#### Conceitos Preliminares

Teoria da Computação – Ciência da Computação



Prof. Daniel Saad Nogueira Nunes

IFB – Instituto Federal de Brasília, Campus Taguatinga



#### Sumário

- Noções Matemáticas
- 2 Lógica



#### Sumário

Noções Matemáticas



# Noções Matemáticas

- Antes de iniciar o nosso estudo em TC, precisamos revisar e abordar conceitos matemáticos básicos.
- Notações e ferramentas que vamos usar.



#### Sumário

- Noções Matemáticas
  - Conjuntos
  - Sequências e Tuplas
  - Funções
  - Relações
  - Grafos
  - Linguagens e Cadeias



#### Conjuntos

- Um conjunto é um grupo de objetos representado como uma unidade.
- Conjuntos podem ter objetos de tipos variados: números, símbolos, pessoas, . . .
- Objetos que estão em um conjunto são denominados de elementos.
- Uma forma de descrever quais elementos estão em um conjunto é utilizar a notação de chaves:

$$\{7, 21, 57\}$$



#### Notação (Pertinência)

- Os símbolos ∈ e ∉ são utilizados para denotar pertinência e não-pertinência de elementos em conjuntos.
- Ex:  $7 \in \{7, 21, 57\}$ .
- Ex:  $8 \notin \{7, 21, 57\}$



# Notação (⊆)

- ullet Dizemos que um conjunto A está contido em um conjunto B, se todo o elemento de A está em B.
- Representamos por  $A \subseteq B$ .



#### Notação (Igualdade)

- Dois conjuntos A e B são iguais se todo o elemento de A está em B e vice-versa.
- Em outras palavras, A = B, sse,  $A \subseteq B$  e  $B \subseteq A$ .



#### Notação (⊊)

- Dizemos que um conjunto A está propriamente contido em um conjunto B, se todo o elemento de A está em B, mas B não é igual a A.
- Representamos por  $A \subsetneq B$ .



#### Notação (Ø)

- O conjunto vazio é aquele que não possui elementos.
- Representado por  $\emptyset$ .



- A ordem na descrição não importa.
- Repetições também são ignoradas. Conjuntos são indistinguíveis considerando repetições.
- Ex:  $\{1,2,3\} = \{3,2,1\}.$
- Ex:  $\{1, 1, 1, 1, 2, 3, 4\} = \{1, 2, 3, 4\}.$
- Multiconjuntos: levam em consideração repetições.



#### Definição (Cardinalidade)

- A cardinalidade corresponde ao número de elementos que um conjunto possui.
- Denotamos por |A|.
- $\bullet \ \, {\sf Em \ especial} \ \, |\emptyset| = 0.$



- Alguns conjuntos são finitos.
- Alguns conjuntos são infinitos.
- Ex:  $|\{1,2,3,4\}|=4$ .
- Ex:  $\mathbb{N} = \{1, 2, 3, ...\}$  é infinito.
- Ex:  $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$  é infinito.
- Ex: ℝ é infinito.
- Curiosidade:  $|\mathbb{R}| > |\mathbb{Z}| = |\mathbb{N}|$ .



- Outra maneira de definir conjuntos, é colocando uma propriedade sobre os elementos.
- Conjunto dos pares:  $P = \{x | x = 2y \text{ com } y \in \mathbb{Z}\}$
- Conjunto dos ímpares:  $I = \{x | x = 2y + 1 \text{ com } y \in \mathbb{Z}\}$
- Conjunto dos primos:  $\Pi = \{x | x \in \mathbb{N} \land x > 1 \land \neg \exists y (y < x \land x \mod y = 0)\}$



#### Definição (União)

A união de dois conjuntos A e B corresponde a  $C = \{x | x \in A \text{ ou } x \in B\}.$ 

A união de conjuntos é representada através do símbolo  $\cup$ 

- $\bullet \ \, \mathsf{Exemplo} \,\, \{1,2\} \cup \{2,3\} = \{1,2,3\}.$
- Em especial  $A \cup \emptyset = A$ .



#### Definição (Interseção)

A interseção de dois conjuntos A e B corresponde a  $C = \{x | x \in A \text{ e } x \in B\}.$ 

A interseção de conjuntos é representada através do símbolo ∩.

- Exemplo  $\{1,2\} \cap \{2,3\} = \{2\}.$
- Em especial  $A \cap \emptyset = \emptyset$ .



