# MATEMÁTICA DISCRETA

AULA 3

Profª Thamara Petroli

## CONVERSA INICIAL

### Indução matemática e relações

Olá! Visto que nas primeiras aulas aprendemos basicamente conceitos sobre lógica e conjuntos, observamos também que alguns conceitos lógicos estão relacionados com propriedades importantes de conjunto, além disso vimos que nem tudo se trata de números. Destacando a palavra *relação*, você sabe o que ela significa na matemática? E mais, a lógica nos trouxe formas de argumentar e validar sentenças, mas existem outras formas de fazer a mesma coisa?

Esta aula veio justamente para responder a essas preguntas. Nela, vamos trabalhar com os conceitos de relações e de indução matemática, uma outra ferramenta que utiliza conceitos de lógica para verificarmos e argumentarmos as sentenças/provas matemáticas que vamos fazer.

## TEMA 1 – RELAÇÕES

Falar de matemática e não falar de relações ou comparações é um pouco estranho, pois, intuitivamente, uma relação é uma comparação entre objetos, e está presente no nosso dia a dia constantemente, desde quando estamos em uma loja comparando dois produtos, ou as vantagens e as desvantagens de fazer uma viagem. Podemos dizer ainda que, se temos dois ou mais objetos, existe uma ligação entre eles, seja ela por alguma característica específica ou classificação.

Na matemática, a maneira mais direta de expressar relações entre dois conjuntos é usar pares ordenados compostos pelos elementos desses dois conjuntos. Por essa razão, pode-se dizer que uma *relação* é um conjunto de pares ordenado, no sentido que é um conjunto de listas de dois elementos. Se pensarmos que a relação $R$ funciona como uma regra, ou teste, dizer que dois elementos $x$ e $y$ estão relacionados por $R$, é o mesmo que dizer que esses elementos obedecem à mesma regra $R$, e denotamos como $xRy$.

Por exemplo: seja $R = \{(1,3), (2,2), (3,0)\}$ essa relação nos diz que $1$ está relacionado com o $3$, $1R3$, o $2$ está relacionado com $2$, $2R2$, e o $3$ está relacionado com o $0$, $3R0$.

$$(1,3) \in R, (2,2) \in R, (3,0) \in R$$

Mas note que o $2$ não está relacionado com o $3$, assim $(2,3) \notin R$.

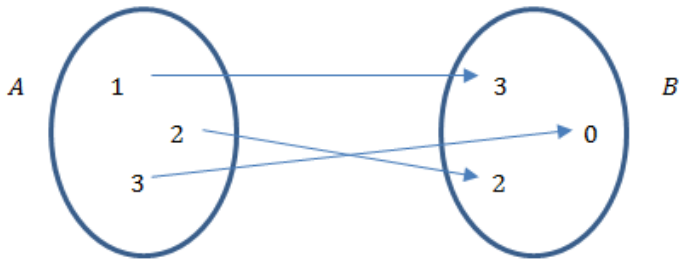
Esse exemplo nos mostra outra forma de pensarmos em relação, dizer que $xRy$, $x$ está relacionado com $y$ pela $R$ significa que $(x,y) \in R$. Logicamente falando, $xRy \Leftrightarrow (x,y) \in R$.

Vejamos outro exemplo: a relação de menor ou igual a no conjunto dos inteiros. Escrevendo essa relação temos $\{(x,y): x,y \in \mathbb{Z} \wedge y - x \in \mathbb{N}\}$, ou seja, procuramos valores inteiros dos quais a sua diferença seja um natural, ou que a diferença seja um inteiro não negativo; mas que no fundo estamos procurando a relação $\{(x,y): x,y \in \mathbb{Z} \wedge x \leq y\}$.

## 1.1 Conceitos iniciais

Formalizando o conceito de relações, temos que uma *relação binária* $R$ de um conjunto $A$ para um conjunto $B$ é um conjunto de pares ordenados $(a,b) \in A \times B$, e denotamos tal relação por $aRb$.

Se os conjuntos $A$ e $B$, tem um número pequeno de elementos, podemos representar tais relações por meio do diagrama, como mostrado a seguir, em que para cada elemento do conjunto $A$, direcionamos uma seta ao elemento do conjunto $B$.




Tal exemplo mostra a relação $R = \{1,3), (2,2), (3,0)\}$, em que $A = \{1,2,3\}$ e $B = \{3,0,2\}$.

Podemos ainda encontrar relações sobre um único conjunto, relações do tipo de $A$ *em* $A$, ou *sobre* $A$.

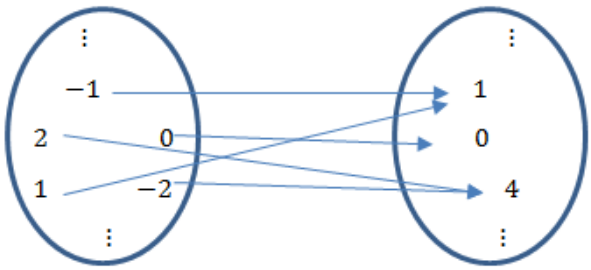
Exemplo: seja $A = \{1,2,3,4\}$. Defina o conjunto que satisfaz a relação $R = \{(a,b): a \; divide \; b\}$.

Note que estamos falando de uma *relação de* $A$ *em* $A$, e mais $(a,b) \in R$, assim queremos todos os pares ordenados que tais que $a$ e $b$ não excedam o valor $4$ e que haja a divisão de $b$ por $a$, logo temos:

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

Em uma relação $R = \{(a, b) \in A \times B\}$, dizemos que o elemento $a$ pertence ao *domínio* de $R$, denotado por $Dom(R)$ e $b$ pertence à *imagem* ou contradomínio de $R$, que denotamos por $Img(R)$. De maneira que $Dom(R) \subseteq A$ e $Img(R) \subseteq B$, mas não necessariamente o domínio e a imagem coincidem com os conjuntos $A$ e $B$.

Exemplo: seja $R$ a relação $\{(x, x^2): x \in \mathbb{Z}\}$. Primeiro note que temos uma relação de $\mathbb{Z}$ nele mesmo, em que no domínio de $R$ são todos os elementos de $\mathbb{Z}$, mas a imagem é apenas um subconjunto de $\mathbb{Z}$, pois para cada elemento $x$, a relação leva ao seu quadrado perfeito, vejamos um esquema parcial em diagramas:




Logo, a imagem $Im(R) = \{0, 1, 4, 9, 16, 25, \cdots\} \subseteq \mathbb{Z}$.

Vale a pena observar que em muitos casos nos deparamos com relações que envolvem ordenação, sendo assim são respeitadas as regras de comparação do espaço que estamos trabalhando, por exemplo, como a maioria dos exemplos que estamos trabalhando são relações binárias definidas sobre os números reais, então os sinais de comparações utilizados são $=, \leq, \geq, <, >, \neq$, etc.

## 1.2 Tipos de relações

Relações restritas: seja $R$ uma relação de $A$ em $B$, e sejam $A' \subset A$ e $B' \subset B$. Então a *restrição* de $R$ a $A'$ e $B'$ é o conjunto dos pares de $(a, b) \in R$.

- Exemplo: seja $R$ a relação dos inteiros aos reais, $xRy$, em que $y$ é a raiz quadrada de $x$. A relação restrita de $R$ é dada por $A' = \mathbb{N}$ e $B' = \mathbb{R}$, pois sabemos que não existe raiz negativa definida nos reais, logo restringimos o domínio que era $Dom(R) = \mathbb{Z}$, para $A'$.

Relação identidade: é a relação $R$ de $A$ nele mesmo definida como $\{(x,x): x \in A\}$. Ou podemos definir como a relação identidade restrita ao seu domínio $A$.

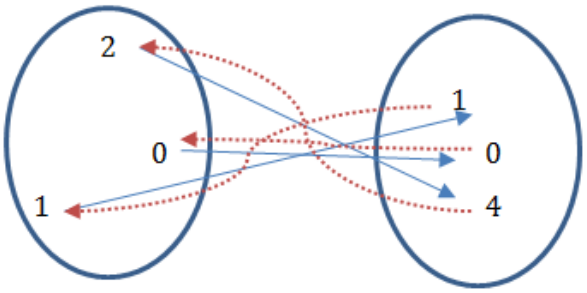
- Exemplo: se $\mathrm{A} = \{0,1,2\}$, então, $\mathrm{R} = \{(0,0),(1,1),(2,2)\}$.

