Técnicas de demonstração

Prof. Willian Tokura

Faculdade de Ciências Exatas e Tecnologia - FACET

Métodos de demonstração: Introdução

- Uma **demonstração** é uma argumentação matemática da certeza a respeito de uma afirmação.
- O nível de detalhamento de uma demonstração pode depender do tipo de leitor ao qual ela se destina, levando em conta fatores como:
  - o conhecimento do leitor sobre o assunto;
  - a maturidade do leitor;
  - o nível de rigor almejado.
- Nesta seção vamos nos focar em demonstrações utilizando o rigor matemático esperado de um profissional em nível de graduação na área de ciências exatas.

Terminologia

- Um **axioma (ou postulado)** é uma afirmação assumida como verdadeira sem a necessidade de uma demonstração, ou seja, uma "verdade a princípio".

- Um **resultado** é uma afirmação que se pode demonstrar ser verdadeira.

  Resultados recebem diferentes nomes, de maneira mais ou menos subjetiva:

  - Um **teorema** é um resultado considerado interessante em si mesmo.
  - Uma **proposição** é um resultado considerado "de menor interesse".
  - Um **lema** é um resultado auxiliar, geralmente usado para quebrar a demonstração de um resultado mais complexo em partes menores.
  - Um **corolário** é um resultado derivável facilmente a partir de outro resultado já demonstrado, consistindo em uma consequência mais ou menos imediata.

- Uma **demonstração (ou prova)** é um argumento que mostra que uma afirmação (teorema, proposição ou lema) segue de um conjunto de premissas.

- Uma **conjectura** é suposição bem fundada, porém (ainda) sem demonstração. Uma vez demonstrada, uma conjectura se torna um resultado.

Evidência versus demonstração

- $\boxed{\text{Exemplo 1}}$ Seja a fórmula $p(n) = n^2 + n + 41$.

  Conjectura: $\forall n \in \mathbb{N} : p(n)$ é primo.

  Temos evidências de que a conjectura poderia ser verdadeira?

  Testando valores de $n = 0, 1, \ldots, 39$ a proposição é sempre verdadeira, ou seja, $p(n)$ é primo para $0 \leq n \leq 39$:

n	0	1	2	3	...	20	...	39
$p(n)$	41	43	47	53	...	461	...	1601

  Daí, podemos ficar tentados a concluir:

  Isto não pode ser uma coincidência! A hipótese deve ser verdadeira!

  Mas não é: $p(40) = 1681 = 41 \cdot 41$, que não é primo!

  Logo, a conjectura é falsa. $\triangleleft$

- Moral da história: evidência não é o mesmo que demonstração!

Evidência versus demonstração

- $\boxed{\text{Exemplo 2}}$ Em 1 769, Euler (1 707–1 783) conjecturou que

$$a^4 + b^4 + c^4 = d^4$$

não tem solução no conjunto dos números inteiros positivos.

Durante mais de dois séculos, ninguém conseguiu encontrar valores de a, b, c e d que satisfizessem a equação.

O insucesso de todos os matemáticos envolvidos era evidência de que a conjectura poderia ser verdadeira.

218 anos depois, em 1 987, Noam Elkies proveu um contra-exemplo:

$$95\,800^4 + 217\,519^4 + 414\,560^4 = 422\,481^4.$$

Logo, esta conjectura também é <u>falsa</u>. $\triangleleft$

- <u>Ausência de demonstração não o mesmo que demonstração de ausência!</u>

Métodos de demonstração

- Construir uma demonstração é uma arte.

  Cada caso é um caso: não existe uma "receita fechada" para construir demonstrações para todas as afirmações.

- Existem, entretanto, técnicas que são úteis para demonstrar uma grande quantidade de afirmações.

  Aqui vamos cobrir vários métodos de demonstração, incluindo:

  1. demonstração direta;
  2. demonstração por contraposição;
  3. demonstração por contradição (ou demonstração por redução ao absurdo).
  4. demonstração por contra-exemplo; e
  5. demonstração por exaustão e divisão em casos.

- Outros métodos de demonstração (e.g., demonstração por indução matemática) serão cobertos mais adiante neste curso.

Como escrever uma demonstração

- Escreva claramente qual a afirmação que se deseja demonstrar.

  (É comum preceder a afirmação com uma qualificação como **"Teorema"**, **"Lema"**, ou **"Proposição"**.)

- Delimite claramente o escopo da demonstração.

  Indique o início da demonstração com **"Demonstração."** ou **"Prova."**

  Indique o fim da demonstração com um marcador. Podem-se usar:

  - um quadradinho $\square$, ou
  - a abreviação **Q.E.D.** (do latim *"quod erat demonstrandum"*), ou
  - sua tradução em português, **C.Q.D.** (*"conforme queríamos demonstrar"*).