#### Definição (Complemento)

O complemento de um conjunto A é outro conjunto cujos elementos em consideração são exatamente aqueles que não estão em A.

Denotamos o complemento de  ${\cal A}$  por  ${\cal A}.$ 

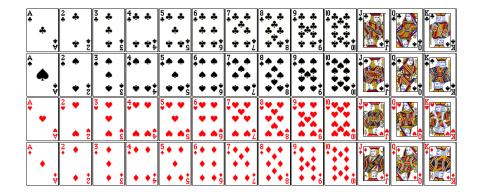


#### Definição (Produto Cartesiano)

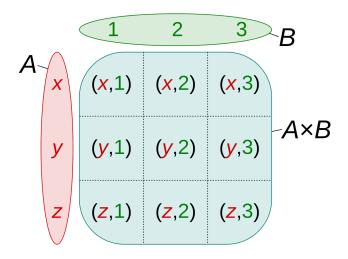
Se A e B são conjuntos, o produto cartesiano de A por B é dado por:

$$A\times B=\{(a,b)|a\in A\wedge b\in B\}$$











#### Notação (Produto Cartesiano)

$$\underbrace{A \times A \times A \dots A}_{k} = A^{k}$$

- Ex:  $\mathbb{R}^2$ , o plano cartesiano.
- Ex:  $\mathbb{R}^3$ , espaço tridimensional.
- Ex:  $\mathbb{R}^n$ .
- Ex:  $\mathbb{N}^2 = \{(1,1), (1,2) \dots (2,1), (2,2) \dots \}$



#### Definição (Partes de um Conjunto)

As partes de um cojunto A, denotada por  $\mathcal{P}(A)$ , corresponde ao conjunto dos subconjuntos de A.

Se 
$$|A|=n$$
, então  $|\mathcal{P}(A)|=2^n$ 

$$\bullet \ \, \mathsf{Ex:} \ \, \mathcal{P}(\{1,2,3\}) = \{\emptyset,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$$



#### Sumário

- Noções Matemáticas
  - Conjuntos
  - Sequências e Tuplas
  - Funções
  - Relações
  - Grafos
  - Linguagens e Cadeias



# Sequências e Tuplas

#### Definição (Sequências)

Sequências de objetos são listas destes objetos. Diferentemente dos conjuntos, a ordem aqui importa, bem como as repetições.



# Sequências e Tuplas

- Ex:  $F = (1, 1, 2, 3, 5, 8, \ldots)$ .
- Ex:  $\Pi' = (2, 3, 5, 7, 11, \ldots)$ .
- $\bullet \ \, \mathsf{Ex:} \,\, (1,1,1,1,1,1,1,1,1) \neq (1).$



# Sequências e Tuplas

#### Notação

Tuplas Uma sequência de k elementos é denominado uma k-tupla.

- Ex: (7, 21, 57) é uma tripla.
- Ex: (1,4) é um par.
- $\bullet$  Ex: (1,5,3,4,7,8,1) é uma 7-tupla.



#### Sumário

- Noções Matemáticas
  - Conjuntos
  - Sequências e Tuplas
  - Funções
  - Relações
  - Grafos
  - Linguagens e Cadeias



#### Funções

Funções são objetos matemáticos que mapeia elementos de um conjunto em outro.

Se f mapeia elementos de D em CD, denotamos por:

$$f: D \to CD$$

D é chamado de domínio e CD é chamado de contradomínio.

Para ser uma função, cada elemento de  ${\cal D}$  deve ter exatamente 1 mapeamento.



- Ex:  $f(x): \mathbb{N} \to \mathbb{N}$  com  $x \mapsto x^2$ . Então f(2)=4, f(3)=9, f(20)=400.
- Ex:  $+: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$  com  $(x,y) \mapsto x$  mais y. Então +(2,2)=4, +(1,5)=6.



#### Definição

#### Funções Injetoras

- Se  $x \neq y \rightarrow f(x) \neq f(y)$  a função é dita injetora.
- Ou seja, elementos diferentes do domínio são mapeados em elementos diferentes no contradomínio.



#### Definição

#### Funções Sobrejetoras

- $\bullet \ \, \mathsf{Seja} \,\, f:D\to CD \,\, \mathsf{e} \,\, \mathsf{o} \,\, \mathsf{conjunto} \,\, \mathsf{iamgem} \,\, I=\{f(x),x\in D\}.$
- f é dita sobrejetora quando |I|=|CD|, ou seja, todos os elementos do contradomínio foram mapeados.