Relação inversa: se $R$ é uma relação de $A$ em $B$, então, sua *relação inversa*, denotada por $R^{-1}$, é a relação de $B$ em $A$.

$$R^{-1} = \{(b,a): (a,b) \in R\}$$

Podemos definir ainda como aquela $bR^{-1}a$ se, e somente se $aRb$. Note ainda $Dom(R^{-1}) = Img(R)$ e $Img(R^{-1}) = Dom(R)$.

- Exemplo: seja a relação dada pelo diagrama, destacada pelas setas azuis, então, a sua respectiva relação inversa é dada pelas setas vermelhas:




Composição de relação: sejam $R$ e $S$ duas relações. Então a *relação composta* de $R$ com $S$, denotada por $S \circ R$, é definida como:

$$S \circ R = \{(a,c): (\exists b)(a,b) \in R \wedge (b,c) \in S\}$$

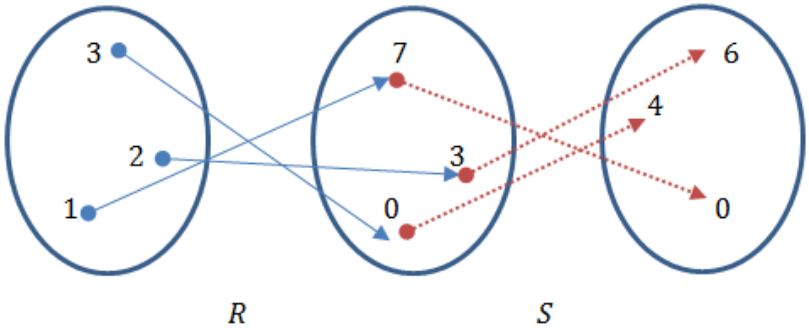
Note que deve existir um elemento na imagem de $R$ que esteja no domínio de $S$, ou seja, $Img(R) \cap Dom(S) = \{b\}$.

- Exemplo: sejam $\mathrm{R} = \{(1,7),(2,3),(3,0)\}$ e $\mathrm{S} = \{(7,0),(3,6),(0,4)\}$. Logo a composição $\mathrm{S} \circ \mathrm{R} = \{(1,0),(2,6),(3,4)\}$.

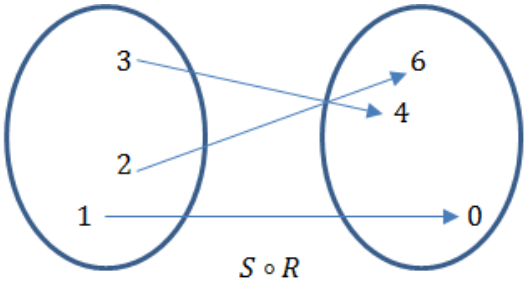
Observe que para que o par ordenado $(1,0) \in S \circ R$, foram tomados os pares ordenados $(1,7) \in R$ e $(7,0) \in S$.

Assim como o par $(2,6) \in S \circ R$, foram tomados $(2,3) \in R$ e $(3,6) \in S$.

Analisando por meio de diagramas:




Ou:




Inversa da composição: sejam $R$ e $S$ relações, então a sua inversa é dada como:

$$(S \circ R)^{-1} = R^{-1} \circ S^{-1}$$

Ou seja, a *inversa da composição* é a composição das inversas.

- Exemplo: tomando o exemplo anterior tínhamos $\mathrm{R} = \{(1,7), (2,3), (3,0)\}$, $\mathrm{S} = \{(7,0), (3,6), (0,4)\}$, $\mathrm{S} \circ \mathrm{R} = \{(1,0), (2,6), (3,4)\}$. Com $\mathrm{R}^{-1} = \{(7,1), (3,2), (0,3)\}$, $\mathrm{S}^{-1} = \{(0,7), (6,3), (4,0)\}$, logo $(\mathrm{S} \circ \mathrm{R})^{-1} = \{(0,1), (6,2), (4,3)\}$ e $\mathrm{R}^{-1} \circ \mathrm{S}^{-1} = \{(0,1), (6,2), (4,3)\}$.

Podemos ainda encontrar composições do tipo $R^{-1} \circ R$, ou $R \circ R^{-1}$, essas composições, apesar de parecerem iguais, são diferentes e devemos tomar um cuidado ao operá-las. Por exemplo, se $R = \{(1,2), (1,7), (2,7)\}$ então $R^{-1} = \{(2,1), (7,1), (7,2)\}$ e, assim, $R^{-1} \circ R = \{(1,1), (7,7), (2,7), (2,2)\}$ e $R \circ R^{-1} = \{(2,2), (1,1), (1,2), (2,1)\}$. Além do mais, essas composições diferem da identidade dessa relação $I = \{(1,1), (2,2), (7,7)\}$.

## 1.3 Propriedades

Seja $R$ uma relação definida em um conjunto $A$. Então, valem as seguintes propriedades:

- $R$ é *reflexiva* sobre $A$, se e somente se, $(\forall\, a \in A)\, aRa$, ou seja, $(a,a) \in R$ para todo $a \in A$.
- $R$ é *antirreflexiva* sobre $A$, se e somente se, $(\forall\, a \in A) a \neg Ra$, ou seja, $(a,a) \notin R$ para todo $a \in A$.
- $R$ é *simétrica* sobre $A$, se e somente se, $(\forall\, a,b \in A)\, aRb \rightarrow bRa$, ou seja, $(a,b) \in R$ para todo $a,b \in A$.
- $R$ é *antissimétrica* sobre $A$, se e somente se, $(\forall\, a,b \in A)\, aRb \wedge bRa \rightarrow a = b$, ou seja, se $(a,b) \in R$ e $(b,a) \in R$, então $a = b$.
- $R$ é *transitiva* sobre $A$, se e somente se, $(\forall\, a,b,c \in A)\, aRb \wedge bRc \rightarrow aRc$, ou seja, se $(a,b) \in R$ e $(b,c) \in R$, então $(a,c) \in R$.

Exemplo: seja $R = \{(1,1),(1,2),(2,1),\ (1,3)\}$, observe que essa relação é reflexiva somente para o elemento $(1,1) \in R$, mas para os demais elementos é antirreflexiva. Ela também é simétrica e antissimétrica, pois o elemento $(1,2) \in R$ assim como $(2,1) \in R$, tornando-a simétrica, mas para o elemento $(1,3) \in R$ ela não é simétrica, pois $(3,1) \notin R$. Além de tudo ela não é transitiva, pois $(2,1) \in R$ e $(1,3) \in R$, mas $(2,3) \notin R$.

Exemplo: considere a relação $<$ (estritamente menor que) sobre os números naturais. Primeira observação que temos é que $<$ não é reflexiva, já que $2 < 2$ é falso. Ela também é antirreflexiva, pois não podemos fazer a comparação $x < x$, seja qual for o natural escolhido. Essa relação é não é simétrica, pois $1 < 2$ mas $2 \not< 1$. Mas ela é antissimétrica, pois $\forall x,y \in \mathbb{N}$ se $x < y$ e $y < x$ então $x = y$. E ela também é transitiva, pois $\forall x,y,z \in \mathbb{N}$ se $x < y\ e\ y < z$ então $x < z$.

Observação: dizer que uma relação tem potência $n$, $R^n$, equivale a dizer que a operação de composição foi realizada $n$-vezes, isto é, $R^n = \underbrace{R \circ R \circ R \circ \ldots \circ R}_{n-vezes}$. Por exemplo: $R^3 = R^2 \circ R = (R \circ R) \circ R$. E como consequência, temos que $R$ é transitiva se e somente se $R^n \subseteq R$.

## 1.4 Relações utilizando matrizes

Primeiramente definimos uma *matriz booleana* quando seus elementos apresentam apenas elementos com valores lógicos $V$ ou $F$, no caso utilizamos os valores $1$ e $0$, respectivamente.

