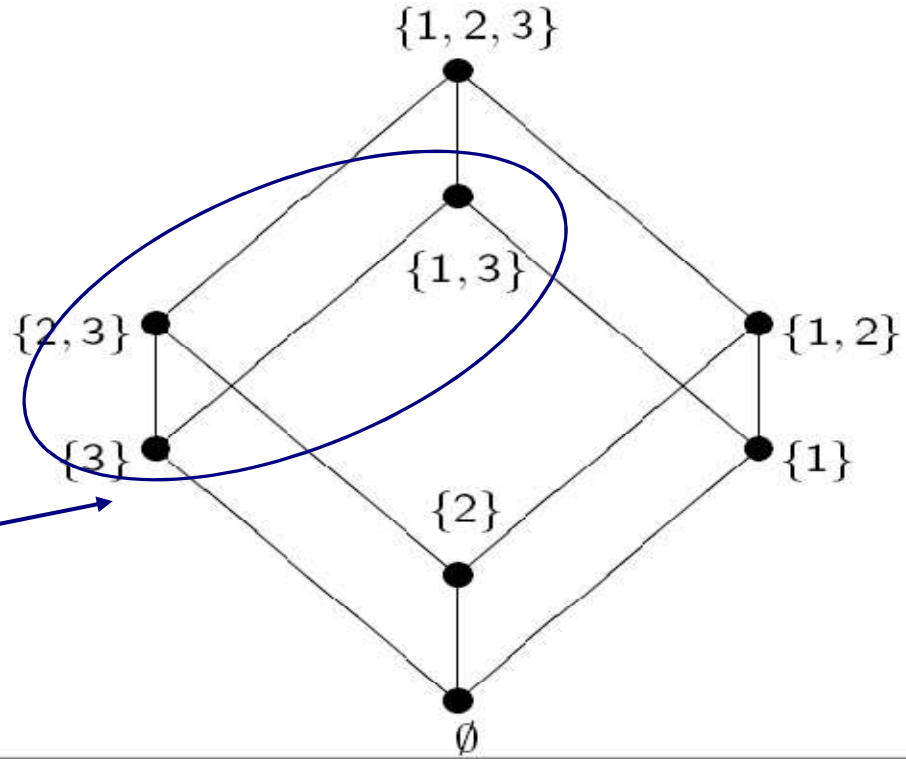
$$X = P(\{1,2,3\})$$

$$Y = \{\{3\}, \{1,3\}, \{2,3\}\}$$



- Dizemos que $a \in X$ é um minorante [resp. majorante] de Y se $a \leq y$ [resp. $y \leq a$], para qualquer $y \in Y$.

Y não tem máximo
Não tem último elemento



É o mínimo de Y
É o primeiro elemento

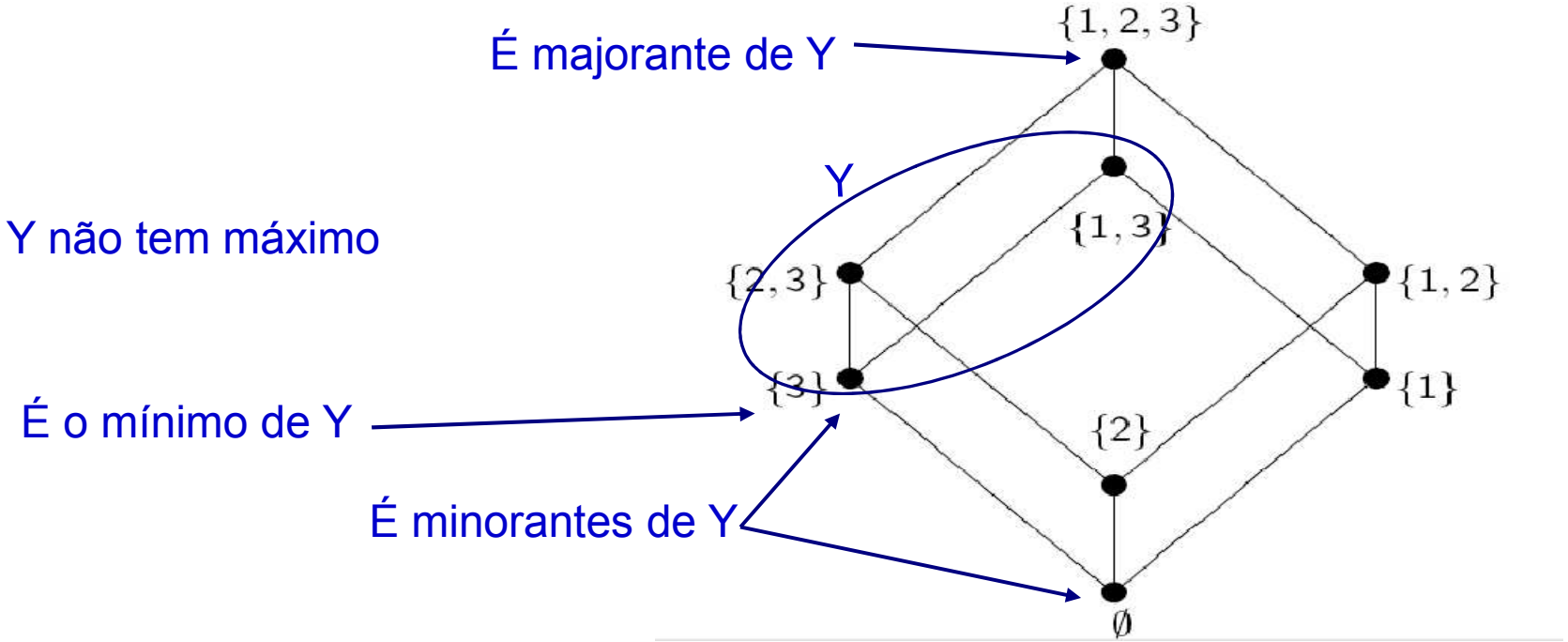
- Chamamos primeiro elemento de Y (ou mínimo de Y) a um elemento $a \in Y$ tal que
$$a \leq y, \text{ para qualquer } y \in Y.$$

- Chamamos último elemento de Y (ou máximo de Y) a um elemento $b \in Y$ tal que
$$y \leq b, \text{ para qualquer } y \in Y.$$

Resumo: Seja $(X, \leq)$ um c.p.o. e Y um subconjunto de X.

Um elemento $a \in X$ diz-se:

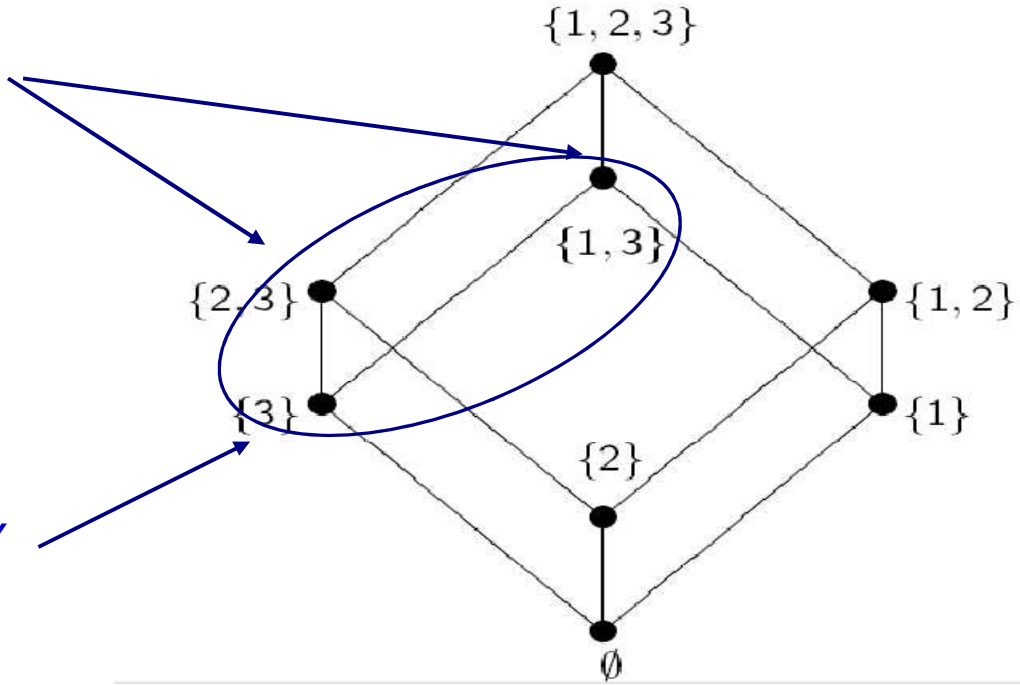
- Majorante de Y, se $\forall y \in Y, \quad y \leq a$
- Minorante de Y, se $\forall y \in Y, \quad a \leq y$
- O máximo de Y (último elemento), se $a \in Y$ e é Majorante de Y
- O mínimo de Y (primeiro elemento), se $a \in Y$ e é Minorante de Y



Diz-se ainda que $a \in X$ é :

- Elemento maximal de Y, se
  i) $a \in Y$
  ii) a não é majorado por nenhum outro elemento diferente de Y

É elemento maximal de Y



É elemento minimal de Y

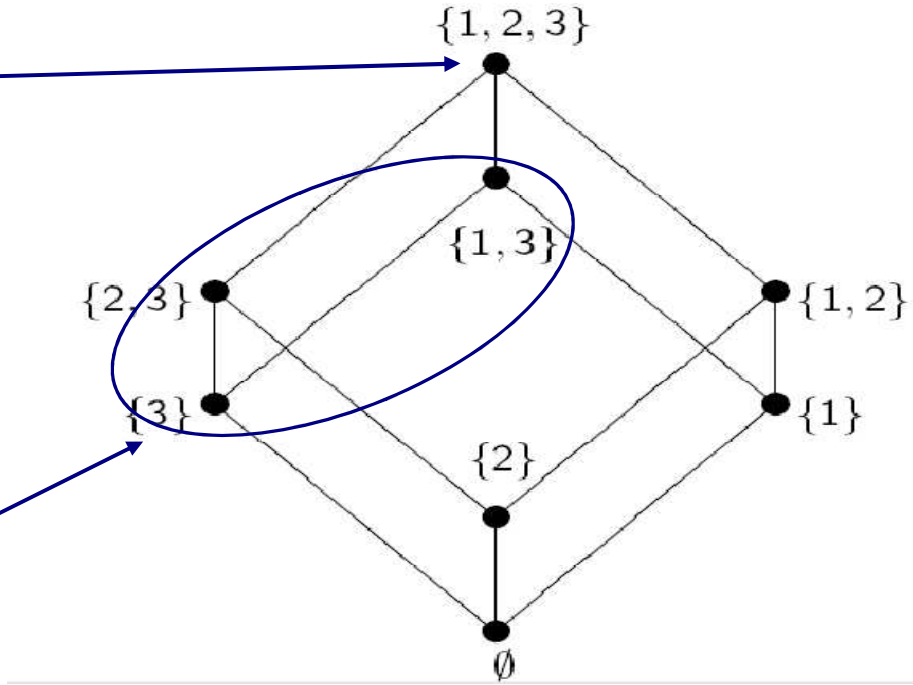
- Elemento minimal de Y, se
  i) $a \in Y$
  ii) a não é minorado por nenhum outro elemento diferente de Y

Diz-se ainda que $a \in X$ é :

- O supremo de Y, se a é o mínimo do conjunto dos majorantes
- O ínfimo de Y, se a é máximo do conjunto dos minorantes

É o supremo de Y

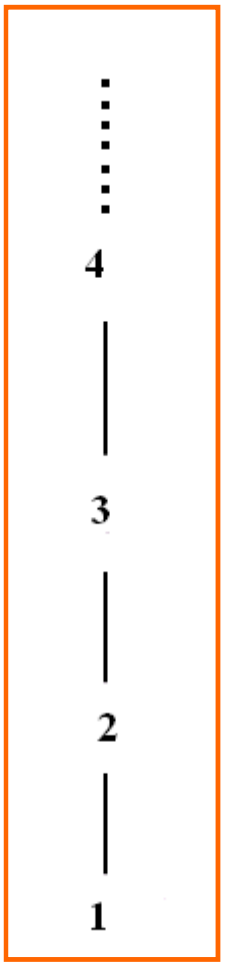
É o ínfimo de Y



Axioma da boa ordenação

O par $(\mathbb{N}, \leq)$ em que $\leq$ denota a ordem usual, é um conjunto bem ordenado.

todo o subconjunto não vazio de $\mathbb{N}$ possui primeiro elemento.



Princípio de Indução

S é um conjunto de números naturais não vazio que satisfaz a condição:

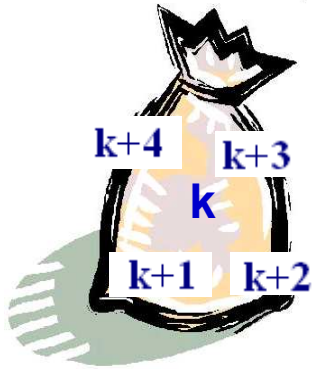
$$\text{Se } n \in S \ (n \in \mathbb{N}) \ \text{ então } n+1 \in S$$

Questão: Que conjunto é S ?

1. Pelo axioma da boa ordenação existe um elemento k que é o mínimo de S

2. Mas,

$$\text{Se } n \in S \ (n \in \mathbb{N}) \ \text{ então } n+1 \in S$$



.....

Conclusão:

$$S = \{k, k+1, k+2, k+3, ...\}$$
$$= \{n \in \mathbb{N} : \ n \geq k\}$$

Princípio de Indução

Se $\phi(n)$ é uma condição na variável $n \in \mathbb{N}$, tal que:

1. $\phi(k)$ é uma proposição verdadeira (em geral $k = 1$)
2. Se $\phi(n)$ é verdadeira então $\phi(n+1)$ é verdadeira

Então,

$\phi(n)$ é verdadeira, para todo $n \geq k$.

Exercício 1: Prove que

$$1+2+3+\ldots+n = \frac{n(n+1)}{2}, \quad \text{para todo } n \in \mathbb{N}$$

Soma dos n primeiros naturais

Efeito dominó

Departamento Matemática (FCT/UNL)

Exercício 2: Prove que

$$2n+1 \leq 2^n, \text{ para qualquer natural } n \geq 3.$$

1. Verificar que para n=3 a proposição é verdadeira.

Ora, para $n = 3$,

$2n + 1 = 2 \times 3 + 1 = 7$ $\qquad$ $2^n = 2^3 = 8$

Tendo-se, $7 \leq 8$ uma proposição verdadeira

2. Supondo que $2n + 1 \leq 2^n$ para algum *n,* mostre-se que

Hipótese

$$2(n+1)+1 \leq 2^{n+1}$$

Tese

Ora,

$$2(n+1)+1 = 2n+2+1 = (2n+1)+2 \leq 2^n+2 \leq 2^n+2^n$$
$$= 2 \times 2^n = 2^{n+1} \quad \text{c.q.d.}$$

Hipótese

Conclusão: 1 e 2 permitem afirmar que a condição é verdadeira para n≥3

Exercício 3:

Consideremos a sucessão $(a_n)_{n\geq 0}$ *definida por*

$$\begin{cases} a_0 &= 1 \\ a_1 &= 2 \\ a_n &= 4a_{n-1} - 4a_{n-2} \end{cases} .$$

Então $a_n = 2^n$, *para qualquer* $n \in \mathbb{N}_0$.