#### Definição

Funções Bijetoras São aquelas que são Injetoras e Sobrejetoras.

Mapeamento um para um.



#### Sumário

- Noções Matemáticas
  - Conjuntos
  - Sequências e Tuplas
  - Funções
  - Relações
  - Grafos
  - Linguagens e Cadeias



# Relações

#### Definição (Relações)

Uma relação ou predicado é um subconjunto de algum conjunto com alguma propriedade específica.



# Relações

- Exemplos:  $P \subseteq \mathbb{N}$  e  $P := \{x | x \text{ \'e par}\}.$
- $\bullet <\subseteq \mathbb{N} \times \mathbb{N} \text{ e} <:= \{(a,b)|a < b\}.$



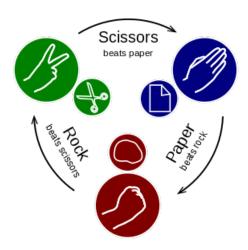
## Relações

#### Notação

Relações Se R é uma relação e  $x \in R$ , dizemos que x vale, x é verdadeiro ou simplesmente x tem a propriedade R.



## Relações





## Sumário

- Noções Matemáticas
  - Conjuntos
  - Sequências e Tuplas
  - Funções
  - Relações
  - Grafos
  - Linguagens e Cadeias



## Definição (Grafos)

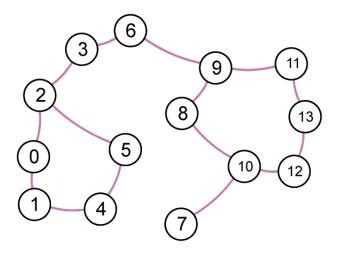
Um grafo não dirigido, ou grafo simples, é uma dupla G=(V,E) sendo V o conjunto de vértices e  $E\subseteq V\times V$  as arestas.



## Definição (Subgrafo)

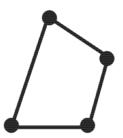
G'=(V',E') é um subgrafo de G(V,E), quando  $V'\subseteq V$  e  $E'\subseteq E$ .







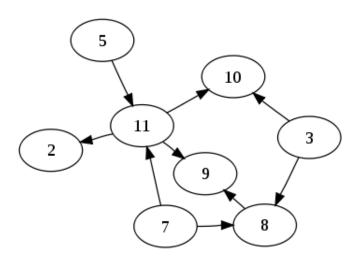






- Grafos também podem ser direcionados.
- Neste caso, a orientação das arestas faz diferença.







- Modelam vários problemas práticos.
- Teoria dos grafos estuda estes objetos.



## Sumário

- Noções Matemáticas
  - Conjuntos
  - Sequências e Tuplas
  - Funções
  - Relações
  - Grafos
  - Linguagens e Cadeias



## Definição (Alfabeto)

Um alfabeto é qualquer conjunto não vazio e finito de símbolos.

- Ex:  $\Sigma = \{0, 1\}.$
- Ex:  $\Sigma = \{a, \dots, z, A, \dots, Z\}.$
- Ex:  $\Gamma = \{0, 1, x, y, z\}.$



## Definição (Cadeias, Palavras ou Strings)

Cadeias, palavras ou *strings* são sequências finitas de símbolos de alfabetos.

- $\bullet$  Supondo  $\Sigma = \{0,1\}$ , então w = 01101101 é uma cadeia válida.
- Suponho  $\Sigma = \{a, \dots, z\}$ , então w = abracadabra é uma cadeia válida.



## Notação (Tamanho de Cadeias)

Seja  $w=w_1w_2w_3\dots w_n$  uma cadeia sobre o alfabeto  $\Sigma.$  Denotamos |w|=n como o tamanho de n.

Em particular, a cadeia vazia,  $\epsilon$ , tem tamanho  $|\epsilon|=0$ .



## Notação (Concatenação)

Suponha cadeias  $x=x_1x_2\dots x_n$  e  $y=y_1y_2\dots y_m$  sobre o alfabeto  $\Sigma.\ xy=x_1x_2\dots x_ny_1y_2\dots y_m$  denota a concatenação de x com y.

Em especial 
$$\underbrace{xxx\dots x}_{k} = x^{k}$$
.



### Notação (Inverso)

Seja  $w=w_1w_2\dots w_n$  uma cadeia sobre o alfabeto  $\Sigma$ .  $w^R=w_nw_{n-1}\dots w_1$  denota o inverso de w.