Assim, sejam $A = \{a_1, a_2, \dots a_m\}$ e $B = \{b_1, b_2, \dots, b_n\}$ conjuntos finitos, onde $n(A) = m$ e $n(B) = n$. E seja $R$ a relação de $A$ para $B$. Uma das maneiras de representar essa relação é por meio de uma matriz $M$, com $m$-linhas e $n$-colunas, definida da seguinte maneira:

$$m_{ij} = \begin{cases} 1, se\ (a_i, b_j) \in R \\ 0, se\ (a_i, b_j) \notin R \end{cases}$$

Traduzindo, para cada elemento da matriz $M$, se a relação entre $a_i$ e $b_j$ é verdadeira ela recebe o valor $1$, caso seja falsa recebe o valor $0$, e assim preenchemos a entrada da matriz $m_{ij}$.

Exemplo: seja $R = \{(4,4), (6,9), (2,5), (7,4)\}$. Escolhendo $A = \{2,4,6,7\}$ e $B = \{4,5,9\}$, então a matriz booleana dessa relação é dada por

$$M = \left(\begin{array}{c|cccc} & 2 & 4 & 6 & 7 \\ \hline 4 & 0 & 1 & 0 & 1 \\ 5 & 1 & 0 & 0 & 0 \\ 9 & 0 & 0 & 1 & 0 \end{array}\right)$$

Obs.: nesse tipo de representação de relação, as propriedades vistas anteriormente devem ser analisadas em cada elemento da matriz. Exemplo: seja a relação $R$ dada pela matriz:

$$M = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

Essa relação é reflexiva, pois $m_{11} = m_{22} = m_{33} = 1$ é simétrica porque a matriz é simétrica, e não é antissimétrica, pois $m_{12} = m_{21} = 1$.

Exemplo: seja $R$ uma relação de $A$ em $B$, onde $aRb$ se, e somente se $a \geq b$. Escolhendo $A = \{1,2,3,4\}$ e $B = \{0,1,2,3\}$, então a matriz booleana dessa relação é dada por

$$M = \left(\begin{array}{c|cccc} \geq & 1 & 2 & 3 & 4 \\ \hline 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 2 & 0 & 1 & 1 & 1 \\ 3 & 0 & 0 & 1 & 1 \end{array}\right)$$

Note que $R$ é simétrica pois $m_{ii} = 1 (\forall i)$ não é simétrica, pois a matriz não é simétrica (ou não coincide com a sua transposta) e não é antissimétrica pois $(2 \geq 1)$ mas $(2 \not\leq 1)$, isto é $(2,1) \in R$ mas $(1,2) \notin R$, logo existirá a igualdade dos elementos apenas quando de fato eles são iguais, pois para os demais casos não é possível fazer a comparação.

## TEMA 2 – RELAÇÕES DE EQUIVALÊNCIA

Com o decorrer do nosso estudo, vamos perceber que encontramos expressões ou tipos de relações mais repetidamente do que as outras, como a relação de igualdade " $=$ ", ou ainda de congruência " $\cong\cong$ ". Esse tipo de relação, a de congruência, é bastante comum quando queremos comparar elementos da geometria, como triângulos, dizer que dois triângulos são congruentes se eles têm os mesmos valores para lados e ângulos, ou seja, quando têm a mesma forma (Scheinerman, 2016).

Dizer que dois objetos são congruentes é muito mais do que dizer que eles são iguais. Quando falamos em termos de relações, falar sobre congruência é o mesmo que falar sobre *relações de equivalências*, e definimos uma relação de equivalência como:

- Seja $\mathrm{R}$ uma relação de um conjunto $\mathrm{A}$. Dizemos que $\mathrm{R}$ é uma relação de equivalência se $\mathrm{R}$ é reflexiva, simétrica e transitiva.

Exemplo: seja $A$ o conjunto de todas as retas do plano, e seja $R$ uma relação sobre $A$, em que $rRs$ se, e somente se $r = s$ ou $r \cap s = \emptyset$, para retas $r, s \in A$.

Essa relação é uma relação de equivalência, pois, além de ser uma relação sobre restas paralelas da geometria plana, é obvio que uma reta é igual a ela mesma, $rRr$ reflexividade. É simétrica, pois $r = s$ ou $s = s$, ou ainsa $r \cap s = s \cap r = \emptyset$; e é transitiva, pois se $r = s$ e $s = t$ então $r = t$.

Outra relação de equivalência importante na matemática é a *congruência de números (módulo $n$)*, e a definimos como:

Seja $n$ um inteiro positivo. Dizemos que os inteiros $x$ e $y$ são *congruentes módulo* $n$ e escrevemos $x \equiv y (mod\ n)$ se $n$ divide $x - y$.

Em outras palavras é o mesmo que dizer $x - y$ é um múltiplo de $n$.

Exemplos:

- $3 \equiv 13\ (mod\ 5)$ porque $3 - 13 = -10 = -2 \cdot 5$ um múltiplo de $5$.
- $2 \equiv 2\ (mod\ 3)$ porque $2 - 2 = 0 = 0 \cdot 3$ um múltiplo de $3$.
- $17 \not\equiv 3\ (mod\ 5)$ porque $17 - 3 = 14$ não um múltiplo de $5$.

Como já falamos, a congruência módulo $n$ é uma relação de equivalência. De fato, ela é reflexiva pois para qualquer $x$, $x \equiv x\ (mod\ n)$, pois $x - x = 0 = 0 \cdot n$ um múltiplo de $n$. É simétrica, pois tomando $x, y$ inteiros, se $x \equiv y$ então $x -$

$y = k \cdot n$, em que $k$ denota o múltiplo de $n$,e se $y \equiv x$ então $y - x = (-k) \cdot n$, ou seja, (-k) também é um múltiplo de $n$, logo, vale a simetria. E, por fim, a transitividade, se $x \equiv y$ e $y \equiv z$, então $x - y = k \cdot n$ e $y - z = p \cdot n$, então fazendo da segunda equação $y = z + p \cdot n$ e substituindo na primeira equação $x - (z + p \cdot n) = k \cdot n \Leftrightarrow x - z - p \cdot n = k \cdot n \Leftrightarrow x - z = k \cdot n + p \cdot n \Leftrightarrow x - z = (k + p) \cdot n$ um múltiplo de $n$. Logo $x \equiv z\ (mod\ n)$.

## 2.1 Classes de equivalência

Seja $R$ uma relação sobre um conjunto $A$, definimos a *classe de equivalência* do elemento $a \in A$ o conjunto:

$$\forall a \in A, \qquad [a]_R = \{x \in A : xRa\}$$

Para qualquer elemento $a \in A$, a classe de equivalência é o conjunto com todos os elementos que estão relacionados com $a$.

Exemplo: vamos determinar algumas classes da relação congruência módulo 2.

Sabemos que $R = \{(x, y) : x \equiv y\ (mod\ 2)\}$, assim, se $x \equiv y\ (mod\ 2)$, então, $x - y = 2\ \cdot n$, ou ainda $x = 2 \cdot n + y$, para algum $n \in \mathbb{Z}$. Então, para determinar as classes $[y]_R$, basta encontrar todos os valores $x$, da forma $x = 2 \cdot n + y$,ou ainda podemos pensar que são todos aqueles que tem resto $y$ quando divididos por 2. Logo, temos duas classes de equivalência, que são:

$$[0]_R = \{\ldots -6, -4, -2, 0, 2, 4, 6 \ldots\}$$
$$[1]_R = \{\ldots -5, -3, -1, 1, 3, 5, 7 \ldots\}$$

Ainda temos que se $R$ é uma relação de equivalência sobre um conjunto $A$, então as afirmações abaixo são equivalentes:

- $aRb$
- $[a]_R = [b]_R$
- $[a]_R \cap [b]_R \neq \emptyset$

Vamos tentar entender como elas funcionam. Vamos olhar primeiro para a afirmação de que $aRb \rightarrow [a]_R = [b]_R$. Se tomarmos um elemento $c \in [a]_R$, então por definição sabemos que existe a relação $cRa$, sabendo que $R$ é uma relação de equivalência então vale a propriedade de transitividade, e mais estamos admitindo $aRb$, logo se $cRa \wedge aRb$ então $cRb$, e assim segue $c \in [b]_R$. E

o mesmo raciocínio vale se tomarmos $d \in [b]_R$, vamos concluir que $d \in [a]_R$. Dessa forma, sabendo que $aRb$, e tomando qualquer elemento de $[a]_R$, ou $[b]_R$, concluiremos que esse elemento está em $[b]_R$, ou respectivamente $[a]_R$. E então segue $[a]_R = [b]_R$.