Princípio de Indução completa (Segundo princípio de indução)

Se $\phi(n)$ é uma condição na variável $n \in \mathbb{N}$, tal que:

1. $\phi(k)$ é uma proposição verdadeira
2. Se $\phi(k)$, $\phi(k+1)$,..., $\phi(n)$ verdadeiras implica que $\phi(n+1)$ é é verdadeira

Então,

$\phi(n)$ é verdadeira, para todo $n \geq k$.

Exercício 3:

Consideremos a sucessão $(a_n)_{n\geq 0}$ *definida por*

$$\begin{cases} a_0 &= 1 \\ a_1 &= 2 \\ a_n &= 4a_{n-1} - 4a_{n-2} \end{cases} .$$

Então $a_n = 2^n$, *para qualquer* $n \in \mathbb{N}_0$.

1. Verificar que para n=0 a proposição é verdadeira.

Ora, para $n = 0$ tem-se que

$$a_0 = 1 \text{ (por definição).}$$

Assim,

$$a_0 = 1 = 2^0 \text{ é uma proposição verdadeira.}$$

2. Supondo que se tem $a_t = 2^t$ para $0 \leq t \leq n$ mostre-se que se tem ainda

$$a_{n+1} = 2^{n+1}$$

Hipótese

2. Supondo que se tem $a_t = 2^t$ para $0 \leq t \leq n$ mostre-se que se tem ainda $a_{n+1} = 2^{n+1}$

Tese

Ora,

$$a_{n+1} = 4a_n - 4a_{n-1} = 4 \times 2^n - 4 \times 2^{n-1}$$

Por definição — Hipótese

$$= 2^n \left(4 - 4 \times \frac{1}{2}\right) = 2^{n+1}. \quad \text{c.q.d.}$$

Conclusão: 1 e 2 permitem afirmar que a condição é verdadeira para n≥0, isto é, $a_n = 2^n$ para qualquer $n \in \mathbb{N}_0$.

Número de elementos de P(X)

Dado um conjunto finito X, denotamos por

$$|X|$$

o número de elementos (cardinal) de X.

Observação:

Seja $Y = \{a, b\}$ então $|Y| = 2$

$$P(Y) = \text{?}$$
$$= \{\emptyset, Y, \{a\}, \{b\}\}$$

$$|P(Y)| = 2^2$$

$X = \{a, b, c\}$ então $|X| = 3$

$$P(X) = \text{?}$$
$$= \{\emptyset, Y, \{a\}, \{b\}, \{c\}, X, \{a, c\}, \{b, c\}\}$$

$$|P(X)| = 2^3$$

Teorema :

Seja X um conjunto com n elementos ($n \in \mathbb{N}_0$). Então,

$$|\mathcal{P}(X)| = 2^n.$$

Demonstração.

Pretende-se mostrar que para qualquer $n \in \mathbb{N}_0$,

> "Se um conjunto tem ***n*** elementos então o cunjunto das suas partes tem $\boldsymbol{2^n}$ elementos".

Efectua-se a demonstração por indução em n.

(1) Para n=0 tem-se $X = \emptyset$ e $\mathcal{P}(X) = \{\emptyset\}$ pelo que $|\mathcal{P}(X)| = 1 = 2^0$.

(2) Suponha-se agora que todo o conjunto Y com n elementos tem $|\mathcal{P}(Y)| = 2^n$ e mostre-se que se X tem n+1 elementos então

$$|\mathcal{P}(X)| = 2^{n+1}$$

(2) Suponha-se agora que todo o conjunto Y com n elementos tem $|\mathcal{P}(Y)| = 2^n$ e mostre-se que se X tem n+1 elementos então $|\mathcal{P}(X)| = 2^{n+1}$

Hipótese

Tese

Ora, se X tem *n* elementos então

$$X=\{x_1, x_2, \ldots, x_n, x_{n+1}\}.$$

Sendo $Y=\{x_1, x_2, \ldots, x_n\}$, tem-se que

$$|Y| = n,$$

pelo que por hipótese de indução,

$$|\mathcal{P}(Y)| = 2^n$$

Como $\mathcal{P}(X) = \mathcal{P}(Y) \cup \{Z \cup \{x_{n+1}\} : Z \in \mathcal{P}(Y)\}$ temos

$$|\mathcal{P}(X)| = |\mathcal{P}(Y)| + \left|\{Z \cup \{x_{n+1}\} : Z \in \mathcal{P}(Y)\}\right|$$

$$= 2^n + 2^n = 2 \cdot 2^n = 2^{n+1} \qquad \text{c.q.d.}$$

1.2 Funções

Sejam X e Y dois conjuntos.

Uma aplicação (ou função) de X em Y

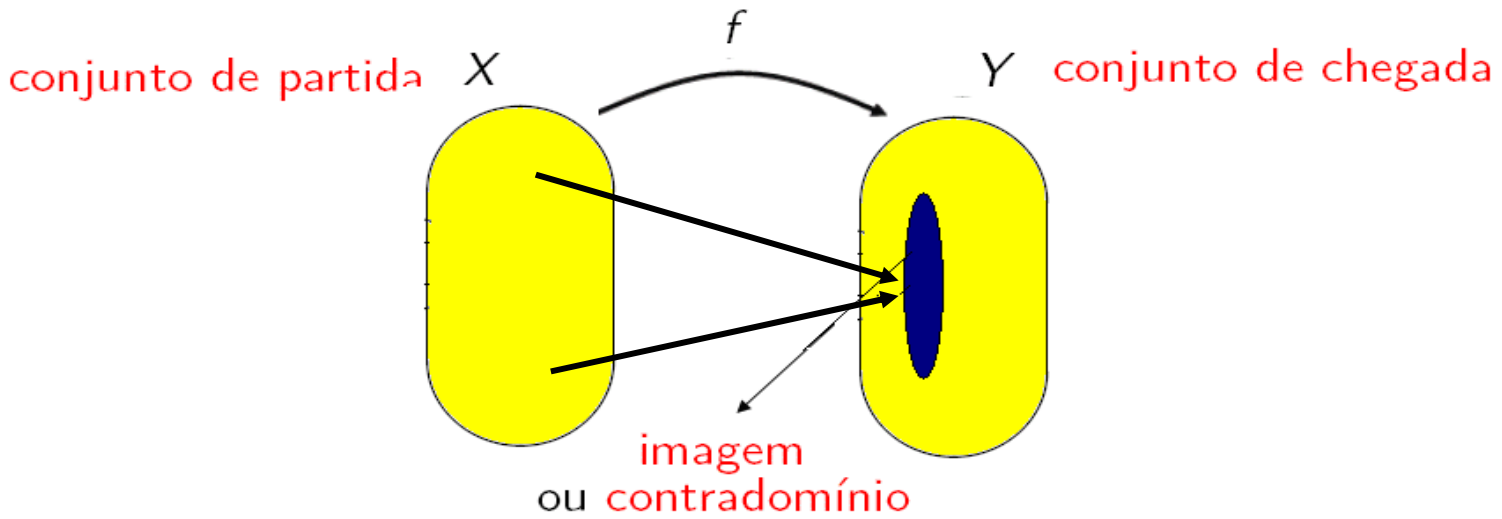
$$f : X \longrightarrow Y$$

é uma relação R de X em Y

$$R = \{(x, y) \in X \times Y : \ y = f(x)\}$$

verificando:

$$(\forall x \in X)\ (\exists^1 y \in Y)\ (x, y) \in R.$$



1.2 Funções

Sejam X e Y dois conjuntos.

Uma aplicação (ou função) de X em Y

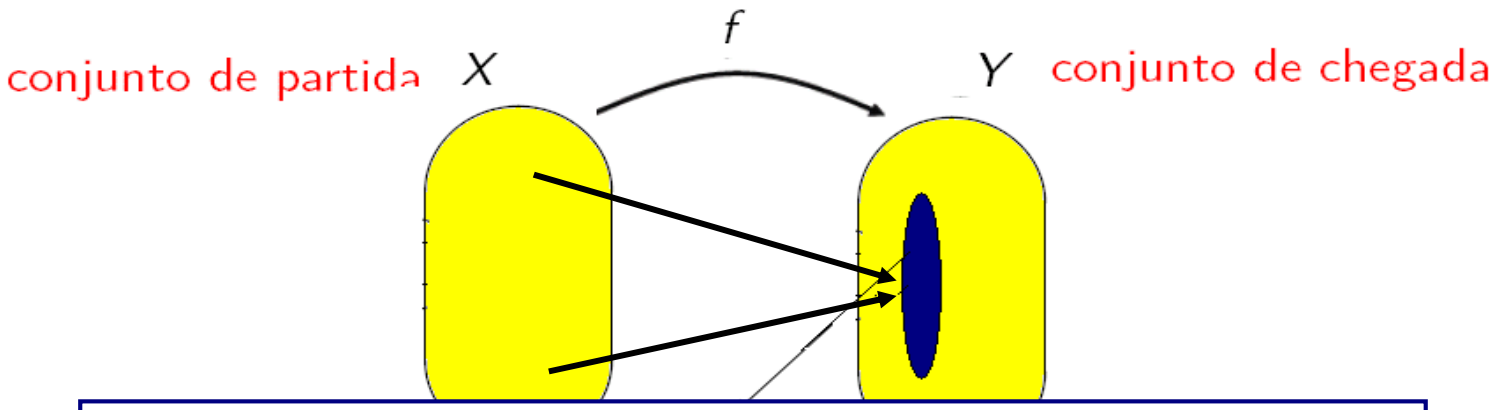
$$f : X \longrightarrow Y$$

é uma relação R de X em Y

$$R = \{(x, y) \in X \times Y : \ y = f(x)\}$$

verificando:

$$(\forall x \in X)\ (\exists^1 y \in Y)\ (x, y) \in R.$$

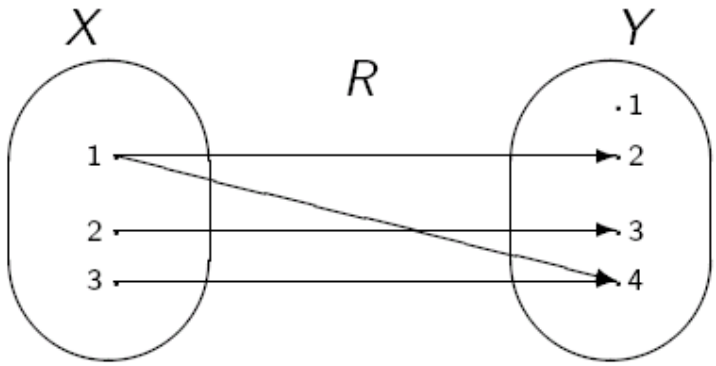


$$Im\, f = \{f(x) \mid x \in X\} = \{y \in Y \mid (\exists x \in X)\ y = f(x)\}.$$

Exemplos:

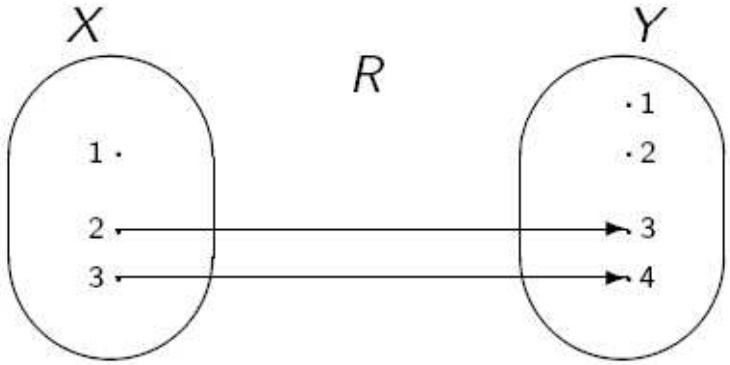
1. Sejam $X = \{1,\ 2,\ 3\}$ e $Y = \{1,\ 2,\ 3,\ 4\}$. Então:

   - $R = \{(1,2),\ (2,3),\ (3,4),\ (1,4)\}$ é uma relação de X em Y,



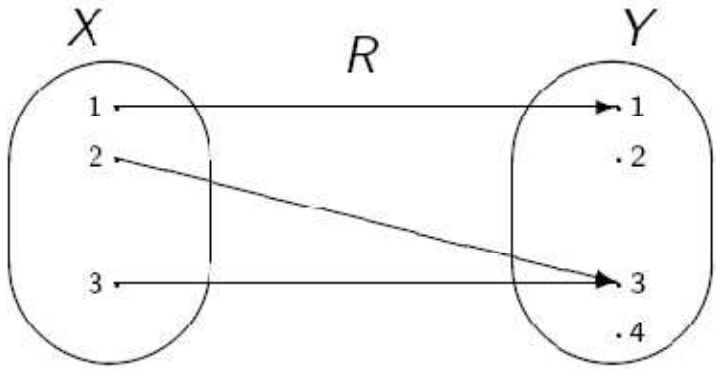
   mas não é uma aplicação de X em Y.

   - $R = \{(2,3),\ (3,4)\}$ é uma relação de X em Y,



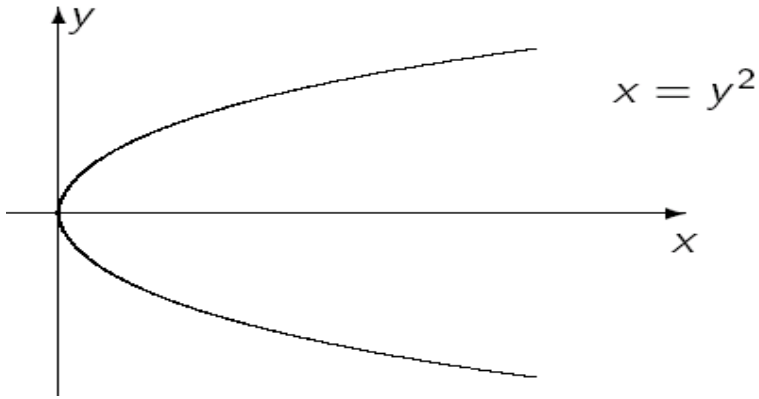
   mas não é uma aplicação de X em Y.