## Definição (Ordem lexicográfica)

A ordem lexicográfica de cadeias da precedência para cadeias menores, e em caso de empate, segue-se a ordem do dicionário.

• Para  $\Sigma = \{0,1\}$ , a ordem lexicográfica sobre todas as palavras sobre o alfabeto  $\Sigma$  é:

$$(\epsilon, 0, 1, 00, 01, 10, 11, 000, \ldots)$$



## Definição (Linguagem)

Uma linguagem L é um conjunto de palavras.

- Ex:  $L_1 = \{ww^R | \text{ w \'e uma cadeia sobre } \Sigma\}$
- Ex:  $L_1 = \{w | w = w^R\}$



## Notação $(\Sigma^*)$

 $\Sigma^*$  é a linguagem formada por todas as cadeias sobre o alfabeto  $\Sigma.$ 

- $\bullet \ \, \mathsf{Para} \, \, \Sigma = \{0,1\} \text{, } \, \Sigma^* = \{\epsilon,0,1,00,01,10,11,\ldots\}.$
- $\begin{array}{l} \bullet \ \ \mathsf{Para} \ \Sigma = \{A,C,G,T\}, \\ \Sigma^* = \{\epsilon,A,C,G,T,AA,AC,AG,AT,\ldots\}. \end{array}$



## Sumário

2 Lógica



# Lógica

• Por que a lógica é importante?



## Lógica

- Utilizamos lógica no dia a dia, na vida profissional e na pessoal.
- Elaboramos conceitos.
- Fazemos observações.
- Formalizamos teorias.
- Utilizamos raciocínio lógico para derivar conclusões a partir de premissas.
- Utilizamos demonstrações ou provas para convencer os outros que estamos corretos.



# Proposições

- Na matemática, uma proposição é uma sentença que pode ser falsa ou verdadeira, mas nunca as duas.
- Por exemplo:
  - "6 é par" é uma proposição verdadeira.
  - "4 é ímpar" é uma proposição falsa.



### Sumário

- 2 Lógica
  - Operadores Lógicos
  - Quantificadores
  - Definições
  - Teoremas
  - Provas
  - Técnicas de Prova



 Podemos combinar proposições para criar outras mais complexas através dos operadores lógicos.



#### Negação

Sejam p uma proposição.

- Não  $p(\neg p)$  é verdadeiro quando p é falso.
- Não  $p(\neg p)$  é falso quando p é verdadeiro.



### Conjunção

- p e q  $(p \land q)$  é verdadeiro quando p **e** q são verdadeiros.
- ullet Caso contrário,  $p \wedge q$  é falso.



### Disjunção

- p ou q  $(p \lor q)$  é verdadeiro quando p **ou** q são verdadeiros.
- $\bullet$  Caso contrário,  $p\vee q$  é falso.



### Implicação

- Se p então q  $(p \Rightarrow q)$  é verdadeiro quando p é falso **ou** q é verdadeiro.
- Caso contrário,  $p \Rightarrow q$  é falso.



#### Implicação

- Se p então q  $(p \Rightarrow q)$  é verdadeiro quando p é falso **ou** q é verdadeiro.
- Caso contrário,  $p \Rightarrow q$  é falso.
- ullet Se p é falso, dizemos que  $p\Rightarrow q$  é *vacuamente* verdadeiro.



#### Bi-implicação

- p se, e somente se, q ( $p \Leftrightarrow q$ ) é verdadeiro quando p e q são falsos ou p e q são verdadeiros.
- Caso contrário,  $p \Leftrightarrow q$  é falso.
- Se  $p \Leftrightarrow q$  é verdadeiro, dizemos que p e q são equivalentes.



## Sumário



- Operadores Lógicos
- Quantificadores
  - Definições
- Teoremas
- Provas
- Técnicas de Prova



- Considere a afirmação "x é par".
- Não podemos dizer se esta afirmação é verdadeira ou falsa, pois não sabemos quem é  $\boldsymbol{x}$ .



- Existem três maneiras básicas de conseguir obter um valor verdade para a afirmação.
  - ① Dizer quem é x. x=6 por exemplo tornaria a afirmação verdadeira.
  - 2 Para todo x inteiro, x é par. O que tornaria a afirmação incorreta, pois nem todo inteiro é par.



- As frases "para todo" e "existe" são chamados de quantificadores.
- Podemos utilizar os símbolos ∀ e ∃ para representá-los de maneira mais compacta.



• Talvez as coisas fiquem mais claras com uma definição matemática.