Agora, se olharmos para a segunda afirmação $[a]_R = [b]_R \rightarrow [a]_R \cap [b]_R \neq \emptyset$. Como $R$ é reflexiva (pois é uma relação de equivalência), sabemos que existe pelo menos $a \in [a]_R$, e mais $[a]_R = [b]_R$, então $a \in [b]_R$, logo $[a]_R \cap [b]_R \neq \emptyset$.

E se olharmos para última implicação $[a]_R \cap [b]_R \neq \emptyset \rightarrow aRb$. Sabendo que a interseção é não vazia, então existe pelo menos um elemento $c \in [a]_R \cap [b]_R$, então $c \in [a]_R \rightarrow cRa$ e $c \in [b]_R \rightarrow cRb$, e pela simetria e transitividade de $R$, segue $aRb$.

Devemos dar um certo destaque na argumentação que fizemos, pois aqui utilizamos ferramentas lógicas para mostrar a veracidade das equivalências. Provamos um teorema: *"*se $R$ é uma relação de equivalência sobre um conjunto $A$, então as afirmações a seguir são equivalentes":

- $aRb$
- $[a]_R = [b]_R$
- $[a]_R \cap [b]_R \neq \emptyset$"

## 2.2 Partições

- Seja A um conjunto. Uma partição de A, denotada $\mathcal{P}(A)$, é um conjunto de conjuntos não vazios, disjuntos dois a dois, cuja união é A.

  A partir dessa definição, quatro pontos devem ser notados:

- Uma partição é um conjunto de conjuntos em que cada elemento da partição é um subconjunto de $A$.
- Uma partição é não vazia.
- Uma partição tem elementos dois a dois disjuntos (interseção vazia de duas partições diferentes).
- União descreve o conjunto todo.

  Vejamos um exemplo: Seja $A = \{0, 1, 2\}$, então:

$$\mathcal{P}(A) = \{\{0\}, \{1\}, \{2\}\}$$

Essa é uma partição de $A$. Poderíamos ter também $\mathcal{P}(A) = \{\{0\}, \{1, 2\}\}$, ou seja, podemos tomar a partição como no é conveniente, desde que satisfaça a

definição de subconjuntos não vazios, dois a dois disjuntos $(\{0\} \cap \{1\} = \emptyset, \{0\} \cap \{2\} = \emptyset,\ \{2\} \cap \{1\} = \emptyset, \{0\} \cap \{1,2\} = \emptyset)$, união leva ao conjunto todo.

Pensando no conceito de classes de equivalência, e no teorema que acabamos de ver, podemos perceber que as classes de equivalência são partições. E mais, como estamos trabalhando com relações podemos afirmar que *uma partição é uma classe de equivalência de* $A$ (Scheinerman, 2016).

## 2.3 Ordenações parciais

Quando estamos trabalhando com relações, frequentemente encontramos exemplos em que usamos relações para ordenar elementos de um conjunto. Sendo assim:

- Uma relação $\mathrm{R}$ em um conjunto $\mathrm{A}$ é chamada de *ordenação parcial* se ela for reflexiva, antissimétrica e transitiva. E esse conjunto $\mathrm{A}$ é chamado de *conjunto parcialmente ordenado*, ou *poset* (terminologia derivada do inglês *partially ordered set*) e o denotamos como $(\mathrm{A}, \mathrm{R})$.

Exemplo: vamos mostrar que a relação "$\geq$", maior ou igual a, é parcialmente ordenado em $\mathbb{Z}$. Esse é um clássico exemplo de ordem parcial.

- Reflexiva: se $a \in \mathbb{Z}$, então satisfaz $a \geq a$.
- Antissimétrica: sejam $a, b \in \mathbb{Z}$, se $a \geq b$ e $b \geq a$, então $a = b$.
- Transitiva: sejam $a, b, c \in \mathbb{Z}$, se $a \geq b$ e $b \geq c$, então segue $a \geq c$.

Como $\mathbb{Z} \subset \mathbb{R}$,é fácil mostrar a ordenação, pois por definição a reta real é um conjunto ordenado.

Exemplo: vamos mostrar que a relação "$\subseteq$", inclusão, é parcialmente ordenado no conjunto $A$.

- Reflexiva: seja $B$ um subconjunto de $A$, então $B \subseteq B$.
- Antissimétrica: sejam $B, C \subseteq A$, se $B \subseteq C$ e $C \subseteq B$, então $B = C$.
- Transitiva: sejam $B, C, D \subseteq A$, se $B \subseteq C$ e $C \subseteq D$, então segue $B \subseteq D$.

Em geral, quando estamos trabalhando com *posets*, utilizamos a notação $\preccurlyeq$ para indicar que existe uma relação de ordenação. Assim, quando dizemos $a \preccurlyeq b$ significa, $(a, b) \in R$ em um poset arbitrário $(A, R)$. Ainda podemos encontrar a notação $a \prec b$,, significando que $a \preccurlyeq b$, mas $a \neq b$.

Quando dois elementos $a, b$ de um poset $(A, \preccurlyeq)$, eles são chamados de *comparáveis* se ou $a \preccurlyeq b$ ou $b \preccurlyeq a$. Caso contrário, eles são chamados de *incomparáveis*.

Um tipo de ordem que utiliza esse tipo de relação é tem um papel muito importante na matemática, é a *ordem lexicográfica*; baseada na ordem das letras do alfabeto, na matemática ela possibilita comparar elementos do plano cartesiano.

Dados dois *posets* $(A_1, \preccurlyeq_1)$ e $(A_2, \preccurlyeq_2)$. A ordem lexicográfica $\preccurlyeq$ em $A_1 \times A_2$ é definida:

$$(a_1, a_2) \prec (b_1, b_2) \Leftrightarrow a_1 \prec b_1 \vee (\, a_1 = b_1 \wedge a_2 \prec b_2)$$

para todo $(a_1, a_2), (b_1, b_2) \in A_1 \times A_2$, ou seja, o primeiro elemento do par ordenado for menor que o primeiro elemento do segundo par ordenado, ou iguais (comparação correspondente aos elementos de $A_1$), e o segundo elemento do primeiro par ordenado for menor que o segundo elemento do segundo par ordenado (comparação entre os elementos de $A_2$).

Por exemplo: seja o *poset* $(\mathbb{Z} \times \mathbb{Z}, \preccurlyeq)$ onde $\mathbb{Z} \times \mathbb{Z} = \{(2,5), (2,8), (5,5), (5,9), (6,11)\}$, em que a ordem lexicográfica $\preccurlyeq$ é a relação de ordem usual $\leq$. Compare $(2,5) \prec (2,8)$, $(2,8) \prec (5,5)$, $(5,9) \prec (6,11)$.

De acordo com a definição de ordem lexicográfica, devemos comparar ordenada a ordenada, então vamos à primeira comparação $(2,5) \prec (2,8)$: aqui $a_1 = 2,\ a_2 = 5,\ b_1 = 2,\ b_2 = 8$ assim $a_1 = 2 = b_1$ e $a_2 = 5 \leq 8 = b_2$. Satisfaz a definição.

Da segunda comparação $(2,8) \prec (5,5)$: aqui $a_1 = 2, a_2 = 8,\ b_1 = 5,\ b_2 = 5$ assim $a_1 = 2 \leq 5 = b_1$ e $a_2 = 8 \geq 5 = b_2$. Logo, não satisfaz a definição, a segunda condição não é satisfeita!

Da terceira comparação $(5,9) \prec (6,11)$: aqui $a_1 = 5, a_2 = 6,\ b_1 = 9,\ b_2 = 11$ assim $a_1 = 6 \leq 9 = b_1$ e $a_2 = 6 \leq 11 = b_2$. Satisfaz a definição.

Podemos generalizar a definição da ordem lexicográfica para $n$ posets, logo a ordem lexicográfica $\preccurlyeq$ em $A_1 \times A_2 \times \ldots \times A_n$ é definida:

$$(a_1, a_2, \ldots, a_n) \prec (b_1, b_2, \ldots, b_n) \Leftrightarrow$$

$$a_1 \prec b_1 \vee [(\exists i > 0 \colon a_1 = b_1, a_2 = b_2, \ldots, a_i = b_1) \wedge a_{i+1} \prec b_{i+1}]$$

para todo $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in A_1 \times A_2 \times \ldots \times A_n$.