- $R = \{(1,1),\ (2,3),\ (3,3)\}$ é uma aplicação de X em Y.

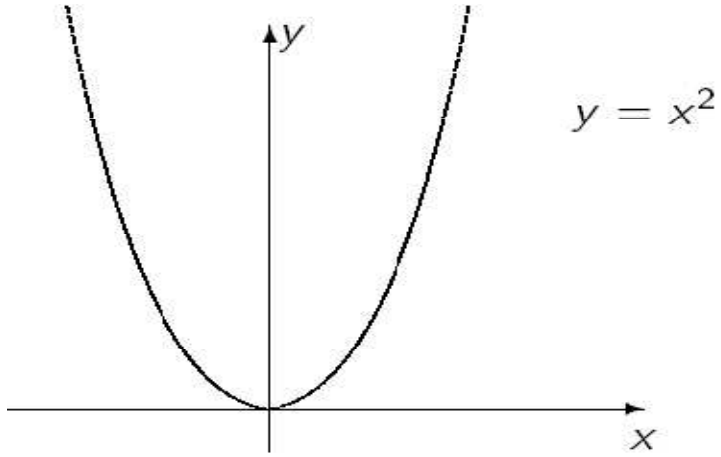


2. Sejam $X = Y = \mathbb{R}$. Então:

- $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} :\ x = y^2\}$ é uma relação de $\mathbb{R}$ em $\mathbb{R}$, mas não é uma aplicação de $\mathbb{R}$ em $\mathbb{R}$.



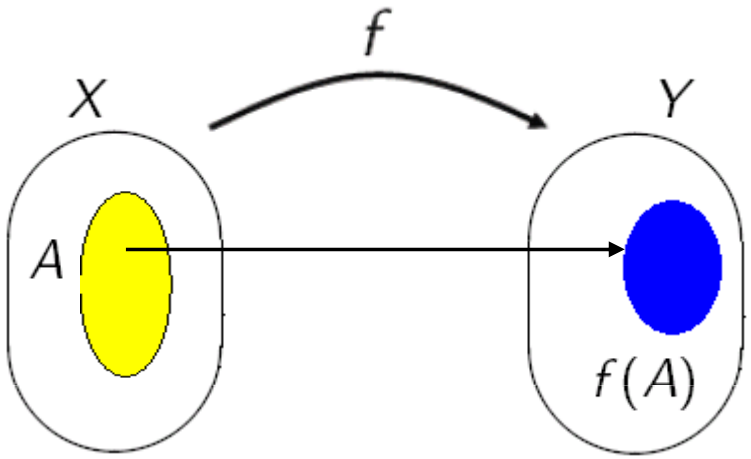
- $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ x^2 = y\}$ é uma aplicação de $\mathbb{R}$ em $\mathbb{R}$.

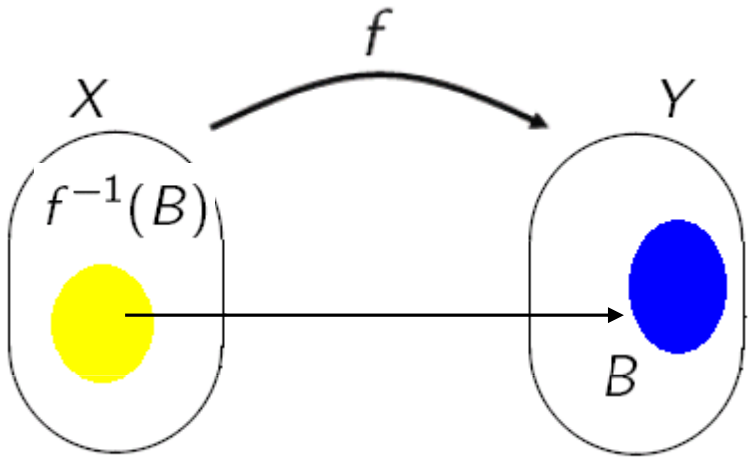


Definição 1.2.1:

Sejam $f : X \longrightarrow Y$ uma aplicação, $A \subseteq X$ e $B \subseteq Y$.

- imagem de A (por meio de f) ao conjunto $f(A) = \{f(x) \mid x \in A\}$;





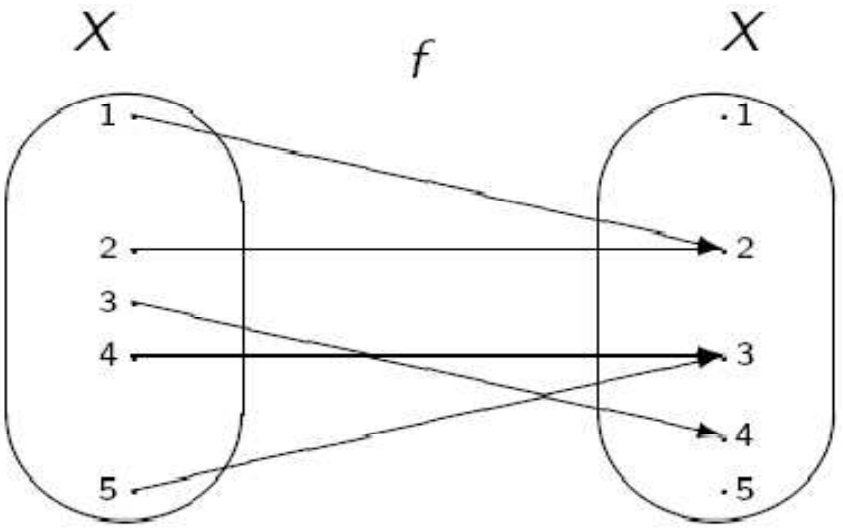
- imagem recíproca (ou pré-imagem) de B (por meio de f) ao conjunto

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}.$$

Exemplos:

Sejam $X = \{1,\ 2,\ 3,\ 4,\ 5\}$, $f : X \longrightarrow X$ tal que

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 2 & 4 & 3 & 3 \end{pmatrix},$$



É aplicação

- $Im\, f = \{2,\ 3,\ 4\}$
- $A = \{1,\ 2,\ 3\} \Rightarrow f(A) = \{2,\ 4\}$
- $B = \{1,\ 2,\ 3\}$
  $\Rightarrow \quad f^{-1}(B) = \{1,\ 2,\ 4,\ 5\}$
- $f(f^{-1}(B)) = \{2,\ 3\} \subset B$

Definição 1.2.2:

Seja $f : X \longrightarrow Y$ uma aplicação. Dizemos que:

1. f é injectiva se

$$\forall a,\ b \in X,\ a \neq b \Rightarrow f(a) \neq f(b)$$

(equivalentemente, se $\forall a,\ b \in X,\ f(a) = f(b) \Rightarrow a = b$);

2. f é sobrejectiva se $f(X) = Y$, isto é, se

$$\forall y \in Y\ \exists x \in X :\ y = f(x);$$

3. f é bijectiva se for simultaneamente injectiva e sobrejectiva

Exemplos:

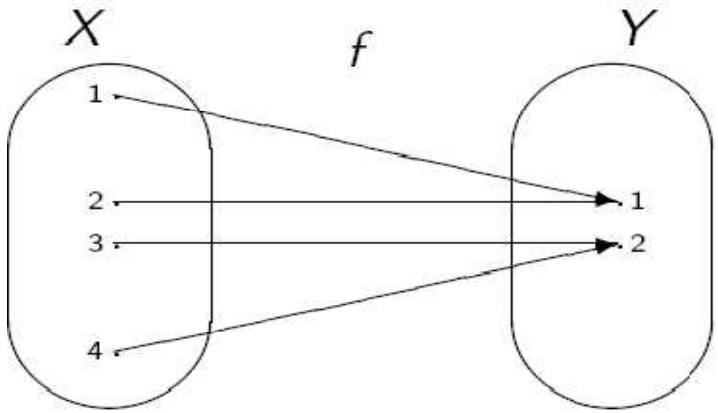
1. A aplicação $f : X \longrightarrow X$ $\qquad X = \{1, 2, 3, 4, 5\}$

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 2 & 4 & 3 & 3 \end{pmatrix}$$

não é injectiva nem sobrejectiva.

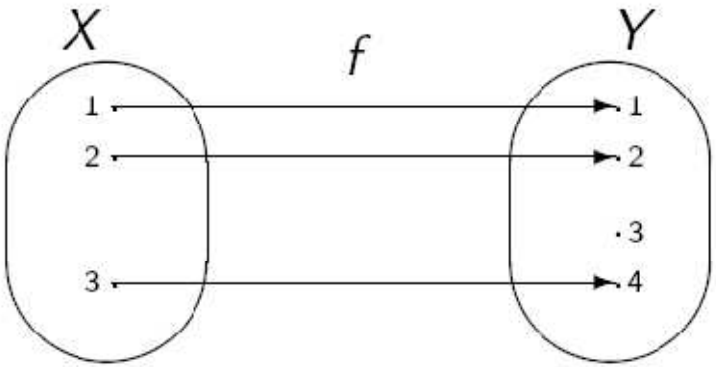
2. A aplicação $f : \mathbb{N} \longrightarrow \mathbb{N}$ definida por $f(n) = n + 1$ para qualquer $n \in \mathbb{N}$ é injectiva e não é sobrejectiva.

3. Sejam $X = \{1, 2, 3, 4\}$, $Y = \{1, 2\}$



f é sobrejectiva e não é injectiva.

4. Sejam $X = \{1,\ 2,\ 3\}$, $Y = \{1,\ 2,\ 3,\ 4\}$ e $f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 4 \end{pmatrix}$ uma aplicação de X em Y.



f é injectiva e não é sobrejectiva.

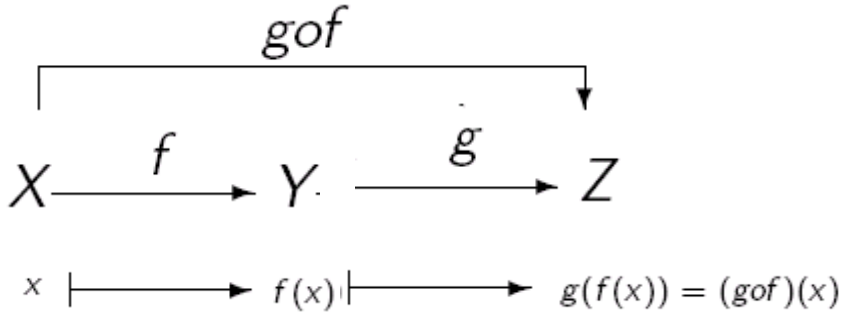
5. Seja X um conjunto qualquer e $f : X \longrightarrow X$ a aplicação definida por

$$f(x) = x, \text{ para qualquer } x \in X.$$

Então, f é injectiva e sobrejectiva, donde f é bijectiva.

aplicação identidade de X

$f = 1_X$ ou id_X ou I_X



Teorema 1.2.3:

Sejam $f : X \longrightarrow Y$ *e* $g : Y \longrightarrow Z$ *duas aplicações. Então a relação composição de* g *com* f *de* X *em* Z

$$gof : X \longrightarrow Z$$

é uma aplicação que está definida por

$$(gof)(x) = g(f(x)), \text{ para qualquer } x \in X.$$

Observações: Sejam $f : X \longrightarrow Y$ e $g : Y \longrightarrow Z$ duas aplicações.

1. A composta fog está definida se, e só se, $Z = X$;
2. Se $Z = X$ (as aplicações fog e gof estão definidas) não temos necessariamente $fog = gof$.

Exemplo: Sejam $X = \{1, 2, 3\}$

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

duas aplicações de X em X. Então,

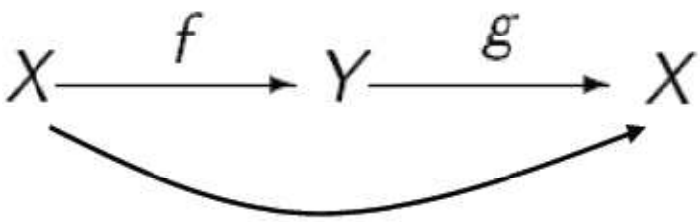
$$fog = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = gof.$$

Teorema 1.2.4:
Sejam $f : X \longrightarrow Y$ *e* $g : Y \longrightarrow Z$ *duas aplicações. Então:*

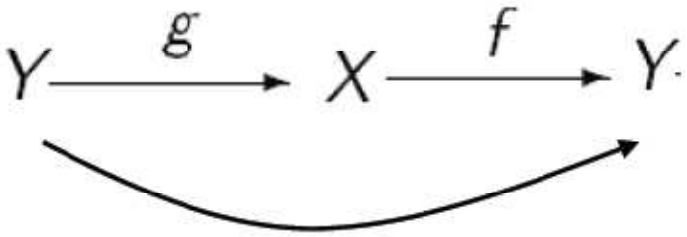
1. *Se* f *e* g *são injectivas, então* gof *é injectiva;*
2. *Se* f *e* g *são sobrejectivas, então* gof *é sobrejectiva;*
3. *Se* f *e* g *são bijectivas, então* gof *é bijectiva.*

Funções invertíveis:

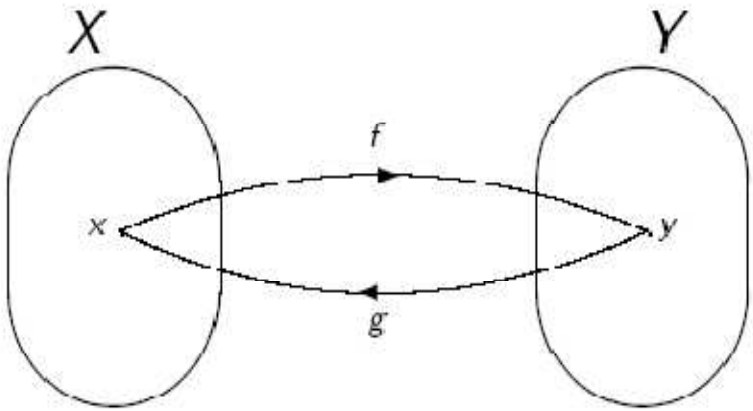
Dizemos que uma aplicação $f : X \longrightarrow Y$ é invertível se existir uma aplicação $g : Y \longrightarrow X$ tal que



$gof = id_X$ e



$fog = id_Y$



Teorema 1.2.5:

Seja $f : X \longrightarrow Y$ *uma aplicação invertível. Então, existe uma e uma só aplicação* $g : Y \longrightarrow X$ *tal que*

$$gof = id_X \qquad e \qquad fog = id_Y .$$

f^{-1} *aplicação inversa de* f

Teorema 1.2.6:

Sejam $f : X \longrightarrow Y$ *e* $g : Y \longrightarrow Z$ *duas aplicações invertíveis. Então, a aplicação* $gof : X \longrightarrow Z$ *é invertível, tendo-se*

$$(gof)^{-1} = f^{-1}og^{-1}.$$

Teorema 1.2.7:

Uma aplicação $f : X \longrightarrow Y$ *é invertível se, e só se, é bijectiva.*

1.3 Divisibilidade

Teorema 1.3.1 (Algoritmo da Divisão)

Sejam $n, m \in \mathbb{Z}$ tais que $m \neq 0$. Então, existem dois únicos inteiros q e r tais que

$$n = mq + r,$$

Resto

Quociente

com $0 \leq r < |m|$.