### Definição (Número par)

Um número x é dito par se e somente se existe um inteiro y tal que x=2y.



ullet Ou seja, estamos definido que um inteiro x é par, se e somente se existe algum y que multiplicado por 2 é igual a x.



 Utilizando a mesma estratégia, podemos definir os números ímpares.



### Definição (Número ímpar)

Um número x é dito ímpar se e somente se existe um inteiro y tal que x=2y+1.



- Os quantificadores podem ser aplicados à propriedades (relações).
- Seja  $P\subseteq \mathbb{N}$  a relação dos inteiros pares e  $I\subseteq \mathbb{N}$  a relação dos números ímpares.
  - ▶ Podemos dizer que  $\exists x P(x)$  é verdadeiro?
  - ▶ Podemos dizer que  $\exists x I(x)$  é verdadeiro?
  - Podemos dizer que  $\forall x P(x)$  é verdadeiro?
  - ▶ Podemos dizer que  $\forall x I(x)$  é verdadeiro?



#### Considerando os inteiros:

- O que  $\forall x \exists y (x = 2y)$  quer dizer?
- O que  $\exists x \exists y (x = 2y)$  quer dizer?
- $\bullet$  O que  $\forall x(\exists y(x=2y) \lor \exists y(x=2y+1))$  quer dizer?



• A ordem dos quantificadores também é muito importante.



Considerando < como a relação de menor entre inteiros:

- $\forall x \exists y (x < y)$  é verdadeiro?
- $\exists x \forall y (x < y)$  é verdadeiro?



### Sumário



- Operadores Lógicos
- Quantificadores
- Definições
- Teoremas
- Provas
- Técnicas de Prova



## Definições

### Definição (Definições)

Definições descrevem os objetos e noções que utilizamos. Uma definição pode ser simples, como a de conjuntos que utilizamos, ou complexa, como a de segurança em sistemas criptográficos.

Ao definir devemos utilizar uma linguagem livre de ambiguidades, para que ser bem claro sobre o que estamos falando.



# Afirmações

### Definição (Afirmações)

Afirmações matemáticas expressam que determinado objeto possui determinada propriedade.

Independente de serem verdadeiras ou falsas, também devem ser precisas.



### Definição (Prova)

Uma prova é uma sequência válida de passos dedutivos chegando a uma conclusão.



### Sumário

- 2 Lógica
  - Operadores Lógicos
  - Quantificadores
  - Definições
  - Teoremas
  - Provas
  - Técnicas de Prova



#### **Teoremas**

### Definição (Teoremas)

Teoremas são enunciados matemáticos verdadeiros e que podem ser provados.



#### Lemas

- Existem teoremas complexos de obter a prova.
- Para facilitar, podemos provar afirmações menores.
- Estas afirmações são chamadas de Lemas.
- Utilizamos Lemas para concluir os teoremas de maneira mais simples.



### Corolário

 Corolários são afirmações verdadeiras que decorrem imediatamente de um teorema.



### Sumário

- 2 Lógica
  - Operadores Lógicos
  - Quantificadores
  - Definições
  - Teoremas
  - Provas
  - Técnicas de Prova



- Uma prova ou demonstração matemática pode ser vista como um argumento para convencer outra pessoa que algo é verdadeiro.
- Uma boa prova deve ser a mais didática possível.
- Algumas estruturas são comuns dependendo da afirmação a qual se quer provar.



Queremos provar que p é verdadeiro:

- Prove diretamente que p é verdadeiro.
- ullet Assuma que p é falso e chegue em uma contradição.



Queremos provar que  $p \wedge q$  é verdadeiro:

ullet Prove diretamente que p vale e prove que q vale.



Queremos provar que  $p \lor q$  é verdadeiro:

- ullet Assuma que p é falso e deduza que q obrigatoriamente tem que ser verdadeiro.
- Assuma q falso e deduza que p obrigatoriamente tem que ser verdadeiro.
- Prove que p é verdadeiro.
- ullet Prove que q é verdadeiro.



Queremos provar que  $p \Rightarrow q$  é verdadeiro:

- ullet Assuma que p vale e deduza que q também vale.
- ullet Assuma q falso e deduza que p tem que ser falso também.



Queremos provar que  $p \Leftrightarrow q$  é verdadeiro:

 $\bullet \ \mathsf{Prove} \ p \Rightarrow q \ \mathsf{e} \ \mathsf{prove} \ q \Rightarrow p.$ 



Queremos provar que  $\exists x P(x)$  é verdadeiro:

ullet Basta encontrar um x que satisfaça a propriedade.