O exemplo a seguir mostra um esquema dessa generalização, em que destacamos os pares ordenados menores que $(3,2)$:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | |
| $(1,7)$ | $(2,7)$ | $(3,7)$ | $(4,7)$ | $(5,7)$ | $(6,7)$ | $(7,7)$ | … |
| $(1,6)$ | $(2,6)$ | $(3,6)$ | $(4,6)$ | $(5,6)$ | $(6,6)$ | $(7,6)$ | … |
| $(1,5)$ | $(2,5)$ | $(3,5)$ | $(4,5)$ | $(5,5)$ | $(6,5)$ | $(7,5)$ | … |
| $(1,4)$ | $(2,4)$ | $(3,4)$ | $(4,4)$ | $(5,4)$ | $(6,4)$ | $(7,4)$ | … |
| $(1,3)$ | $(2,3)$ | $(3,3)$ | $(4,3)$ | $(5,3)$ | $(6,3)$ | $(7,3)$ | … |
| $(1,2)$ | $(2,2)$ | $(3,2)$ | $(4,2)$ | $(5,2)$ | $(6,2)$ | $(7,2)$ | … |
| $(1,1)$ | $(2,1)$ | $(3,1)$ | $(4,1)$ | $(5,1)$ | $(6,1)$ | $(7,1)$ | … |

## TEMA 3 – MÉTODOS DE PROVA 1

Na matemática é comum encontrarmos os termos *definição*, *teorema*, *corolário*, *axiomas*, *postulados*, *demonstração*, entre outros. Inclusive no decorrer das aulas vistas até aqui falamos bastante o termo *definição* e nos deparamos com *teorema*.

Formalmente, uma demonstração é um argumento válido que estabelece a verdade de uma sentença matemática. Nela, utilizamos hipóteses já conhecidas, definições, teoremas, axiomas etc. como verdade, para assim chegar à conclusão desejada. Existem várias técnicas parra construir uma demonstração, escolher o tipo de prova adequada depende muito de para quem a prova é dirigida, e gosto pessoal.

### 3.1 Terminologia

Antes de apresentar algumas técnicas de demonstração ou prova, vamos esclarecer alguns termos técnicos.

A maioria das demonstrações estão ligadas a um teorema, que é uma sentença que se pode demonstrar como verdade. Usualmente, utilizamos esse termo quando as sentenças apresentam tem alguma importância. Os teoremas “menos importantes” chamamos de *proposições*.

Nas demonstrações, dos teoremas ou proposições, os argumentos que darão embasamento, ou consistência, ao raciocínio lógico podem conter *axiomas,* também conhecidos como *postulados,* os quais são sentenças que assumimos ser verdade. Os axiomas podem ser descritos como sentenças que

não são demonstradas e consideradas como óbvias ou um consenso inicial necessário para a construção do argumento. Diferente da *definição,* que trabalha como um guia, e que precisa ser completa, devendo especificar todas as propriedades que identificam o conceito a ser tratado, de maneira clara. Por exemplo, “definição: um inteiro $n$ é par se ele é múltiplo de $2$”.

Podemos ainda nos deparar com teoremas com menor importância chamados *lemas*. Já um *corolário* é uma consequência dos teoremas, proposições e lemas, vistas anteriormente, mas que não deixa de ser um teorema. E, por fim, temos as *conjecturas,* que são sentenças inicialmente impostas como verdadeiras; é uma sentença sobre qual ainda não existe prova e quando demonstrada torna-se um teorema. O último teorema de Fermat é a conjectura mais conhecida da matemática “se $n > 2$, a equação $x^n + y^n = z^n$ não tem soluções inteiras positivas”, que ficou mais de $300$ anos sem demonstração. Alguns casos particulares foram desenvolvidos por matemáticos ao redor do mundo, mas foi somente em 1995 que o matemático inglês Andrew Wiles publicou a sua demonstração, com a colaboração do matemático Richard Taylor.

## 3.2 Prova de implicações

Em muitos casos encontramos sentenças do tipo $p \rightarrow q$, para demonstrar, em que se $p$ é verdade, então, $q$ também é. Vimos na aula de lógica, que $p$ é a nossa hipótese, premissa ou condição; e $q$ é a chamada *tese* ou *conclusão*.

A primeira técnica utilizada para esse tipo de caso, $p \rightarrow q$, é o **método direto** de demonstração. Da qual consiste em admitir $p$ é verdade, e utilizamos uma sequência lógica de argumentos até obter $q$.

Por exemplo: “a soma de dois números inteiros pares é um número par”.

Demonstração:

- Passo 1: suponha que vamos fazer a soma dos inteiros pares $m$ e $n$ (hipótese).
- Passo 2: sendo $m$ um número par, então, existe um inteiro $r$ tal que $m = 2r$ (definição de número par).
- Passo 3: sendo $n$ um número par, então existe um inteiro $s$ tal que $n = 2s$ (definição de número par).

- Passo 4: somando os números $m + n = 2r + 2s = 2(r + s)$ (decorre do passo 2 e 3, e propriedades algébricas).
- Passo 5: chamando $t = r + s$, segue $m + n = 2t$ (decorre do passo 4).
- Passo 6: portanto $m + n$ é par (conclusão do argumento do passo 5, chegando à tese). ■[1]

Geralmente, numa demonstração alguns passos são omitidos, de maneira que se pressupõe que o leitor saiba as definições básicas, por exemplo, se vamos reescrever a demonstração acima ela ficaria: "suponham $m$ e $n$ números pares. Então existem $r, s \in \mathbb{Z}$, tais que $m = 2r$ e $n = 2s$, assim $m + n = 2r + 2s = 2(r + s) = 2t$. Como $r + s = t$ é inteiro, então $m + n = 2t$ é par.■

A segunda técnica é o **método da contra positiva** para provar $p \to q$. Como o nome já sugere, trabalharemos com a negação das preposições, em que assumiremos que a negação da tese $\neg q$ seja verdadeira e concluiremos que a negação da hipótese $\neg p$, ou seja vamos provar $(\neg q) \to (\neg p)$.

Por exemplo: "se $n^2$ é par, então $n$ é par".

Utilizando a abordagem contra positiva, a sentença $p \to q$ tem como $p =$ "$n^2$ é par" e $q =$ "$n$ é par", então $\neg q =$ "$n$ não é par" e $\neg p =$ "$n^2$ não é par".

Prova: suponhamos que $n$ não seja par, ou seja, $n$ é ímpar. Então por definição de número ímpar, $\exists k \in \mathbb{Z}$ tal que $n = 2k + 1$. Portanto, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Como $2k^2 + 2k$ é um número inteiro, pela definição de número ímpar podemos escrever $n^2 = 2t + 1$.

E pelo método da contra positiva, isso prova que se $n^2$ é par, então $n$ é par.■

Terceira técnica é **método de redução ao absurdo**, também conhecida como **método da contradição**. Nesse método, para provar $p \to q$, suponhamos que tanto a hipótese quanto a negação da tese $\neg q$ são verdadeiras, e chegamos a uma contradição; ou seja, provamos que $p \to \neg q$ é *falso*, argumento visto na aula de lógica.

Por exemplo: utilizando o primeiro exemplo "a soma de dois números inteiros pares é par".

[1] Utilizaremos o símbolo "■" para indicar o fim da demonstração. Essa escolha é um tanto pessoal, existem autores que não utilizam nenhum símbolo, há outros que usam " ⊠ " ou " ⋈ " ou " ⋊ ".

Primeiro, vamos reescrever a sentença para então ver quem é $p$ e quem é $q$: “Se $m,n \in \mathbb{Z}$ são pares, então $m+n$ é par”, então a sentença $p \to q$ tem como $p =$ ”$m,n \in \mathbb{Z}$ são pares” e $q =$ “$m+n$ é par”, então $\neg q =$ “$m+n$ não é par”, e se $m+n$ não é par, ele é ímpar.