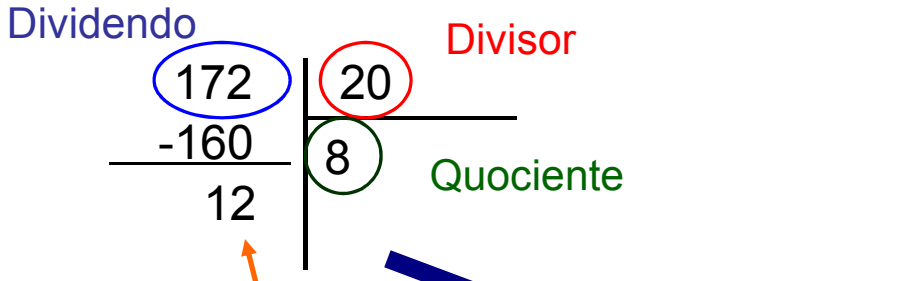
Exemplo:

- n= 172, m= 20

  Então, 172= 20x8+12

  r

  q



172 =20x8 +12

- n= 172, m= -20

  172= 20x8+12 ⇒ 172= -20x(-8)+12

  r

  q

1.3 Divisibilidade

Teorema 1.3.1 (Algoritmo da Divisão)

Sejam $n, m \in \mathbb{Z}$ tais que $m \neq 0$. Então, existem dois únicos inteiros q e r tais que

$$n = mq + r,$$

Resto

Quociente

com $0 \leq r < |m|$.

Exemplo:

- n= 172, m= 20

  Então, 172= 20x8+12 (r, q)

- n= 172, m= -20

  172= 20x8+12 $\Rightarrow$ 172= -20x(-8)+12 (r, q)

- n= -172, m= 20

  172= 20x8+12 $\Rightarrow$ -172= -20x8 -12

  $\Downarrow$

  -172= 20x(-8) -12

  $\Downarrow$

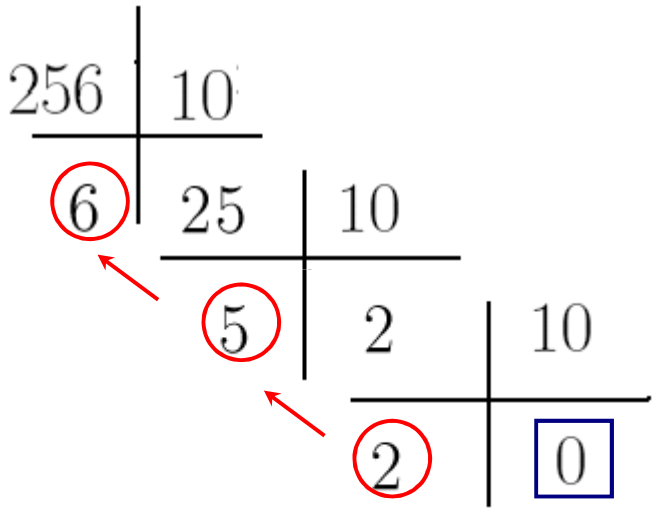
  -172= 20x(-8) -12 +20-20

  $\Downarrow$

  -172= 20x(-9) +8 (r, q)

Sistema Decimal:

$$x = 256 = 2 \times 10^2 + 5 \times 10^1 + 6 \times 10^0$$

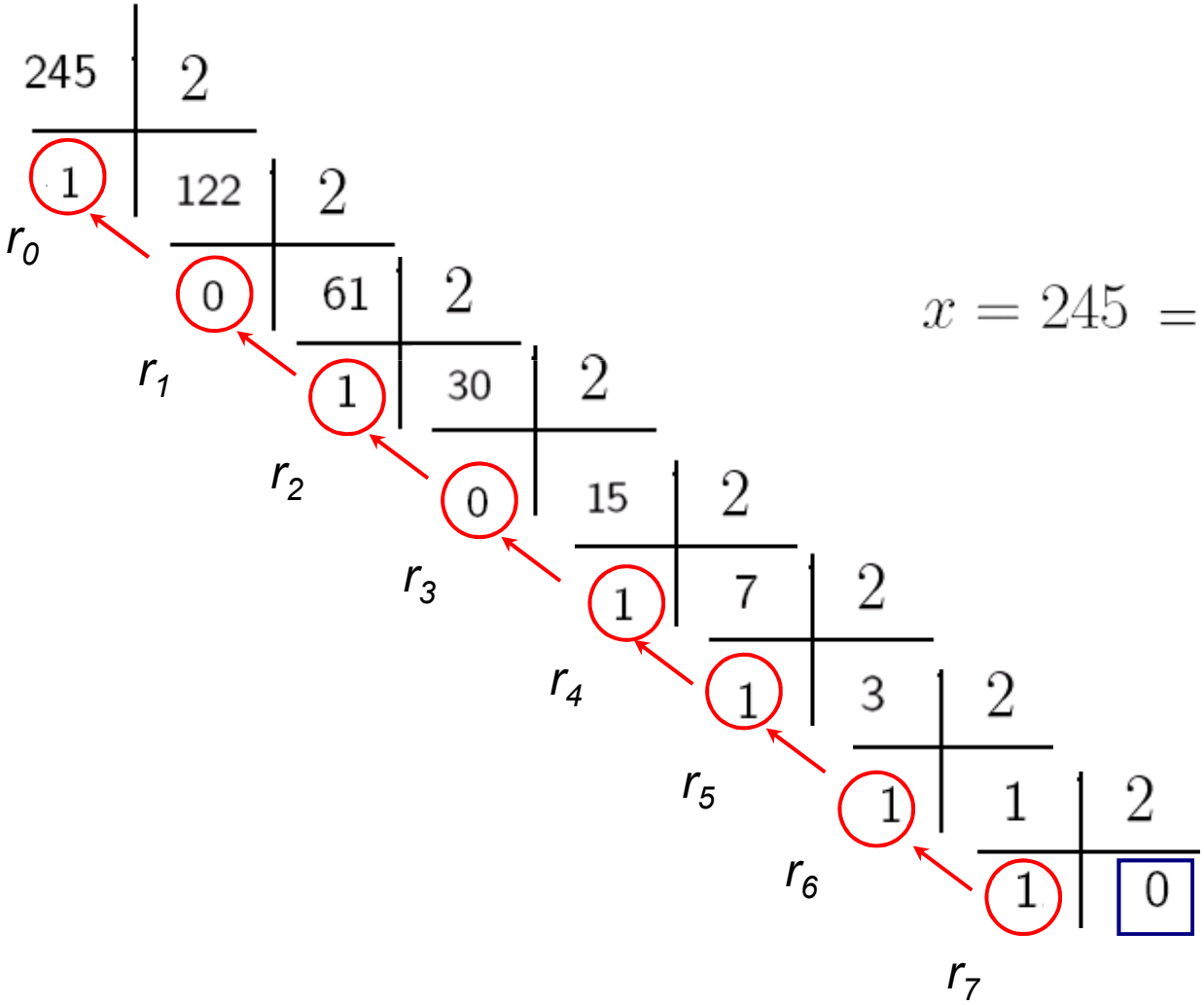


$256 = (2)\,(5)\,(6)$

Sistema Binário:

$$x = 245 = r_k 2^k + r_{k-1} 2^{k-1} + r_{k-2} 2^{k-1} + \ldots + r_1 2^1 + r_0 2^0$$

? ? ? ? ?



$$x = 245 = (11110101)_2$$

Geralmente:

O algoritmo da divisão justifica a representação usual dos inteiros.

Seja $t \geq 2$ um inteiro. Sendo x um inteiro positivo,

$$x = tq_0 + r_0, \text{ com } 0 \leq r_0 < t \quad \text{(Algoritmo da Divisão)}$$

$$q_0 = tq_1 + r_1, \text{ com } 0 \leq r_1 < t \quad \text{(Algoritmo da Divisão)}$$

$$\vdots$$

$$q_{k-2} = tq_{k-1} + r_{k-1}, \text{ com } 0 \leq r_{k-1} < t \quad \text{(Algoritmo da Divisão)}$$

$$q_{k-1} = tq_k + r_k, \text{ com } 0 \leq r_k < t. \quad \text{(Algoritmo da Divisão)}$$

$$\| \\ 0$$

(Tem-se que $0 \leq q_{k-2} < \ldots < q_2 < q_1 < q_0 < x$)

O processo termina quando $q_k = 0$. $\boxed{q_{k-1} = r_k}$

Eliminando os quocientes q_i, obtemos

$x = tq_0 + r_0$, com $0 \leq r_0 < t$ (Algoritmo da Divisão)

$q_0 = tq_1 + r_1$, com $0 \leq r_1 < t$ (Algoritmo da Divisão)

$\vdots$

$q_{k-2} = tq_{k-1} + r_{k-1}$, com $0 \leq r_{k-1} < t$ (Algoritmo da Divisão)

$q_{k-1} = tq_k + r_k$, com $0 \leq r_k < t$. (Algoritmo da Divisão)

O processo termina quando $q_k = 0$.

Eliminando os quocientes q_i, obtemos $\boxed{q_{k-1} = r_k}$

$$q_{k-2} = r_k t + r_{k-1}$$
$$q_{k-3} = r_k t^2 + r_{k-1} t + r_{k-2}$$
$$\vdots$$
$$q_0 = r_k t^{k-1} + r_{k-1} t^{k-2} + \ldots + r_1$$

$$\boxed{x = r_k t^k + r_{k-1} t^{k-1} + \ldots + r_1 t + r_0.}$$

$\boxed{x = (r_k r_{k-1} \ldots r_1 r_0)_t}$

Representação base t

Relação de Divisibilidade

$X = \mathbb{Z}$. Considere a relação | definida por: a, b $\in \mathbb{Z}$

$$a|b \text{ (} a \text{ divide } b\text{)} \iff (\exists k \in \mathbb{Z})\ b = ak$$

b é múltiplo de a

(a é divisor de b)

Observação:

- $(\mathbb{N}, |)$ é um c.p.o..
- $(\mathbb{Z}, |)$ não é c.p.o.. A relação não é anti-simétrica em $\mathbb{Z}$

Máximo divisor comum

Dados dois números inteiros não nulos a e b, denotamos por

$$\boxed{\text{mdc}\{a, b\}}$$

o seu máximo divisor comum.

Definição 1.3.2

Dados dois números inteiros não nulos a e b, chama-se

máximo divisor comum *de a e b*

ao número natural d (caso exista), tal que:

1. $d|a$ e $d|b$;
2. *Se* $c \in \mathbb{Z}$ *é tal que* $c|a$ *e* $c|b$ *então* $c|d$.

Exemplos:

- $mdc\{6, 9\} = 3$ pois:
  1. $3|6$ e $3|9$
  2. Se $c|6$ e $c|9$ então

$$\Updownarrow \qquad \Updownarrow$$

$$6 = ck_1 \qquad 9 = ck_2 \qquad k_1, k_2 \in \mathbb{Z}$$

Logo,

$$3 = 9 - 6 = ck_2 - ck_1 = c\underbrace{(k_2 - k_1)}_{k_3}$$

ou seja, $c|3$

- $mdc\{6,-9\} = mdc\{6,9\} = 3$
- $mdc\{51975,\ 31752\} =$ **?**

51975	3 ←
17325	3 ←
5775	5
1155	3 ←
385	5
77	11
7	7 ←
1	

31752	2
15876	2
7938	2
3969	3 ←
1323	3 ←
441	3 ←
147	3
49	7 ←
7	7
1	

Decompor em factores Primos

$$mdc\{51975,\ 31752\} =$$
$$= 3 \times 3 \times 3 \times 7 = 189$$

Muitos cálculos

Decompor em factores Primos

Algoritmo de Euclides (300 a.c.)

Teorema 1.3.3: (Existência e unicidade do mdc**)**

Dados dois números inteiros não nulos a e b, existe um único número natural d (designado por máximo divisor comum *de a e b) tal que:*

1. $d|a$ e $d|b$;
2. *Se* $c \in \mathbb{Z}$ *é tal que* $c|a$ *e* $c|b$ *então* $c|d$.

Demonstração. [Algoritmo de Euclides] Determinamos sucessivamente os inteiros q_i e r_i, $1 \leq i \leq k+1$ (com $k \geq 2$), tais que

$$a = bq_1 + r_1 , \qquad 0 < r_1 < |b| ,$$ (Algoritmo da Divisão)

$$b = r_1 q_2 + r_2 , \qquad 0 < r_2 < r_1 ,$$ (Algoritmo da Divisão)

$$r_1 = r_2 q_3 + r_3 , \qquad 0 < r_3 < r_2 ,$$ (Algoritmo da Divisão)

$$r_2 = r_3 q_4 + r_4 , \qquad 0 < r_4 < r_3 ,$$ (Algoritmo da Divisão)

$$\vdots$$

$$a = bq_1 + r_1 , \qquad 0 < r_1 < |b| ,$$ (Algoritmo da Divisão)

$$b = r_1 q_2 + r_2 , \qquad 0 < r_2 < r_1 ,$$ (Algoritmo da Divisão)

$$r_1 = r_2 q_3 + r_3 , \qquad 0 < r_3 < r_2 ,$$ (Algoritmo da Divisão)

$$r_2 = r_3 q_4 + r_4 , \qquad 0 < r_4 < r_3 ,$$ (Algoritmo da Divisão)

$$\vdots$$

$$r_{k-2} = r_{k-1} q_k + r_k , \qquad 0 < r_k < r_{k-1} ,$$ (Algoritmo da Divisão)

$mdc\{a, b\}$

$$r_{k-1} = r_k q_{k+1} , \qquad r_{k+1} = 0 .$$ (Algoritmo da Divisão)

Nestas condições, $d = r_k$ verifica as condições (1) e (2) do teorema e é único.

1. $d|a$ e $d|b$;
2. *Se* $c \in \mathbb{Z}$ *é tal que* $c|a$ e $c|b$ *então* $c|d$.