Queremos provar que  $\forall x P(x)$  é verdadeiro:

ullet Não assuma nada sobre x e prove que P(x) vale.



• Por exemplo, vamos provar que, para todo inteiro x, se x é ímpar, então x+1 é par.



- ullet Como queremos mostrar que o resultado vale para qualquer x, não podemos assumir absolutamente nada sobre ele.
- Como o teorema diz respeito a uma implicação (se, então), assumimos a primeira parte e tentamos provar a segunda.



### Demonstração.

 ${\sf Assuma}\ x\ {\sf impar}.$ 

Como x é ímpar, temos que existe um y tal que x = 2y + 1.

Adicionando 1 a ambos os lados, temos que x + 1 = 2y + 2.

Tome w = y + 1, substituindo temos: x + 1 = 2w.

Portanto x+1 é par.



### Sumário

- 2 Lógica
  - Operadores Lógicos
  - Quantificadores
  - Definições
  - Teoremas
  - Provas
  - Técnicas de Prova



#### Prova por casos

A prova por casos divide a prova em diversos casos, transformando-a em múltiplas provas mais simples.



 Vamos pegar o seguinte teorema para ilustrar a técnica de prova por casos:

#### Teorema

Para qualquer inteiro x, o inteiro x(x+1) é par.

• Temos dois casos: x é par ou x é ímpar.



### Demonstração.

Caso 1:  $x \notin par$ .

- Como x é par, temos que existe um y tal que x = 2y.
- Assim, temos que:

$$x(x+1) = 2y(2y+1)$$

- Tome w = 2(y+1).
- Assim:

$$x(x+1) = 2y(2y+1) = 2w$$

• Logo x(x+1) é par.



### Demonstração.

Caso 2:  $x \in \text{impar}$ .

- Como x é ímpar, temos que existe um y tal que x = 2y + 1.
- Assim, temos que:

$$x(x+1) = (2y+1)(2y+2) = (2y+1)(y+1)2$$

- Tome w = (2y+1)(y+1).
- Assim:

$$x(x+1) = (2y+1)(2y+2) = (2y+1)(y+1)2 = 2w$$

• Logo x(x+1) é par.



#### Prova por Construção

Muitos teoremas afirmam a existência de um tipo particular de objeto.

Provas por construção mostram que é possível construir um objeto do referido tipo.



### Exemplo

Um grafo k-regular é aquele que todos os nós tem grau k.

#### **Teorema**

Para qualquer n > 2 par, existe um grafo 3-regular com n nós.

Demonstração.

$$E = \{(i,i+1)|0 \leq i \leq n-2\} \cup \{n-1,0\} \cup \{(i,i+n/2)|0 \leq i \leq n/2-1\}$$





# Prova por Contradição

#### Prova por Contradição

Assume-se que um teorema é falso. Uma vez concluído o absurdo, podemos concluir que o teorema é de fato verdadeiro.



# Exemplo

Teorema

 $\sqrt{2}$  é irracional.

Demonstração.



### Exemplo

Suponha  $\sqrt{2}$  racional.

Logo  $\sqrt{2}=\frac{n}{m}$ , uma fração reduzida. Obviamente, n ou m é ímpar.

Elevando os dois lados ao quadrado temos:

 $2=\frac{n^2}{m^2}$ , e portanto  $n^2=2m^2$ , então  $n^2$  é par, e n também é.

Se n é par, temos n=2k para algum k.

Substituindo, temos  $n^2=(2k)^2=4k^2$ . Logo  $4k^2=2m^2$  e portanto  $m^2=2n^2$  o que torna  $m^2$  par e consequentemente m par. Mas n e m não podem ser simultaneamente pares. Contradição.

 $\sqrt{2}$  tem que ser irracional.



# Prova por Indução

### Prova por Indução

Prova-se o caso base. Assume que a propriedade vale para todo k < n. Tentamos provar que vale para n utilizando as hipóteses de indução e o caso base.



### Prova por Indução

#### Teorema

O n ésimo termo de uma P.A de razão r é  $a_0 + rn$ .

#### Demonstração.

Para n=0,  $a_0=a_0$ . Suponha que a propriedade vale para todo k< n.

Sabemos que  $a_n = a_{n-1} + r$ , pela definição da P.A. Aplicando a hipótese de indução sobre  $a_{n-1}$ , temos:

$$a_n = a_0 + r(n-1) + r = a_0 + rn$$