A prova: suponhamos $m$ e $n$ números pares. Então existem $r,s \in \mathbb{Z}$, tais que $m = 2r$ e $n = 2s$, já pela definição de número ímpar existe um inteiro $t$ tal que $m+n = 2t+1$. Sendo assim, $m+n = 2r+2s$, mas $m+n = 2t+1$, então $2r+2s = 2t+1 \Leftrightarrow 2r+2s-2t = 1 \Leftrightarrow 2(r+s-t) = 1 \Leftrightarrow r+s-t = 1/2$ e essa é uma afirmação falsa, pois a soma e subtração de números inteiros é um número inteiro, ou seja $r+s-t \in \mathbb{Z}$.

E essa contradição prova que se $m,n \in \mathbb{Z}$ são pares, então $m+n$ é par.■

A quarta técnica é o **método com tese conjuntiva**, o qual prova sentenças do tipo $p \to (q \wedge r)$, pelas propriedades lógicas, tal sentença é equivalente à $(p \to q) \wedge (p \to r)$. Para provar esse tipo de sentença $p \to (q \wedge r)$, basta provar, utilizando as técnicas anteriores, as sentenças separadamente $(p \to q)$ e em seguida $(p \to r)$.

Por exemplo: “se $10$ divide um número inteiro $n$, então $2$ divide $n$ e $5$ divide $n$”.

Aqui $p =$ ”$10$ divide um número inteiro $n$”, $q =$ “$2$ divide $n$” e $r =$ ”$5$ divide $n$”.

Prova: primeiro vamos provar $p \to q$, traduzindo-a, “Se $10$ divide um número inteiro $n$, então $2$ divide $n$”. De fato, se $10$ divide $n$, então podemos decompor $n$ como $n = 10k$, sendo $k$ um número inteiro, assim $n = 10k = (2 \cdot 5)k = 2(5k)$, ou seja, decompomos $n$ como um múltiplo de $2$, logo $2$ divide $n$.

Analogamente, o caso $p \to r$: “se $10$ divide um número inteiro $n$, então $5$ divide $n$”.

Se $10$ divide $n$, então podemos decompor $n$ como $n = 10k$, sendo $k$ um número inteiro, assim $n = 10k = (2 \cdot 5)k = 5(2k)$, ou seja, decompomos $n$ como um múltiplo de $5$, logo $5$ divide $n$.■

A quinta técnica é o **método com hipótese disjuntiva**, usada para provar sentenças do tipo $(p \vee q) \to r$, logicamente falando, vamos provar $(p \to q) \wedge (q \to r)$. Note que a houve a troca do operador $\vee$ por $\wedge$.

Por exemplo: “sejam $m,n \in \mathbb{Z}$, se $m$ é par ou $n$ é par, então $mn$ é par”.

Observe que $p =$ "$m$ é par", $q =$ "$n$ é par", $r =$ "$mn$ é par". Vamos realizar a prova de $(p \to q) \wedge (q \to r)$, analisando os casos separadamente. Prova:

Caso 1: "se $m$ é par, então $mn$ é par". De fato, sejam $m, n \in \mathbb{Z}$, e $m$ par, então existe $k \in \mathbb{Z}$, tal que $m = 2k$. Portanto, $mn = (2k)n = 2(kn)$ é um número par para qualquer $n$, pela definição de número par.

Caso 2: "se $n$ é par, então $mn$ é par". De fato, sejam $m, n \in \mathbb{Z}$, e $m$ par, então existe $t \in \mathbb{Z}$, tal que $n = 2t$. Portanto, $mn = m(2t) = 2(mt)$ é um número par para qualquer $m$, pela definição de número par.■

Outro caso comum em teoremas são as sentenças do tipo $p \leftrightarrow q$, **"p é verdade se, e somente se, q é verdade"**. Logicamente falando, $p \leftrightarrow q$ é equivalente à $(p \to q) \wedge (q \to p)$. Sendo assim, para provar esse tipo de sentença, basta utilizarmos as estratégias vistas anteriormente, e provarmos as sentenças, separadamente, $(p \to q)$ e em seguida $(q \to p)$.

Por exemplo: "se $n \in \mathbb{Z}$, então $n$ é ímpar $\leftrightarrow$ $n^2$ é ímpar".

Prova: primeiro vamos provar a "ida" ($\to$): "Se $n \in \mathbb{Z}$, então $n$ é ímpar $\to$ $n^2$ é ímpar".

De fato, se $n \in \mathbb{Z}$ é ímpar, então por definição de número ímpar, $\exists k \in \mathbb{Z}$ tal que $n = 2k + 1$. Logo, $n^2 = (2k+1)^2 = 4k^2 + 2k + 1 = 2(k^2 + k) + 1$, chamando o inteiro $k^2 + k = t$, segue $n^2 = 2t + 1$, ou seja, um número ímpar.

Agora vamos provar a "volta" ($\leftarrow$): "se $n^2$ é ímpar, então $n$ é ímpar".

Note que aqui utilizar a técnica direta não é vantajosa, pois se $n^2$ é ímpar, então $\exists k \in \mathbb{Z}$ tal que $n^2 = 2k + 1$. Logo, $n = \pm\sqrt{n^2} = \pm\sqrt{2k+1}$, e não é interessante trabalhar nessa abordagem. Então, vamos utilizar do método da contra positiva, $(\neg q) \to (\neg p)$. Suponhamos que $n$ não é ímpar, logo, ele seria um número par, e assim $\exists k \in \mathbb{Z}$ tal que $n = 2k$, sendo assim $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$, chamando $t = 2k^2$, segue $n^2 = 2t$ um número par. E, portanto, temos que se $n^2$ é ímpar, então $n$ é ímpar.■

## TEMA 4 – MÉTODOS DE PROVA 2

Nos teoremas, assim como encontramos operadores de implicação, encontramos quantificadores universal ($\forall$) e existencial ($\exists$). Sendo assim, esse tema será direcionado a métodos de prova que envolvem esses operadores.

## 4.1 Prova com o quantificador universal

A técnica popular utilizada – na verdade ela já foi indiretamente apresentada –, na maioria dos exemplos vistos, oquantificador universal $(\forall)$ estava presente, como no exemplo "se $n \in \mathbb{Z}$, então $n$ é ímpar $\leftrightarrow n^2$ é ímpar", na verdade deveríamos reescrever tal frase para "$(\forall n \in \mathbb{Z})(n$ é ímpar $\leftrightarrow n^2$é ímpar)". **Omitimos a existência do quantificador** e realizamos a prova, mas para usar esse tipo de tática devemos tomar cuidado para não particularizar a demonstração para apenas alguns casos, precisamos sempre deixar a premissa mais geral possível.

## 4.2 Prova com o quantificador existencial

Sabemos que o quantificador existencial $(\exists)$ é basicamente o oposto do quantificador universal $(\forall)$, enquanto um trabalha com a maior generalização possível o outro trabalha com casos particulares.

Por exemplo: "existem três números inteiros positivos tais que $x^2 + y^2 = z^2$".

Reescrevendo a sentença com quantificadores, temos "$(\exists x, y, z \in \mathbb{Z}^+)(x^2 + y^2 = z^2)$".

E de fato existem, esses são chamados de *triplas pitagóricas*, e um exemplo dessa existência é a tripla $3, 4$ e $5$; pois, $3^2 + 4^2 = 5^2 \Leftrightarrow 9 + 16 = 25$.■

Esse tipo de demonstração que acabamos de ver é chamada de **demonstração construtiva**, em que tomamos um elemento específico do domínio com que estamos trabalhando e mostramos que a sentença é verdadeira para esse elemento. Devemos salientar que essa tática é válida, pois toda vez que usamos o quantificador existencial, por exemplo, $(\exists a \in A)(P(a) \rightarrow V)$, devemos ter em mente que estamos falando que **existe pelo menos** um elemento do domínio para qual a sentença é verdadeira para esse elemento.

Vejamos outro exemplo: "para todo $n$ inteiro positivo, existe uma sequência de $n$ números inteiros consecutivos que não são primos".

Prova: sejam $n$ um inteiro positivo, tomamos um número $x = (n+1)! + 2$. Note que $x$ é par, então $2$ divide $x = (n+1)! + 2$. Tomando seu consecutivo, ou seja, $x + 1$, segue $x + 1 = (n+1)! + 2 + 1 = (n+1)! + 3$, e mais $3$ divide esse número. Agora se continuarmos esse processo, tomando $(n-1)$º consecutivo, $x + (n-1)$ temos $x + (n-1) = (n+1)! + 2 + (n-1) = (n+1)! + n + 1$, e

assim segue $n+1$ divide esse número. Portanto, todos os inteiros consecutivos $x+k$ com $0 \leq k \leq n$ são não primos, e mais, eles foram uma sequência de $n$ inteiros consecutivos. ■

Outra técnica que temos é a **demonstração não construtivas**, também conhecida como **demonstração desconstrutiva**. Da qual é possível demonstrar a existência de um elemento que satisfaz a sentença sem precisar exibi-lo explicitamente.