Exemplo: Utilizar o algoritmo de Euclides para calcular $mdc\{51975,\ 31752\}$

$$51975 = 31752 \cdot 1 + 20223 \quad \text{(Algoritmo da Divisão)}$$

$$31752 = 20223 \cdot 1 + 11529 \quad \text{(Algoritmo da Divisão)}$$

$$20223 = 11529 \cdot 1 + 8694 \quad \text{(Algoritmo da Divisão)}$$

$$11529 = 8694 \cdot 1 + 2835 \quad \text{(Algoritmo da Divisão)}$$

$$8694 = 2835 \cdot 3 + \boxed{189} \quad \text{(Algoritmo da Divisão)}$$

$$2835 = 189 \cdot 15 + \boxed{0.} \quad \text{(Algoritmo da Divisão)}$$

Assim, $\text{mdc}\{51975, 31752\} = \boxed{189.}$

Igualdade de Bezout

$189 = \text{mdc}\{51975, 31752\}$

$51975 = 31752 \cdot 1 + 20223$ ←
$31752 = 20223 \cdot 1 + 11529$ ←
$20223 = 11529 \cdot 1 + 8694$ ←
$11529 = 8694 \cdot 1 + 2835$ ←
$8694 = 2835 \cdot 3 + 189$ ←
$2835 = 189 \cdot 15 + 0$

$$
\begin{aligned}
189 &= 8694 - 2835 \cdot 3 \\
&= 8694 - (11529 - 8694) \cdot 3 \\
&= 8694 \cdot 4 - 11529 \cdot 3 \\
&= (20223 - 11529) \cdot 4 - 11529 \cdot 3 \\
&= 20223 \cdot 4 - 11529 \cdot 7 \\
&= 20223 \cdot 4 - (31752 - 20223) \cdot 7 \\
&= 20223 \cdot 11 - 31752 \cdot 7 \\
&= (51975 - 31752) \cdot 11 - 31752 \cdot 7 \\
&= 51975 \cdot 11 - 31752 \cdot 18 \ .
\end{aligned}
$$

Coeficientes da igualdade de Bezout

Assim $\underbrace{189}_{\text{mdc\{a,b\}}} = \underbrace{51975}_{a} \cdot \mathbf{11} + \underbrace{31752}_{b} \cdot (-\mathbf{18})$.

mdc{a,b}= am + bn

Teorema 1.3.4: (Igualdade de Bezout)

Dados dois números inteiros não nulos a e b, existem números inteiros m e n (designados por coeficientes da Igualdade de Bezout*) tais que*

$$\text{mdc}\{a, b\} = am + bn.$$

Demonstração. Seja $d = \text{mdc}\{a, b\}$. Pelo Algoritmo de Euclides, temos

$$\begin{aligned} a &= bq_1 + r_1 \ , \quad 0 < r_1 < |b| \\ b &= r_1 q_2 + r_2 \ , \quad 0 < r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3 \ , \quad 0 < r_3 < r_2 \end{aligned} \tag{1}$$

$$\dots$$

$$r_{k-2} = r_{k-1} q_k + d \ , \quad 0 < d = r_k < r_{k-1},$$

para certo $k \in \mathbb{N}$. Então, $d - r_{k-2} - r_{k-1} q_k \quad (*)$ e, mais geralmente, para $i \in \{1, \dots, k\}$, $r_i = r_{i-2} - r_{i-1} q_i \quad (**)$ (tomando $r_0 = b$ e $r_{-1} = a$). Assim, partindo de $(*)$ e substituindo sucessivamente cada r_i usando $(**)$, obtemos d como *combinação linear* de a e de b. □

Observação

Os coeficientes da Igualdade de Bezout, para dois números inteiros não nulos dados, não são únicos. Por exemplo, $1 = \text{mdc}\{2, 3\}$ e temos

$$1 = 2 \cdot (-1) + 3 \cdot 1 = 2 \cdot 2 + 3 \cdot (-1) = 2 \cdot (-4) + 3 \cdot 3 = \cdots \ .$$

.

Mínimo múltiplo comum

Dados dois números inteiros não nulos a e b, denotamos por

$$\boxed{\text{mmc}\{a,\ b\}}$$

o seu mínimo múltiplo comum.

Teorema 1.3.4: (Existência e unicidade do mmc**)**

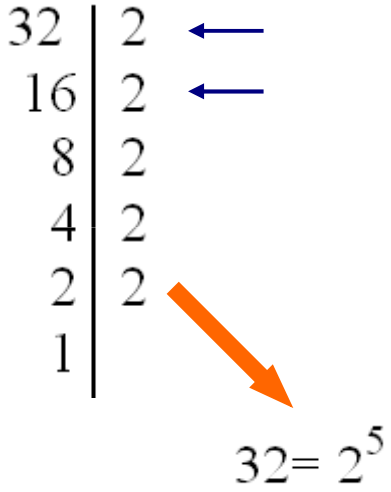
Dados dois números inteiros não nulos a e b, existe um único número natural m (designado por mínimo múltiplo comum de a e b) tal que:

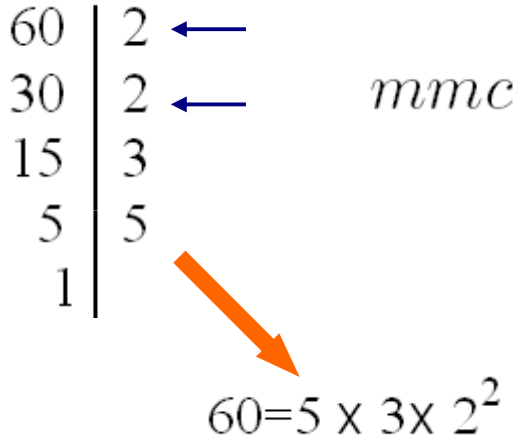
1. $a|m$ e $b|m$; (m é múltiplo de a e b)
2. *Se* $c \in \mathbb{Z}$ *é tal que* $a|c$ *e* $b|c$ *então* $m|c$. (m é o menor múltiplo de a e b, positivo)

Exemplos:

- $mmc\{6, 9\} = 18 = mmc\{-6, 9\}$
- $mmc\{32, 60\} =$ **?**

Decompor em factores Primos





$mmc\{32, 60\} = 5 \times 3 \times 2^5$

$= 480$

(Factores diferentes
e
Factores comuns
com maior grau)

Recordar:

$mdc\{32, 60\} = 2 \times 2 = 4$ (Factores comuns com menor grau)

- $mmc\{32060, 31652\} =$ **?**

Decompor em factores Primos

32060	2
16030	2
8015	5
1603	7
229	?

!!!!!!!

- $mmc\{32060, 31652\} = ?$

Decompor em factores Primos

32060	2
16030	2
8015	5
1603	7
229	229
1	

31652	2
15826	2
7913	41
193	193
1	

$31652 = 193 \times 41 \times 2^2$

$32060 = 229 \times 5 \times 7 \times 2^2$

$mmc\{32060, 31652\} =$

$= 229 \times 5 \times 7 \times 193 \times 41 \times 2^2$

$= 253690780.$

Teorema 1.3.5: *Dados dois inteiros não nulos a e b, então*

$$\text{mmc}\{a,\ b\} = \frac{|ab|}{\text{mdc}\{a,\ b\}}.$$

- $mmc\{32060, 31652\} = ?$

Recorrendo ao algoritmo de Euclides

$$\begin{aligned}
32060 &= 31652 \times 1 + 408 \\
31652 &= 408 \times 77 + 236 \\
408 &= 236 \times 1 + 172 \\
236 &= 172 \times 1 + 64 \\
172 &= 64 \times 2 + 44 \\
64 &= 44 \times 1 + 20 \\
44 &= 20 \times 2 + \boxed{4} \\
20 &= 4 \times 5 + 0\ ,
\end{aligned}$$

$$\begin{aligned}
mmc\{32060, 31652\} &= \\
&= \frac{32060 \times 31652}{4} \\
&= 253690780.
\end{aligned}$$

- $mmc\{32060, 31652\} = ?$

32060	2
16030	2
8015	5
1603	7
229	229
1	

31652	2
15826	2
7913	41
193	193
1	

$31652 = 193 \times 41 \times 2^2$

$32060 = 229 \times 5 \times 7 \times 2^2$

$mdc\{32060, 31652\} = 2^2$

$$\frac{32060 \times 31652}{4} = \frac{(229 \times 5 \times 7 \times 2^2)(193 \times 41 \times 2^2)}{4}$$

$$= 229 \times 5 \times 7 \times 193 \times 41 \times 2^2 = mmc\{32060, 31652\}$$

Definição 1.3.6:

1. Um número inteiro p diz-se *primo* se $p > 1$ e p apenas possui como divisores positivos 1 e p.

2. Dois números inteiros não nulos a e b dizem-se *primos entre si* se

$$\text{mdc}\{a, b\} = 1.$$

Curiosidades:

- Estudados, desde a antiguidade. Nomeadamente, quanto à procura de uma regularidade ou lei de formação destes números. Mas, passado milénios, os matemáticos ainda não a descobriram. Um facto que está provado é que são em número infinito (Euclides, no século III a.c.).

- No século III antes da nossa era, o matemático grego Eratóstenes "inventou" um método, ainda actual, que permite determinar os números primos inferiores a um dado número. A este método dá-se o nome de Crivo de Eratóstenes.

- No século III antes da nossa era, o matemático grego Eratóstenes inventou um método, ainda actual, que permite determinar os números primos inferiores a um dado número. A este método dá-se o nome de Crivo de Eratóstenes.

Números primos inferiores a 100

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Definição 1.3.6:

1. Um número inteiro p diz-se *primo* se $p > 1$ e p apenas possui como divisores positivos 1 e p.

2. Dois números inteiros não nulos a e b dizem-se *primos entre si* se

$$\text{mdc}\{a, b\} = 1.$$

Observações:

(0) 0 e 1 não são primos;

(1) O número 2 é o único primo que é par;

(2) Se a|b e a|c então a|(b+c);

(3) Se a|b então a|(kb), com k inteiro;

(4) Se a é primo e $a \nmid b$ então mdc{a, b}=1.

Lema

Sejam a e b dois números inteiros não nulos e primos entre si. Seja $c \in \mathbb{Z}$ tal que $a|bc$. Então $a|c$.

Demonstração. Atendendo à Igualdade de Bezout, existem inteiros m e n tais que

$$1 = am + bn.$$

Donde $c = amc + bnc$. Como $a|bc$, então em particular $a|bnc$. Além disso, claramente, $a|amc$. Logo $a|(amc + bnc)$, ou seja, $a|c$. □

Lema

Seja p um número primo e sejam $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ (com $n \in \mathbb{N}$) tais que $p|a_1 a_2 \cdots a_n$. Então $p|a_i$, para algum $i \in \{1, \ldots, n\}$.

Demonstração. Por indução em n. Para $n = 1$ é imediato. Admitamos então o resultado válido para $n-1$, para certo $n > 1$. Sejam $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ tais que $p|a_1 a_2 \cdots a_n$. Ora, se $p|a_1 a_2 \cdots a_{n-1}$, por hipótese de indução, $p|a_i$, para algum $i \in \{1, \ldots, n-1\}$. Se, pelo contrário $p \not| a_1 a_2 \cdots a_{n-1}$, então

$$\text{mdc}\{p, a_1 a_2 \cdots a_{n-1}\} = 1,$$

visto que p é um número primo. Neste caso, pelo lema anterior, deduzimos que $p|a_n$. □

Teorema 1.3.7: (Teorema Fundamental da Aritmética)

Todo o número inteiro maior do que um pode ser escrito como um produto de números primos (com um só factor, no caso do número ser primo). Além disso, uma tal decomposição em números primos é essencialmente única, i.e. duas decomposições apenas diferem na ordem pela qual os primos são escritos.

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}, \qquad p_1, p_2, \ldots, p_k \text{ são números primos}$$

Exemplo: Escrever n=51975 como o produto de números primos.

Decompor em factores primos

51975	3
17325	3
5775	5
1155	3
385	5
77	11
7	7
1	

51975 = 3x3x3x5x5x11x7

$= 3^3.5^2.11.7 = 5^2.3^3.\ 7.11$

$= 3^3.5^2.\ 7.11$

forma standard de n

(Base crescente)

Teorema 1.3.7: (Teorema Fundamental da Aritmética)

Todo o número inteiro maior do que um pode ser escrito como um produto de números primos (com um só factor, no caso do número ser primo). Além disso, uma tal decomposição em números primos é essencialmente única, i.e. duas decomposições apenas diferem na ordem pela qual os primos são escritos.

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}, \qquad p_1, p_2, \ldots, p_k \text{ são números primos}$$

Exemplo: Escrever n=51975 como o produto de números primos.

Decompor em factores primos

51975	3
17325	3
5775	5
1155	3
385	5
77	11
7	7
1	

51975 = 3x3x3x5x5x11x7

$= 3^3.5^2.11.7 = 5^2.3^3.\ 7.11$

$= 3^3.5^2.\ 7.11$

forma standard de n

(Base crescente)

Teorema 1.3.8:

Sejam

$$m = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k} \quad e \quad n = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$$

($k \in \mathbb{N}$), em que $p_1 < p_2 < \cdots < p_k$ são números primos e s_i e t_i são números inteiros não negativos, para $i = 1, 2, \ldots, k$. Sejam

$$u_i = min\{s_i, t_i\} \quad e \quad v_i = max\{s_i, t_i\},$$

para qualquer $i = 1, 2, \ldots, k$. Então:

1. $mdc\{m, n\} = p_1^{u_1} p_2^{u_2} \cdots p_k^{u_k}$;
2. $mmc\{m, n\} = p_1^{v_1} p_2^{v_2} \cdots p_k^{v_k}$.

Exemplo:

$mmc\{32, 60\} =$

32	2
16	2
8	2
4	2
2	2
1	

$32 = 2^5$

$mdc\{32, 60\} =$

60	2
30	2
15	3
5	5
1	

$60 = 2^2 \times 3 \times 5$

Teorema 1.3.8:

Sejam

$$m = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k} \quad e \quad n = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$$

($k \in \mathbb{N}$), em que $p_1 < p_2 < \cdots < p_k$ são números primos e s_i e t_i são números inteiros não negativos, para $i = 1, 2, \ldots, k$. Sejam

$$u_i = min\{s_i, t_i\} \quad e \quad v_i = max\{s_i, t_i\},$$

para qualquer $i = 1, 2, \ldots, k$. Então:

1. $mdc\{m, n\} = p_1^{u_1} p_2^{u_2} \cdots p_k^{u_k}$;
2. $mmc\{m, n\} = p_1^{v_1} p_2^{v_2} \cdots p_k^{v_k}$.

Exemplo:

$mmc\{32, 60\} = 2^5 \times 3^1 \times 5^1$

$mdc\{32, 60\} = 2^2 \times 3^0 \times 5^0$

32	2
16	2
8	2
4	2
2	2
1	

$32 = 2^5 \times 3^0 \times 5^0$

60	2
30	2
15	3
5	5
1	

$60 = 2^2 \times 3 \times 5$

Hoje em dia são conhecidos inúmeros resultados importantes sobre números primos que não permitem no entanto caracterizar todos estes números.