Por exemplo: “existem dois números reais irracionais $x$ e $y$ tais que $x^y$ é racional”.

Prova: sabemos que $\sqrt{2}$ é irracional, então podemos tomar $x = y = \sqrt{2}$, então $x^y = \left(\sqrt{2}\right)^{\sqrt{2}}$. Se esse número é racional, então temos dois números irracionais $x$ e $y$, onde $x^y$ é racional, tomando $x = y = \sqrt{2}$. Por sua vez, se $\left(\sqrt{2}\right)^{\sqrt{2}}$ é irracional, podemos tomar $x = \left(\sqrt{2}\right)^{\sqrt{2}}$ e $y = \sqrt{2}$, logo $x^y = \left(\left(\sqrt{2}\right)^{\sqrt{2}}\right)^{\sqrt{2}}$ utilizando as propriedades de potência, $x^y = \left(\left(\sqrt{2}\right)^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^{\sqrt{2}\cdot\sqrt{2}} = \left(\sqrt{2}\right)^2 = 2$, que é um número racional. Logo, tomamos dois números irracionais que resultaram em um número racional. ■

## 4.3 Prova com existência e unicidade

Esse tipo de prova tem duas etapas:

- Prova da existência: na qual provamos a existência de que pelo menos um elemento do domínio satisfaz a sentença.
- Prova da unicidade: em que provamos que se existe esse elemento, ele é único.

Lembramos que um teorema que contém esse tipo de quantificado é escrito como $(\exists! a \in A)P(a)$ e é logicamente equivalente $\big((\exists a \in A)P(a)\big) \wedge ((\forall b \in A)(\big(P(a) \wedge P(b)\big) \rightarrow a = b)$.

E para provar esse tipo de sentença na primeira etapa podemos utilizar as técnicas **construtiva** e **não construtiva**. Já para demonstrar a unicidade, supõe-se que $b$ também é um elemento do domínio $A$ que satisfaz a sentença $P(b)$, e assim utilizando argumentos lógicos e técnicas vistas anteriormente,

concluímos que isso só será possível se esse elemento $b$ é igual ao elemento $a$, da primeira etapa.

Por exemplo: “se $a, b \in \mathbb{R}$ e $a \neq 0$, então, existe um único $x \in \mathbb{R}$, tal que $ax + b = 0$”.

Prova: primeiro vamos mostrar a existência, utilizando o método construtivo, basta tomarmos um elemento do domínio que satisfaça a sentença, então se tomarmos $x = -b/a$ (que também é real) e substituirmos na premissa segue $a \cdot \left(-\frac{b}{a}\right) + b = -b + b = 0$. Portanto, a existência está provada.

Agora vamos a parte da unicidade: suponha que exista $y \in \mathbb{R}$, de maneira $ay + b = 0$. Como sabemos $ax + b = 0$, então $ax + b = ay + b$, subtraindo $b$ em ambos os lados, temos $ax = ay$; agora dividindo ambos os lados por $a \neq 0$ (por hipótese) chegamos $x = y$. Tínhamos dois números reais, $x$ e $y$, e chegamos à conclusão que eles são iguais $(x = y)$, caso eles não sejam iguais $(x \neq y)$, então $ay + b \neq 0$.■

## 4.4 Prova por contraexemplo

Demonstrações desse tipo são usadas em casos que queremos negar a sentença $(\forall a \in A)P(a)$. Assim, se tomarmos a sua negação, temos $(\exists a \in A)\neg P(a)$, ou seja, encontraríamos um elemento que contrariasse a sentença. Resumindo, apresentamos um exemplo que não satisfaz uma certa sentença, e esse tipo de técnica é chamado de **contraexemplo**.

Por exemplo: “para todo primo $n$, o inteiro $2^n - 1$ é primo”.

Prova: utilizando a técnica de contraexemplo, então, basta tomar $n = 11$, que temos $2^{11} - 1 = 2047 = 23 \times 89$ que não é primo. Logo, essa sentença não é válida.■

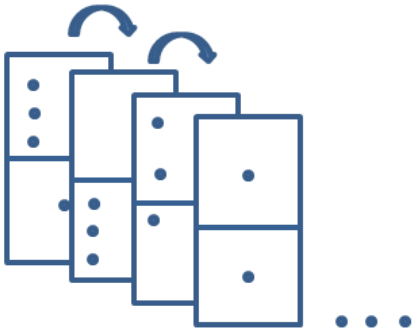
# TEMA 5 – PRINCÍPIO DA INDUÇÃO MATEMÁTICA

Essa é uma das técnicas de demonstração que consideramos a mais simples. Esse tipo de demonstração tem uma relação de boa ordem, em que todo conjunto não vazio de elementos tem um elemento mínimo segundo essa relação de ordem, e um exemplo mais utilizado é o conjunto dos naturais. Utilizamos o princípio da boa ordem para provar propriedade que valem para todo elemento.

A melhor analogia para tentarmos entender como funciona o princípio da indução é o efeito dominó!

Colocando as peças em pé, uma ao lado da outra, quando derrubamos a primeira todas as demais serão derrubadas.

Figura 1 – Efeito dominó



Para que o processo ocorra de maneira correta, a primeira peça é derrubada em direção às demais. Se qualquer outra peça está suficientemente próxima da próxima, então, ao ser derrubada, derrubará a próxima, que derrubará a próxima, e assim sucessivamente, até que todas as peças sejam derrubadas (Menezes, [S.d.]).

Assim, a demonstração por indução é dividida em basicamente duas partes (Rosen, 2010):

- Primeira parte ou *ponto base*: ela mostra que a proposição é verdadeira para o número inteiro positivo 1.
- Segunda parte ou *passo de indução*: ela mostra que se a proposição for verdadeira para um número positivo, então deve ser mantida para o número inteiro seguinte.

  Em termos lógicos, escrevemos:

$$P(1) \wedge [\forall k(P(k) \rightarrow P(k+1)] \rightarrow \forall n\, P(n)$$

ou seja, se a proposição é válida para o primeiro termo e os $k$ –demais, então, ela é verdadeira para o domínio dos números inteiros positivos.

Fazer a demonstração, seguimos sempre uma “receita”:

1. Verificamos a base da indução, $k = 0$ (às vezes para $k = 0$ não faz sentido, então começamos por $k = 1$).
2. Fixado um $k$, suponhamos que $P(k)$ é verdadeira.

3. Demonstrar o passo de indução $P(k) \rightarrow P(k+1)$.

Por exemplo: “para qualquer $n \in \mathbb{N}$, tem-se que $n < 2^n$.”

Seguindo o passo a passo, primeiro devemos mostrar a base de indução:

*Base de indução*: $k = 0$

$$0 < 2^0 = 1$$

Ela é verdadeira!

Para nos convencermos melhor que a sentença é verdadeira para outros valores, tomemos $k = 1$

$$1 < 2^1 = 2$$

Ela é verdadeira!

Agora para $k = 2$

$$2 < 2^2 = 4$$

Ela é verdadeira!

E para $k = 3$

$$3 < 2^3 = 8$$

Ela é verdadeira! Verificados que a sentença é válida para os primeiros valores de $k$, vamos ao próximo passo.