Teorema 1.3.9: Todo o número primo maior que 2 é da forma $4n \pm 1$, com n um natural.

Demonstração.

Seja p um número primo. Pelo algoritmo da divisão, existem inteiros m e r tais que

$$p = 4m + r, \quad 0 \leq r < 4.$$

Assim, $r = 0, 1, 2, 3$. É fácil concluir que se p é primo então $r \neq 0$ e $r \neq 2$. Se p é primo então é da forma

$$p = 4m + 1 \text{ com } m \in \mathbb{N}$$

ou

$$p = 4m + 3 = 4m + 3 - 4 + 4 = 4\underbrace{(m+1)}_{n \in \mathbb{N}} - 1. \square$$

Questão: O número 79 é primo?

Como 79=4x20-1 então o resultado anterior não permite decidir se é ou não primo.

Teorema 1.3.10:

Se $n \geq 2$ não é um número primo, então existe um número primo p tal que $p|n$ e $p^2 \leq n$.

Prova. Como $n \geq 2$ e n não é primo, então $n = pqa$, com p e q primos tais que $p \leq q$ e $a \in \mathbb{N}$. Donde $p^2 \leq pq \leq n$.

Questão: O número 79 é primo?

Se 79 não fosse primo, pela propriedade anterior, teria de existir um número primo p divisor de 79 tal que $p^2 \leq 79$. Como $11^2 = 121 > 79$, então $p \in \{2, 3, 5, 7\}$. Mas nenhum destes quatro primos é divisor de 79.

1.4 Congruências lineares

Sejam $n \in \mathbb{N}$ e R a relação de congruência módulo n (sobre $\mathbb{Z}$). X= $\mathbb{Z}$

aRb se e só se $(\exists k \in \mathbb{Z})\, a - b = kn.$

a- b é múltiplo n

$a \equiv b \pmod{n}$

a é congruente com b módulo n

É uma relação de equivalência

classe (de congruência) módulo n de $a \in \mathbb{Z}$ (classe de equivalência de a)

$$[a]_n = \{\ldots,\ a-2n,\ a-n,\ a,\ a+n,\ a+2n,\ldots\} = a + n\mathbb{Z}.$$

Exemplos: Para $n = 4$,

- $[0]_4 = \{\ldots,\ -8,\ -4,\ 0,\ 4,\ 8,\ldots\} = 4\mathbb{Z}$;
- $[1]_4 = \{\ldots,\ -7,\ -3,\ 1,\ 5,\ 9,\ldots\} = 1 + 4\mathbb{Z}$;
- $[2]_4 = \{\ldots,\ -6,\ -2,\ 2,\ 6,\ 10,\ldots\} = 2 + 4\mathbb{Z}$;
- $[3]_4 = \{\ldots,\ -5,\ -1,\ 3,\ 7,\ 11,\ldots\} = 3 + 4\mathbb{Z}$.

O conjunto quociente $\mathbb{Z}/R$ com R a relação $\equiv (\mathrm{mod}\ n)$ designa-se por

$$\mathbb{Z}/R = \mathbb{Z}_n$$

diz-se o "Conjunto dos inteiros módulo n"

Ora,

$$\mathbb{Z}_n = \{[a]_n : a \in \mathbb{Z}\} = \{[0]_n, [1]_n, [2]_n, [3]_n, \ldots, [n-1]_n\}$$

Se $a \in \mathbb{Z}$ então, aplicando o algoritmo da divisão,

$$a = nq + r, \quad 0 \leq r < n.$$

$$\Updownarrow$$

$$a - r = nq \text{ (múltiplo de n)}$$

$$\Updownarrow$$

$$a \equiv r (\mathrm{mod}\ n)$$

$$\Updownarrow$$

$$[a]_n = [r]_n$$

Teorema 1.4.1: *Seja* $n \in \mathbb{N}$.

Então cada inteiro é congruente módulo n precisamente com um dos inteiros $0,\ 1,\ 2, \ldots,\ n-1$, *i.e.*

$$\mathbb{Z}_n = \{[0]_n,\ [1]_n, \ldots,\ [n-1]_n\}.$$

Exemplo: n=4.

Qual a classe de congruência de 25?

25=4x6+1 $\Rightarrow\ [25]_4 = [1]_4$ **"25 é congruente módulo 4 com 1"**

Qual a classe de congruência de -201?

$$\begin{aligned} 201 = 4\times 50+1 \Rightarrow\ -201 &= -4\times 50-1 \\ &= 4(-50)-1+4-4 \\ &= 4(-51)+3 \ \Rightarrow\ [-201]_4 = [3]_4 \end{aligned}$$

"-201 é congruente módulo 4 com 3"

Teorema 1.4.2: *Sejam* $a, b, c, d \in \mathbb{Z}$ *tais que*

$$a \equiv b \,(mod\, n) \;\; e \;\; c \equiv d \,(mod\, n).$$

Então,

- $a + c \equiv b + d \,(mod\, n)$
- $ac \equiv bd \,(mod\, n)$.

Operações no conjunto das classes (mod n)

Podem definir-se em $\mathbb{Z}_n$ operações de adição $\oplus$ e de multiplicação $\otimes$, dadas por:

$$[a]_n \oplus [b]_n = [a + b]_n \qquad [a]_n \otimes [b]_n = [ab]_n.$$

Teorema 1.4.3: (Propriedades das operações em classes (mod n))

Sejam $x, y, z \in \mathbb{Z}_n$ *e sejam* $\overline{0} = [0]_n$ *e* $\overline{1} = [1]_n$. *Então:*

- $x \oplus y = y \oplus x; \quad (x \oplus y) \oplus z = x \oplus (y \oplus z);$
- $x \oplus \overline{0} = x;$
- *Existe* $x' \in \mathbb{Z}_n$ *tal que* $x \oplus x' = \overline{0};$

$x = [a]_n$, com $a \in \mathbb{Z}$, então $x' = [-a]_n$ pois $x \oplus x' = \overline{0}$.

Ao elemento x' chamamos simétrico de x em $\mathbb{Z}_n$ e representamo-lo por $-x$.

Exemplo: n=13 $\mathbb{Z}_{13} = \{[0]_{13},\ [1]_{13},\ [2]_{13}, \ldots, [12]_{13}\}$

- $-[0]_{13} = [0]_{13}$
- $-[2]_{13} = [-2]_{13} = [11]_{13}$ pois $-2 = 13(-1) + 11$

Se $a \in \{1, \ldots, n-1\}$ então

– $[a]_n = [-a]_n = [n-a]_n$ e temos também $n - a \in \{1, \ldots, n-1\}$.

Teorema 1.4.3: (continuação)

- $x \otimes y = y \otimes x$; $(x \otimes y) \otimes z = x \otimes (y \otimes z)$;
- $x \otimes \overline{1} = x$;
- $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$.

Definição 1.4.4:

Um elemento $x \in \mathbb{Z}_n$ diz-se invertível se existe $x' \in \mathbb{Z}_n$ tal que

$$x \otimes x' = \overline{1} = [1]_n.$$

Se existir x´, diz-se que x´ é o inverso de x

Exemplos:

n=4 $\mathbb{Z}_4 = \{[0]_4,\ [1]_4,\ [2]_4,\ [3]_4\}$

- $[0]_4$ tem inverso ? Não, pois $[0]_4 \otimes [a]_4 = [0]_4 \neq [1]_4$
- $[3]_4$ tem inverso ? Sim, pois $[3]_4 \otimes [3]_4 = [9]_4 = [1]_4$
- $[2]_4$ tem inverso ?

Não, pois

$$[2]_4 \otimes [0]_4 = [2 \times 0]_4 = [0]_4$$
$$[2]_4 \otimes [1]_4 = [2 \times 1]_4 = [2]_4$$
$$[2]_4 \otimes [2]_4 = [2 \times 2]_4 = [4]_4 = [0]_4$$
$$[2]_4 \otimes [3]_4 = [2 \times 3]_4 = [6]_4 = [2]_4$$

Conclusão: $n \in \mathbb{N} \quad \mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$

Dado $a \in \{0, \ldots, n-1\}$, achar o inverso da classe $[a]_n$ é encontrar um elemento $x \in \{0, \ldots, n-1\}$ tal que

$$[a]_n \otimes [x]_n = [1]_n$$
$$\Updownarrow$$
$$[ax]_n = [1]_n$$
$$\Updownarrow$$
$$\boxed{ax \equiv 1 \pmod{n}}$$

Caso particular de uma congruência linear

Definição 1.4.5:

Chamamos congruência linear a uma expressão da forma

$$\mathbf{ax \equiv b \,(mod\, n)}\ ,$$

em que $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$ (constantes) e x é uma variável inteira (i.e. toma valores em $\mathbb{Z}$).

Uma solução da congruência linear $ax \equiv b \,(\mathrm{mod}\, n)$ é um número inteiro α tal que $a\alpha \equiv b \,(\mathrm{mod}\, n)$.

Teorema 1.4.6:

Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Se $\alpha \in \mathbb{Z}$ é uma solução da congruência linear $ax \equiv b \,(mod\, n)$, então qualquer $\beta \in [\alpha]_n$ é também uma solução.

Demonstração. Uma vez que $a\alpha \equiv b \,(\mathrm{mod}\, n)$ e $\beta \equiv \alpha \,(\mathrm{mod}\, n)$, então existem $u, v \in \mathbb{Z}$ tais que

$$a\alpha - b = un \quad \text{e} \quad \beta - \alpha = vn.$$

Assim,

$$\begin{aligned} a\beta - b &= a(\alpha + vn) - (a\alpha - un) \\ &= a\alpha + avn - a\alpha + un \\ &= (av + u)n \end{aligned}$$

e portanto $a\beta \equiv b \,(\mathrm{mod}\, n)$. □

Observação:

Para $n \in \mathbb{N}$, definamos

$$Z_n = \{0, 1, \ldots, n-1\}.$$

Uma vez que $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$, o teorema anterior diz-nos que uma congruência linear fica completamente resolvida quando determinarmos as suas soluções em Z_n.

Exemplos:

- Consideremos a congruência linear $2x \equiv 1 \pmod 4$.

Procurar x tal que
2x-1= múltiplo 4

$$\mathbb{Z}_4 = \{[0]_4,\ [1]_4,\ [2]_4,\ [3]_4\} \qquad Z_4 = \{0,\ 1,\ 2,\ 3\}$$

$$2 \times 0 = 0 \not\equiv 1 (\text{mod } 4)$$
$$2 \times 1 = 2 \not\equiv 1 (\text{mod } 4)$$
$$2 \times 2 = 4 \equiv 0 \not\equiv 1 (\text{mod } 4)$$
$$2 \times 3 = 6 \equiv 2 \not\equiv 1 (\text{mod } 4)$$

Portanto, não possui quaisquer soluções em $\mathbb{Z}$.

- Determinemos as soluções da congruência linear $2x \equiv 1 \pmod 5$.

$$\mathbb{Z}_5 = \{[0]_5,\ [1]_5,\ [2]_5,\ [3]_5, [4]_5\}$$

$$Z_5 = \{0, 1, 2, 3, 4\}$$

Procurar x tal que
2x-1= múltiplo 5

$$2 \times 0 = 0 \equiv 0 (\text{mod } 5)$$
$$2 \times 1 = 2 \equiv 2 (\text{mod } 5)$$
$$2 \times 2 = 4 \equiv 4 (\text{mod } 5)$$
$$2 \times 3 = 6 \equiv 1 (\text{mod } 5)$$
$$2 \times 4 = 8 \equiv 3 (\text{mod } 5)$$

O conjunto das soluções é

$$[3]_5 = 3 + 5\mathbb{Z} = \{\ldots, -12, -7, -2, 3, 8, 13, \ldots\}.$$

!!!!!!!!!!!!!!!!!

- Determinemos as soluções da congruência linear $2x \equiv 4 \pmod{500}$.

Teorema 1.4.7

Sejam $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ e $d = mdc\{a, n\}$. Então a congruência linear

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

- *tem soluções em $\mathbb{Z}$ se e só se $d|b$;*
- *caso $d|b$, então a congruência linear possui exactamente d soluções em Z_n.*

Notas da demonstração:

mdc{a,n}= au + nv

Igualdade de Bezout

1. Sejam $u, v \in \mathbb{Z}$ tais que $d = au + nv$ e tomemos

$$\alpha = \frac{bu}{d} \in \mathbb{Z} \quad e \quad m = \frac{n}{d} \in \mathbb{Z}.$$

2. $\alpha,\ \alpha + m,\ \alpha + 2m, \ldots,\ \alpha + (d-1)m$

são d soluções não congruentes módulo n de $ax \equiv b \pmod{n}$.

3. Estas d soluções podem não pertencer todas a Z_n, mas atendendo aos teorem anteriores, podemos determinar d soluções em Z_n.

Exemplos:

- Determinemos as soluções da congruência linear $2x \equiv 4 \pmod{500}$.

Seja $d = \text{mdc}\{2, 500\} = 2$.

$Z_{500} = \{0, 1, 2, 3, 4, \ldots, 499\}$

Como $d = 2$ divide $b = 4$ então a congruência linear tem soluções e tem exactamente $d = 2$ soluções em Z_{500}.

? $\alpha,\ \alpha + m$?

$$2 = \text{mdc}\{2,500\} = 2u + 500v = 2 \times \underset{u}{1} + 500 \times 0$$

$$\alpha = \frac{bu}{d} = \frac{4 \times 1}{2} = 2 \qquad m = \frac{n}{d} = \frac{500}{2} = 250$$

$$\alpha = 2, \quad \alpha + m = 2 + 250 = 252$$

São duas soluções em Z_{500}

Conclusão: $[2]_{500} \cup [252]_{500}$ é o conjunto de todas as soluções em $\mathbb{Z}$

- Consideremos agora a congruência linear $224x \equiv 154 \pmod{385}$ e determinemos todas as suas soluções em Z_{385}.

Como $d = \text{mdc}\{224,\ 385\} = 7$ e 7 é um divisor de $b = 154\ (= 7 \times 22)$, então $224x \equiv 154 \pmod{385}$ possui exactamente 7 soluções em Z_{385}. Por outro lado, temos $7 = 224 \cdot (-12) + 385 \cdot 7$ (donde $u = -12$), pelo que

$$\alpha = \frac{154 \times (-12)}{7} = -264,$$

é uma solução de $224x \equiv 154 \pmod{385}$. Note que $\alpha \notin Z_{385}$.

Seja

$$m = \frac{n}{d} = \frac{385}{7} = 55.$$

Então, $\alpha + km = -264 + k55$, com $k = 0, 1, 2, 3, 4, 5, 6$, i.e.

$-264, -209, -154, -99, -44$, 11 e 66

são sete solucões não congruentes módulo 385. Como

Encontrar as correspondentes soluções em

$121 \equiv (-264) \pmod{385}$, $176 \equiv (-209) \pmod{385}$,
$231 \equiv (-154) \pmod{385}$, $286 \equiv (-99) \pmod{385}$ e $341 \equiv (-44) \pmod{385}$,
então

$$11, 66, 121, 176, 231, 286 \text{ e } 341$$

são as sete soluções de $224x \equiv 154 \pmod{385}$ em Z_{385}.

Congruências lineares equivalentes:

Considere a congruência linear

$$1502x \equiv 1004 \pmod{500}$$

Ora,

$$\begin{array}{r|l} 1502 & 500 \\ \cline{2-2} 2 & 3 \end{array}$$

$$1502 \equiv 2 \pmod{500}$$

$$\begin{array}{r|l} 1004 & 500 \\ \cline{2-2} 4 & 2 \end{array}$$

$$1004 \equiv 4 \pmod{500}$$

Assim,

$$\begin{array}{c} 1502x \equiv 1004 \pmod{500} \\ \Updownarrow \\ 2x \equiv 4 \pmod{500} \end{array}$$

uma vez que as soluções da segunda congruência são as mesmas que as da primeira.

Porquê?

Teorema 1.4.8:

Seja $n \in \mathbb{N}$ e sejam $a, a', b, b' \in \mathbb{Z}$ tais que $a \equiv a' \,(\mathrm{mod}\, n)$ e $b \equiv b' \,(\mathrm{mod}\, n)$. Então, as congruências lineares

$$ax \equiv b \,(\mathrm{mod}\, n) \quad e \quad a'x \equiv b' \,(\mathrm{mod}\, n)$$

possuem exactamente as mesmas soluções.

Demonstração.

$$a \equiv a' \pmod{n} \Leftrightarrow a - a' = k_1 n, \quad k_1 \in \mathbb{Z}$$
$$b \equiv b' \pmod{n} \Leftrightarrow b - b' = k_2 n, \quad k_2 \in \mathbb{Z}$$

Seja α uma solução de $ax \equiv b \pmod{n}$.

Assim,

$$a\alpha \equiv b \pmod{n} \Leftrightarrow a\alpha - b = k_3 n, \quad k_3 \in \mathbb{Z}.$$

Ora,

$$a'\alpha - b' = (a - k_1 n)\alpha - (b - k_2 n) = a\alpha - k_1 n\alpha - b + k_2 n$$
$$= k_3 n - k_1 n\alpha + k_2 n = \underbrace{(k_3 - k_1\alpha + k_2)}_{k_4} n = k_4 n.$$

Então, $a'\alpha \equiv b' \pmod{n}$

Analogamente se conclui que se α é solução de $a'x \equiv b' \pmod{n}$, então também é solução de $ax \equiv b \pmod{n}$. □

Observação

O resultado anterior permite-nos concluir que, para estudar todas as congruências lineares do tipo $ax \equiv b \pmod{n}$, com $n \in \mathbb{N}$ e $a, b \in \mathbb{Z}$, basta estudar aquelas em que $a, b \in Z_n$.

Sistemas de congruências:

Sendo $x \in \mathbb{Z}$ e $n, m \in \mathbb{N}$, então

$$[x]_{nm} \subseteq [x]_n \cap [x]_m.$$

$$[3]_{4\times 8} \subseteq [3]_4 \cap [3]_8$$

Considere as duas congruências lineares

$$2x \equiv 2 \pmod 4, \quad 3x \equiv 1 \pmod 8 .$$

3 é solução das duas congrências pois

$$2 \times 3 - 2 = 4 = 4 \times 1 \qquad \text{e} \qquad 3 \times 3 - 1 = 8 = 8 \times 1.$$

Então podemos afirmar que todos os elementos da classe

$$[3]_{32} = 3 + 32\mathbb{Z}$$

são soluções comuns das duas congruências.

Podemos generalizar?

Teorema 1.4.9:

Sejam $m, n \in \mathbb{N}$ e sejam $a, a', b, b' \in \mathbb{Z}$. Seja α uma solução (comum) das congruências lineares

$$ax \equiv b \,(\mathrm{mod}\, m) \quad e \quad a'x \equiv b' \,(\mathrm{mod}\, n).$$

Então, qualquer $\beta \in [\alpha]_{mn}$ é ainda uma solução de ambas as congruências lineares.

Demonstração.

Basta atender a que $[\alpha]_{mn} \subseteq [\alpha]_m \cap [\alpha]_n$ □

Lema 1.4.10:

Sejam $m, n \in \mathbb{Z}$ tais que $1 = mdc\{m, n\}$ e sejam $b, b' \in \mathbb{Z}$. Então as congruências lineares $x \equiv b \pmod{m}$ e $x \equiv b' \pmod{n}$ têm uma e uma só solução comum em Z_{mn}.

Demonstração. Tomar $u, v \in \mathbb{Z}$ tais que $1 = mu + nv$. Então $\alpha \in Z_{mn}$ tal que $\alpha \equiv (bnv + b'mu) \pmod{mn}$ é a solução pretendida. □

Exemplo: Considere as congruências lineares

$$x \equiv 5 \pmod{2} \quad \text{e} \quad x \equiv 6 \pmod{3}.$$

Como mdc{2, 3}=1 então existe uma solução comum em Z_6.

Ora,

1= mdc{2, 3}= 2 u + 3 v =2(-1) + 3(1). **(Identidade de Bezout)**

? ?

Assim,

6x2(-1) + 5x3(1) = -12 + 15 =3 é solução das duas congruências.

Conclusão: $[3]_{2\times 3} = [3]_6$ são todas as soluções comuns às duas congruências

Teorema 1.4.11:

Sejam $m, n \in \mathbb{N}$ tais que $1 = mdc\{m, n\}$ e sejam $a, a', b, b' \in \mathbb{Z}$. Se as congruências lineares $ax \equiv b \pmod{m}$ e $a'x \equiv b' \pmod{n}$ têm ambas soluções, então existe uma solução comum a ambas em Z_{mn}.

Demonstração. Sejam α e α' soluções de $ax \equiv b \pmod{m}$ e de $a'x \equiv b' \pmod{n}$, respectivamente. Atendendo ao lema anterior, o sistema de congruência lineares

$$\begin{cases} x \equiv \alpha \pmod{m} \\ x \equiv \alpha' \pmod{n} \end{cases}$$

possui uma (única) solução $\beta \in Z_{mn}$. Claramente, β é também uma solução de $ax \equiv b \pmod{m}$ e de $a'x \equiv b' \pmod{n}$. □

Exemplo: Considere as congruências lineares

$4x \equiv 12 \pmod{5}$ e $3x \equiv 6 \pmod{4}$.

$\alpha \in Z_5$ $\quad$ $\alpha' \in Z_4$

Será que têm soluções comuns?

Pelo Teorema, existe $\beta \in Z_{20}$ que é solução comum.

Exemplo: (Cont.)

Determinemos em Z_{20} uma solução comum às congruências lineares

$$4x \equiv 12 \pmod 5 \qquad \text{e} \qquad 3x \equiv 6 \pmod 4.$$

Uma solução de $4x \equiv 2 \pmod 5$ é $\alpha = 3$ e uma solução de $3x \equiv 6 \pmod 4$ é $\alpha' = 2$.

Seguidamente, calculamos a (única) solução comum em Z_{20}

$$x \equiv 3 \pmod 5 \qquad \text{e} \qquad x \equiv 2 \pmod 4$$

(note-se que $1 = \text{mdc}\{4,\ 5\}$): temos $1 = 5 \cdot 1 + 4 \cdot (-1)$, donde

$$\beta = 2 \cdot 5 \cdot 1 + 3 \cdot 4 \cdot (-1) = -2$$

é uma solução comum.

Como

$$-2 \equiv 18 \pmod{20},$$

então 18 é a (única) solução comum em Z_{20} às congruências $x \equiv 3 \pmod 5$ e $x \equiv 2 \pmod 4$ e, consequentemente, também uma solução comum às congruências iniciais.

Teorema 1.4.7

Sejam $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ e $d = mdc\{a, n\}$. Então a congruência linear

$$ax \equiv b \,(mod\, n)$$

- *tem soluções em $\mathbb{Z}$ se e só se $d|b$;*
- *caso $d|b$, então a congruência linear possui exactamente d soluções em Z_n.*

Notas da demonstração:

mdc{a,n}= au + nv

Igualdade de Bezout

1. Sejam $u, v \in \mathbb{Z}$ tais que $d = au + nv$ e tomemos

$$\alpha = \frac{bu}{d} \in \mathbb{Z} \quad e \quad m = \frac{n}{d} \in \mathbb{Z}.$$

2. $\alpha,\ \alpha + m,\ \alpha + 2m, \ldots,\ \alpha + (d-1)m$

são d soluções não congruentes módulo n de $ax \equiv b \,(\mathrm{mod}\, n)$.

3. Estas d soluções podem não pertencer todas a Z_n, mas atendendo aos teorem anteriores, podemos determinar d soluções em Z_n.

Exemplos:

- Determinemos as soluções da congruência linear $2x \equiv 4 \pmod{500}$.

Seja $d = \text{mdc}\{2, 500\} = 2$.

$Z_{500} = \{0, 1, 2, 3, 4, \ldots, 499\}$

Como $d = 2$ divide $b = 4$ então a congruência linear tem soluções e tem exactamente $d = 2$ soluções em Z_{500}.

? $\alpha,\ \alpha + m$?

$$2 = \text{mdc}\{2,500\} = 2u + 500v = 2 \times \underset{u}{1} + 500 \times 0$$

$$\alpha = \frac{bu}{d} = \frac{4 \times 1}{2} = 2 \qquad m = \frac{n}{d} = \frac{500}{2} = 250$$

$$\alpha = 2, \quad \alpha + m = 2 + 250 = 252$$

São duas soluções em Z_{500}

Conclusão: $[2]_{500} \cup [252]_{500}$ é o conjunto de todas as soluções em $\mathbb{Z}$

- Consideremos agora a congruência linear $224x \equiv 154 \pmod{385}$ e determinemos todas as suas soluções em Z_{385}.

Como $d = \text{mdc}\{224,\ 385\} = 7$ e 7 é um divisor de $b = 154\ (= 7 \times 22)$, então $224x \equiv 154 \pmod{385}$ possui exactamente 7 soluções em Z_{385}. Por outro lado, temos $7 = 224 \cdot (-12) + 385 \cdot 7$ (donde $u = -12$), pelo que

$$\alpha = \frac{154 \times (-12)}{7} = -264,$$

é uma solução de $224x \equiv 154 \pmod{385}$. Note que $\alpha \notin Z_{385}$.

Seja

$$m = \frac{n}{d} = \frac{385}{7} = 55.$$

Então, $\alpha + km = -264 + k55$, com $k = 0, 1, 2, 3, 4, 5, 6$, i.e.

$-264, -209, -154, -99, -44$, 11 e 66

são sete solucões não congruentes módulo 385. Como

Encontrar as correspondentes soluções em

$121 \equiv (-264) \pmod{385}$, $176 \equiv (-209) \pmod{385}$,
$231 \equiv (-154) \pmod{385}$, $286 \equiv (-99) \pmod{385}$ e $341 \equiv (-44) \pmod{385}$,
então

$$11, 66, 121, 176, 231, 286 \text{ e } 341$$

são as sete soluções de $224x \equiv 154 \pmod{385}$ em Z_{385}.

Congruências lineares equivalentes:

Considere a congruência linear

$$1502x \equiv 1004 \pmod{500}$$

Ora,

$$\begin{array}{r|l} 1502 & 500 \\ \cline{2-2} 2 & 3 \end{array}$$

$$1502 \equiv 2 \pmod{500}$$

$$\begin{array}{r|l} 1004 & 500 \\ \cline{2-2} 4 & 2 \end{array}$$

$$1004 \equiv 4 \pmod{500}$$

Assim,

$$\begin{array}{c} 1502x \equiv 1004 \pmod{500} \\ \Updownarrow \\ 2x \equiv 4 \pmod{500} \end{array}$$

uma vez que as soluções da segunda congruência são as mesmas que as da primeira.

Porquê?

Teorema 1.4.8:

Seja $n \in \mathbb{N}$ e sejam $a, a', b, b' \in \mathbb{Z}$ tais que $a \equiv a' \,(\mathrm{mod}\, n)$ e $b \equiv b' \,(\mathrm{mod}\, n)$. Então, as congruências lineares

$$ax \equiv b \,(\mathrm{mod}\, n) \quad e \quad a'x \equiv b' \,(\mathrm{mod}\, n)$$

possuem exactamente as mesmas soluções.

Demonstração.

$$a \equiv a' \pmod{n} \Leftrightarrow a - a' = k_1 n, \quad k_1 \in \mathbb{Z}$$
$$b \equiv b' \pmod{n} \Leftrightarrow b - b' = k_2 n, \quad k_2 \in \mathbb{Z}$$

Seja α uma solução de $ax \equiv b \pmod{n}$.

Assim,

$$a\alpha \equiv b \pmod{n} \Leftrightarrow a\alpha - b = k_3 n, \quad k_3 \in \mathbb{Z}.$$

Ora,

$$a'\alpha - b' = (a - k_1 n)\alpha - (b - k_2 n) = a\alpha - k_1 n\alpha - b + k_2 n$$
$$= k_3 n - k_1 n\alpha + k_2 n = \underbrace{(k_3 - k_1\alpha + k_2)}_{k_4} n = k_4 n.$$

Então, $a'\alpha \equiv b' \pmod{n}$

Analogamente se conclui que se α é solução de $a'x \equiv b' \pmod{n}$, então também é solução de $ax \equiv b \pmod{n}$. □

Observação

O resultado anterior permite-nos concluir que, para estudar todas as congruências lineares do tipo $ax \equiv b \pmod{n}$, com $n \in \mathbb{N}$ e $a, b \in \mathbb{Z}$, basta estudar aquelas em que $a, b \in Z_n$.

Sistemas de congruências:

Sendo $x \in \mathbb{Z}$ e $n, m \in \mathbb{N}$, então

$$[x]_{nm} \subseteq [x]_n \cap [x]_m.$$

$$[3]_{4\times 8} \subseteq [3]_4 \cap [3]_8$$

Considere as duas congruências lineares

$$2x \equiv 2 \pmod 4, \quad 3x \equiv 1 \pmod 8 .$$

3 é solução das duas congrências pois

$$2 \times 3 - 2 = 4 = 4 \times 1 \qquad \text{e} \qquad 3 \times 3 - 1 = 8 = 8 \times 1.$$

Então podemos afirmar que todos os elementos da classe

$$[3]_{32} = 3 + 32\mathbb{Z}$$

são soluções comuns das duas congruências.