Hipótese de indução: suponha que, para $k \in \mathbb{N}$ $p(k)$ é verdadeira

$$p(k): k < 2^k$$

Passo de indução: vamos provar que seja válida para $k + 1 \in \mathbb{N}$. Sabendo que:

$$k < 2^k$$

Então, se somarmos $1$ em ambos os lados da desigualdade:

$$k + 1 < 2^k + 1$$

Por outro lado:

$$2^k + 1 = 2^k + 2^0 \leq 2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$$

Logo:

$$k + 1 < 2^{k+1}$$

Portanto, para qualquer $n \in \mathbb{N}$, tem-se que $n < 2^n$. ■

Exemplo: mostre que se $n$ for um inteiro positivo, então:

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Demonstração: *passo base:* $P(0)$ é verdadeira, pois

$$0 = \frac{0(0+0)}{2}$$

Não está convencido? Vejamos para alguns outros valores, primeiro note que $P(1)$ também é verdadeira, pois:

$$0 + 1 = \frac{1(1+1)}{2}$$

E para $P(2)$ também é verdadeira, pois:

$$0 + 1 + 2 = 3 = \frac{2(2+1)}{2} = \frac{2(3)}{2}$$

E $P(3)$ também é:

$$0 + 1 + 2 + 3 = 6 = \frac{3(3+1)}{2} = \frac{3(4)}{2}$$

Visto que a sentença é válida para outros valores, vamos ao próximo passo.

Hipótese de indução: suponha que $P(k)$ é verdadeira, logo:

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}$$

Passo de indução: vamos provar que $P(k+1) = \frac{(k+1)(k+2)}{2}$. Somando os $(k+1)$ temos:

$$1 + 2 + 3 + \cdots + k + (k+1)$$

Sabemos que sabendo que $1 + 2 + 3 + \cdots + k \overset{\star}{=} \frac{k(k+1)}{2}$, logo:

$$\underbrace{1 + 2 + 3 + \cdots + k}_{\star} + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1)}{2} + \frac{2(k+1)}{2}$$

$$= \frac{(k+1)(k+2)}{2} = \frac{(k+1)((k+1)+1)}{2} = P(k+1)$$

Logo, $P(k+1)$ é válida. Portando, segue que $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$.

■

Exemplo: use a indução para mostrar que se $n$ for um inteiro positivo, então:

$$1 + 2^1 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 1$$

Demonstração: passo base: $P(0)$ é verdadeira pois

$$1 = 2^{0+1} - 1 = 2^1 - 1 = 2 - 1 = 1$$

Hipótese de indução: suponha que $P(k)$ é verdadeira, logo

$$1 + 2^1 + 2^2 + 2^3 + \cdots + 2^k = 2^{k+1} - 1$$

Passo de indução: vamos provar que $P(k+1) = 2^{(k+1)+1} - 1$. Somando os $(k+1)$ termos

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^k + 2^{k+1}$$

Sabemos que sabendo que $1 + 2^1 + 2^2 + 2^3 + \cdots + 2^k \overset{\star}{=} 2^{k+1} - 1$, logo

$$\underbrace{1 + 2 + 2^2 + 2^3 + \cdots + 2^k}_{\star} + 2^{k+1} = 2^{k+1} - 1 + 2^{k+1}$$

$$= 2 * 2^{k+1} - 1 = 2^{(k+1)+1} - 1 = 2^{k+2} - 1 = P(k+1)$$

Logo, $P(k+1)$ é válida. Portanto, segue que $1 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$. ■

## 4.4 Generalização do Princípio da Indução Matemática

Sabemos que o mesmo assunto pode ser tratado de maneiras diferentes, e isso depende de como o autor do livro está tratando esse assunto. Sendo assim, podemos encontrar variações da abordagem do princípio da indução, que no fundo são equivalentes, mas podem facilitar algumas provas.

É possível *generalizar o passo base*, já que muitas vezes precisamos provar uma sentença aberta $P(n)$ que vale para todos os naturais que são maiores ou iguais a um certo $n_0$. O teorema a seguir formaliza essa generalização, em que, ao invés de começarmos uma demonstração pelo número 0 (zero), a iniciamos por $n_0$.

"Seja $P(n)$ uma sentença aberta sobre $\mathbb{N}$. Se $P(n_0)$ é verdadeira e $\forall k \geq n_0,\ (P(k) \rightarrow P(k+1))$; então $P(n)$ é verdadeira para todo $n \in \mathbb{N}$ com $n \geq n_0$."

Exemplo: $n^2 > 3n$ para todo $n \in \mathbb{N}$ com $n \geq 4$.

Demonstração: note que aqui a sentença começa a partir $n_0 = 4$.

*Passo base:* para $n = 4$, temos $4^2 = 16 > 12 = 3(4)$. Logo, é válida a sentença.

Verificando para $n = 5$, temos $5^2 = 25 > 15 = 3(5)$. Válida também.

Hipótese de indução: suponhamos que para $n = k$, a sentença também seja válida, logo $k^2 > 3k$.

Passo de indução: tomando $(k+1)^2 = k^2 + 2k + 1$ assim partindo do fato que sabemos $k^2 > 3k$ segue que ao somarmos $2k + 1$ em ambos os lados da desigualdade (para não alterá-la) segue

$$(k+1)^2 = k^2 + 2k + 1 > 3k + 2k + 1 \ (\star)$$

Observe que ainda não chegamos na conclusão que gostaríamos, pois $3(k+1) = 3k + 3 \neq 3k + 2k + 1$, ou seja, o $2k$ está "atrapalhando" nossa demonstração, então devemos lidar com ele. Para isso, devemos utilizar outras hipóteses do nosso enunciado, que ainda não foram utilizadas. Lembrando da hipótese inicial de que essa sentença só é válida para valores $k \geq 4$, então ao multiplicarmos por 2 (dois) a nossa desigualdade, temos $2k \geq 8$. Sendo assim:

$$3k + 2k + 1 \geq 3k + 8 + 1 = 3k + 9 = 3(k+1) + 6 > 3(k+1) \quad (\star\star)$$

Partindo de $(\star)$ e utilizando $(\star\star)$:

$$(k+1)^2 = k^2 + 2k + 1 > 3k + 2k + 1 > 3(k+1)$$

E então segue $(k+1)^2 > 3(k+1)$. ■

Ainda podemos encontrar uma versão do princípio de indução que dada uma sentença $P(n)$, que parte de um número arbitrário $n_0$, é possível usar um incremento de passo maior que 1 (um). O teorema a seguir garante exatamente isso:

"Seja $P(n)$ uma sentença aberta sobre $\mathbb{N}$, $n_0$ um número natural qualquer, e $p \in \mathbb{N}^*$. Se $P(n_0), P(n_0+1), \ldots P(n_0+p-1)$ são verdadeiras, e $\forall k \geq n_0$ $(P(k) \rightarrow P(k+p)$ é verdadeira, então $P(n)$ é verdadeira seja qual for $n \geq n_0$."

Exemplo: "para qualquer valor inteiro $n \geq 8$, pode ser obtido como decomposição de soma múltiplos de 3 e/ou 5".

Demonstração: *passo base* – para $n = 8$, temos $8 = 3 + 5$. Logo, é válida a sentença.

Verificando para $n = 9$, temos $9 = 3 + 3 + 3 = 3 \cdot 3$. Válida também.

Note que para $n = 10$, temos $10 = 5 + 5 = 2 \cdot 5$. Válida também.

Já para $n = 11$, segue $11 = 3 + 3 + 5$. Válida também.

Hipótese de indução: suponhamos que para $n = k$, a sentença também seja válida, desde $k \geq 8$.

Passo de indução: vamos utilizar o passo $p = 3$, para concluir a demonstração. Sabendo que a sentença é válida para $n = k$, se somarmos $3$, então a sentença para $k + 3$ continuará válida. Portanto, a $P(k + 3)$ é verdadeira. Argumento análogo utilizando o passo $p = 5$.

■

## FINALIZANDO

Esta foi uma aula bastante teórica, abstrata e com muitos conceitos novos. Aprendemos a utilizar a lógica a nosso favor, e estudamos técnicas de demonstração.

Nas próximas aulas, trabalharemos com um conceito bastante familiar: funções. Vamos rever seus principais conceitos e introduziremos os conceitos de estruturas algébricas.

## REFERÊNCIAS

MENEZES, P. B. **Notas da disciplina Matemática Discreta para Computação e Informática.** Departamento de Informática Teórica. Porto Alegre: Instituto de Informática – UFRGS, [S.d]. Disponível em: <ftp://ftp.inf.ufrgs.br/pub/blauth/Discretas/Mat_Discreta8.pdf>. Acesso em: 17 abr. 2020.

ROSEN, K. H. **Matemática discreta e suas aplicações**. 6. ed. São Paulo: Editora AMGH, 2010.

SCHEINERMAN, E. R. **Matemática discreta**: uma introdução. 3. ed. São Paulo: Cengage Learning, 2016.