Podemos generalizar?

Teorema 1.4.9:

Sejam $m, n \in \mathbb{N}$ e sejam $a, a', b, b' \in \mathbb{Z}$. Seja α uma solução (comum) das congruências lineares

$$ax \equiv b \,(\mathrm{mod}\, m) \quad e \quad a'x \equiv b' \,(\mathrm{mod}\, n).$$

Então, qualquer $\beta \in [\alpha]_{mn}$ é ainda uma solução de ambas as congruências lineares.

Demonstração.

Basta atender a que $[\alpha]_{mn} \subseteq [\alpha]_m \cap [\alpha]_n$ □

Lema 1.4.10:

Sejam $m, n \in \mathbb{Z}$ tais que $1 = mdc\{m, n\}$ e sejam $b, b' \in \mathbb{Z}$. Então as congruências lineares $x \equiv b \pmod{m}$ e $x \equiv b' \pmod{n}$ têm uma e uma só solução comum em Z_{mn}.

Demonstração. Tomar $u, v \in \mathbb{Z}$ tais que $1 = mu + nv$. Então $\alpha \in Z_{mn}$ tal que $\alpha \equiv (bnv + b'mu) \pmod{mn}$ é a solução pretendida. □

Exemplo: Considere as congruências lineares

$$x \equiv 5 \pmod{2} \quad \text{e} \quad x \equiv 6 \pmod{3}.$$

Como mdc{2, 3}=1 então existe uma solução comum em Z_6.

Ora,

1= mdc{2, 3}= 2 u + 3 v =2(-1) + 3(1). **(Identidade de Bezout)**

? ?

Assim,

6x2(-1) + 5x3(1) = -12 + 15 =3 é solução das duas congruências.

Conclusão: $[3]_{2\times 3} = [3]_6$ são todas as soluções comuns às duas congruências

Teorema 1.4.11:

Sejam $m, n \in \mathbb{N}$ tais que $1 = mdc\{m, n\}$ e sejam $a, a', b, b' \in \mathbb{Z}$. Se as congruências lineares $ax \equiv b \pmod{m}$ e $a'x \equiv b' \pmod{n}$ têm ambas soluções, então existe uma solução comum a ambas em Z_{mn}.

Demonstração. Sejam α e α' soluções de $ax \equiv b \pmod{m}$ e de $a'x \equiv b' \pmod{n}$, respectivamente. Atendendo ao lema anterior, o sistema de congruência lineares

$$\begin{cases} x \equiv \alpha \pmod{m} \\ x \equiv \alpha' \pmod{n} \end{cases}$$

possui uma (única) solução $\beta \in Z_{mn}$. Claramente, β é também uma solução de $ax \equiv b \pmod{m}$ e de $a'x \equiv b' \pmod{n}$. □

Exemplo: Considere as congruências lineares

$4x \equiv 12 \pmod{5}$ e $3x \equiv 6 \pmod{4}$.

$\alpha \in Z_5$ $\quad$ $\alpha' \in Z_4$

Será que têm soluções comuns?

Pelo Teorema, existe $\beta \in Z_{20}$ que é solução comum.

Exemplo: (Cont.)

Determinemos em Z_{20} uma solução comum às congruências lineares

$$4x \equiv 12 \pmod 5 \qquad \text{e} \qquad 3x \equiv 6 \pmod 4.$$

Uma solução de $4x \equiv 2 \pmod 5$ é $\alpha = 3$ e uma solução de $3x \equiv 6 \pmod 4$ é $\alpha' = 2$.

Seguidamente, calculamos a (única) solução comum em Z_{20}

$$x \equiv 3 \pmod 5 \qquad \text{e} \qquad x \equiv 2 \pmod 4$$

(note-se que $1 = \text{mdc}\{4,\ 5\}$): temos $1 = 5 \cdot 1 + 4 \cdot (-1)$, donde

$$\beta = 2 \cdot 5 \cdot 1 + 3 \cdot 4 \cdot (-1) = -2$$

é uma solução comum.

Como

$$-2 \equiv 18 \pmod{20},$$

então 18 é a (única) solução comum em Z_{20} às congruências $x \equiv 3 \pmod 5$ e $x \equiv 2 \pmod 4$ e, consequentemente, também uma solução comum às congruências iniciais.

1.5 Relações de recorrência

Seja $(a_n)_{n\geq 0}$ uma sucessão de números reais.

$a_0, a_1, a_2, a_3, \ldots, a_n, \ldots$

Diz-se que a sucessão está definida por recorrência se a partir de certa ordem (ordem p) o termo a_n está relacionado com alguns dos seus predecessores $a_0, a_1, \ldots, a_{n-1}$.

Exemplos:

- A sucessão de Fibonacci $(f_n)_{n\geq 1}$ está definida por

$$f_1 = 1 \quad \& \quad f_2 = 2 \longrightarrow \text{Condições iniciais}$$

e

$$f_n = f_{n-1} + f_{n-2} \quad (n \geq 3):$$

Relação de recorrência

$$1, \quad 2, \quad 3, \quad 5, \quad 8, \quad 13, \quad 21, \quad 34, \quad \ldots$$

"Resolver" uma relação de recorrência, sujeita a certas condições iniciais, é determinar uma *"expressão explícita"* para o termo geral da sucessão.

- Seja $(a_n)_{n\geq 1}$ a sucessão definida pela relação de recorrência

Relação de recorrência $a_n = a_{n-1} + 3, \quad n \geq 2,$

com a condição inicial $a_1 = 2.$

Condição inicial

2, 5, 8, 11, 14, 17,...

Ora,

$$
\begin{aligned}
a_n &= a_{n-1} + 3 \\
&= (a_{n-2} + 3) + 3 && = a_{n-2} + 2 \cdot 3 \\
&= (a_{n-3} + 3) + 2 \cdot 3 && = a_{n-3} + 3 \cdot 3 \\
&\ldots && \ldots \\
&= (a_{n-k} + 3) + (k-1) \cdot 3 && = a_{n-k} + k \cdot 3 \\
&\ldots && \ldots \\
&= a_1 + (n-1) \cdot 3 \\
&= 2 + 3(n-1),
\end{aligned}
$$

i.e. $\boxed{a_n = 2 + 3(n-1), \text{ para } n \geq 1.}$

(Prove usando o princípio de indução)

- Vamos resolver a relação de recorrência $a_n = 2a_{n-1}$ sujeita à condição inicial $a_0 = 1$. Temos

Relação de recorrência

Condição inicial

$$
\begin{aligned}
a_n &= 2a_{n-1} \\
&= 2 \cdot 2a_{n-2} && = 2^2 a_{n-2} \\
&= 2^2 \cdot 2a_{n-3} && = 2^3 a_{n-3} \\
&\ldots \\
&= 2^k a_{n-k} \\
&\ldots \\
&= 2^n a_0 = 2^n, && \text{i.e. } \boxed{a_n = 2^n, \text{ para } n \geq 0.}
\end{aligned}
$$

(Prove usando o princípio de indução)

Definição 1.5.1:

Uma *relação de recorrência linear homogénea de grau k ($k \geq 1$) com coeficientes constantes* é uma expressão da forma

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

com $c_1, \ldots, c_k$ constantes (reais) e $c_k \neq 0$.

$$a_n = 21a_{n-1} + 13a_{n-2}$$

Exemplos:

- A expressão $f_n = f_{n-1} + f_{n-2}$ (utilizada na definição da sucessão de Fibonacci) é uma relação de recorrência linear homogénea de grau 2 com coeficientes constantes.
- A expressão $a_n = 2a_{n-1}$ é uma relação de recorrência linear homogénea de grau 1 com coeficientes constantes.
- A relação de recorrência $a_n = 3a_{n-1}a_{n-2}$ não é linear.
- A relação de recorrência $a_n = a_{n-1} + 3$ não é homogénea.
- A relação de recorrência $a_n = 3na_{n-1}$ não tem coeficientes constantes.

Recorrências lineares homogéneas de coeficientes constantes de grau 1 e 2

1 Grau 1:

Uma relação de recorrência do tipo

$$a_n = c a_{n-1},$$

com a condição inicial $a_0 = a$ é da forma

$$a_n = a c^n, \quad n \geq 0.$$

2 Grau 2:

Uma relação de recorrência do tipo

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} \quad (c_1, c_2 \in \mathbb{R})$$

com as condições iniciais $a_0 = C_0$ e $a_1 = C_1$ é da forma:

$$x^2 - c_1 x - c_2 = 0 \quad \text{(Equação auxiliar)}$$

Tem duas raízes reais r_1 e r_2

$$a_n = b\, r_1^n + d\, r_2^n, \qquad n \geq 0.$$

Tem uma raízes real dupla r

$$a_n = b\, r^n + d\, n\, r^n, \qquad n \geq 0.$$

Lema 1.5.2:

Seja $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ $(c_1, c_2 \in \mathbb{R})$ uma relação de recorrência linear homogénea de grau 2 com coeficientes constantes.

Sejam S_n e T_n duas sucessões que satisfazem a relação de recorrência constantes (reais).

Então a sucessão $U_n = bS_n + dT_n$ também satisfaz a relação de recorrência.

Demonstração.

Se (S_n) e (T_n) satisfazem a recorrência linear então

$$S_n = c_1 S_{n-1} + c_2 S_{n-2} \quad (n \geq 2) \quad \text{e} \quad T_n = c_1 T_{n-1} + c_2 T_{n-2} \quad (n \geq 2).$$

Assim,

$$\begin{aligned} U_n = bS_n + dT_n &= b(c_1 S_{n-1} + c_2 S_{n-2}) + d(c_1 T_{n-1} + c_2 T_{n-2}) \\ &= bc_1 S_{n-1} + bc_2 S_{n-2} + dc_1 T_{n-1} + dc_2 T_{n-2} \\ &= c_1(bS_{n-1} + dT_{n-1}) + c_2(bS_{n-2} + dT_{n-2}) \\ &= c_1 U_{n-1} + c_2 U_{n-2} \end{aligned}$$

□

Lema 1.5.3:

Seja $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ $(c_1, c_2 \in \mathbb{R})$ uma relação de recorrência linear homogénea de grau 2 com coeficientes constantes. Seja r uma raiz da equação $x^2 - c_1 x - c_2 = 0$. Então, a sucessão $(r^n)_{n \in \mathbb{N}_0}$ satisfaz a relação de recorrência.

Demonstração. Por hipótese, r é raiz de $x^2 - c_1 x - c_2 = 0$, pelo que $r^2 - c_1 r - c_2 = 0$, ou seja, $r^2 = c_1 r + c_2$. Então

$$\begin{aligned} c_1 r^{n-1} + c_2 r^{n-2} &= r^{n-2}(c_1 r + c_2) \\ &= r^{n-2} r^2 = r^n, \end{aligned}$$

como pretendido. □

$1,\ r,\ r^2,\ r^3, \ldots$

Exemplo: Considere a relação de recorrência linear

$$a_n = a_{n-1} + 6\, a_{n-2}\ .$$

Como

$$x^2 - x - 6 = 0 \Leftrightarrow \text{x = -2 ou x = 3,}$$

então as sucessões $S_n=(-2)^n$ e $T_n=(3)^n$ satisfazem a recorrência linear.

1, -2, 4, -8, 16, -32,…..

1, 3, 9, 27, 81, …..

Teorema 1.5.4:

Seja $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ $(c_1, c_2 \in \mathbb{R})$ *uma relação de recorrência linear homogénea de grau 2 com coeficientes constantes tal que a equação*

$$x^2 - c_1 x - c_2 = 0$$

admite duas raízes distintas r_1 *e* r_2. *Seja* $(a_n)_{n\geq 0}$ *a sucessão definida pela relação de recorrência sujeita às condições iniciais*

$$a_0 = C_0 \quad e \quad a_1 = C_1.$$

Então, existem constantes (reais) b *e* d *tais que*

$$a_n = b\, r_1^n + d\, r_2^n, \qquad n \geq 0.$$

Demonstração.

Resulta directamente dos 2 lemas anteriores. □

Exemplos:

- Vamos resolver a relação de recorrência

$$a_n = 5a_{n-1} - 6a_{n-2}$$ Relação de recorrência

sujeita às condições iniciais $a_0 = 7$ e $a_1 = 16$. Condições iniciais

Ora,

$$x^2 - 5x + 6 = 0 \Leftrightarrow x - 2 \text{ e } x - 3.$$

Atendendo ao teorema anterior, temos

$$a_n = b\,2^n + d\,3^n, \quad n \geq 0,$$

para certas constantes b e d tais que

$$\begin{cases} b + d = a_0 = 7 \\ 2b + 3d = a_1 = 16, \end{cases}$$

ou seja (resolvendo o sistema), $b = 5$ e $d = 2$.

Logo, $a_n = 5 \cdot 2^n + 2 \cdot 3^n$, para $n \geq 0$.

Teorema 1.5.5:

Seja $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ $(c_1, c_2 \in \mathbb{R})$ *uma relação de recorrência linear homogénea de grau 2 com coeficientes constantes tal que a equação* $x^2 - c_1 x - c_2 = 0$ *admite uma raiz dupla* r. *Seja* $(a_n)_{n\geq 0}$ *a sucessão definida pela relação de recorrência sujeita às condições iniciais*

$$a_0 = C_0 \quad e \quad a_1 = C_1.$$

Então, existem constantes (reais) b *e* d *tais que*

$$a_n = b\, r^n + d\, n\, r^n, \qquad n \geq 0.$$

Demonstração.

Do Lema 1.5.3 tira-se que a sucessão $S_n = r^n$ satisfaz a recorrência. O facto da r ser raíz dupla permite ainda concluir que $T_n = nr^n$ é uma sucessão que satisfaz a recorrência.
O resultado segue agora do Lema 1.5.2. □

Exemplo:

Relação de recorrência

- Vamos resolver a relação de recorrência $c_n = 4c_{n-1} - 4c_{n-2}$ sujeita às condições iniciais $c_0 = 1$ e $c_1 = 1$.

Ora, Condições iniciais

$$x^2 - 4x + 4 = 0 \Leftrightarrow x = 2 \quad \text{(raiz dupla)}$$

Atendendo ao teorema anterior, temos

$$c_n = b\,2^n + d\,n\,2^n, \quad n \geq 0,$$

para certas constantes b e d tais que

$$\begin{cases} b = c_0 = 1 \\ 2b + 2d = c_1 = 1 \end{cases} \Leftrightarrow b = 1 \text{ e } d = -\tfrac{1}{2}.$$

Logo, $\boxed{a_n = 2^n - \frac{1}{2}\,n\,2^n = 2^n - n2^{n-1}, \quad \text{para } n \geq 0.}$