- Escreva a demonstração de tal forma que ela seja autocontida.

  - Use linguagem natural (português) de forma clara, empregando sentenças completas e bem estruturadas.
  - Podem-se utilizar fórmulas matemáticas, equações, etc., quando necessário.

Demonstração direta

- Forma geral:

  1. Expresse a afirmação a ser demonstrada na forma:

  $$\forall x \in D : (\, P(x) \;\rightarrow\; Q(x)\,)$$

     Esta etapa às vezes é feita mentalmente.

  2. Comece a demonstração supondo que x é um elemento específico do domínio D, mas escolhido arbitrariamente, para o qual a hipótese $P(x)$ é verdadeira.

     Normalmente abreviamos esta etapa dizendo *"Assuma que $x \in D$ e $P(x)$ é verdadeiro"* ou *"Seja $x \in D$ tal que $P(x)$"*.

  3. Mostre que a conclusão $Q(x)$ é verdadeira utilizando definições, resultados anteriores e as regras de inferência lógica.

- Importante: Como $x \in D$ é escolhido arbitrariamente,
  - ele não depende de nenhuma suposição especial sobre x, e,
  - portanto, ele ser generalizado para todos os elementos de D.

- **Definição:**

  (i) Um inteiro n é **par** se existe um inteiro k tal que $n = 2k$.

  (ii) Um inteiro n é **ímpar** se existe um inteiro k tal que $n = 2k + 1$.

- Exemplo 3 Mostre que se n é um inteiro ímpar, então n^2 é ímpar.

Demonstração. Queremos mostrar que

$$\forall n \in \mathbb{Z} : (\, P(n) \; \rightarrow \; Q(n) \,),$$

onde

- $P(n)$ é o predicado *"n é um inteiro ímpar"*, e
- $Q(n)$ é o predicado *"n^2 é ímpar"*.

Para produzir uma demonstração direta, assumimos que para um inteiro n a hipótese da implicação, $P(n)$, seja verdadeira, ou seja, que n é ímpar.

Então, pela definição de número ímpar, existe um inteiro k tal que $n = 2k + 1$.

Demonstração direta

- $\boxed{\text{Exemplo 3}}$ (Continuação)

Queremos mostrar que a conclusão da implicação, $Q(n)$, é verdadeira, ou seja, que n^2 também é ímpar.

Para isto podemos calcular

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

Mas note que isso significa que

$$n^2 = 2k' + 1,$$

onde $k' = 2k^2 + 2k$ é um inteiro.

Logo, pela definição de número ímpar, n^2 também é ímpar e está concluída nossa demonstração. $\square$

- **Definição:** Um inteiro a é um **quadrado perfeito** se existe um inteiro b tal que $a = b^2$.

- Exemplo 4 Mostre que se m e n são quadrados perfeitos, então mn é um quadrado perfeito.

  Demonstração. Para demonstrar esta proposição, vamos assumir que m e n sejam quadrados perfeitos. Pela definição de quadrado perfeito, devem existir inteiros s e t tais que $m = s^2$ e $n = t^2$.

  O objetivo da demonstração é mostrar que mn será um quadrado perfeito quando m e n o forem. Para ver isto, podemos calcular

$$mn = s^2t^2 = (st)^2.$$

  Mas é claro que st também é um inteiro, logo mn satisfaz a definição de quadrado perfeito (já que $mn = (st)^2$), e a conclusão da implicação também é verdadeira.

  Logo concluímos a demonstração de que a afirmação é verdadeira. $\square$

- **Definição:**
  - (i) Um número real n é **racional** quando existem inteiros p e q, com $q \neq 0$, tais que $n = p/q$.
  - (ii) Um número real n é **irracional** quando ele não é racional.

- $\boxed{\text{Exemplo 5}}$ Mostre que a soma de dois números racionais é um número racional.

Demonstração. Formalmente, queremos mostrar que para todo número real r e todo número real s, se r e s são racionais, então $r + s$ também é racional.

Para dar uma demonstração direta desta afirmação, vamos assumir que r e s sejam racionais. Pela definição de número racional, devem existir então inteiros p e q, com $q \neq 0$, tais que $r = p/q$, e devem existir também inteiros t e u, com $u \neq 0$, tais que $s = t/u$.

- $\boxed{\text{Exemplo 5}}$ (Continuação)

Para mostrar que $r + s$ também será racional quando r e s o forem, podemos calcular

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu + qt}{qu}.$$

Note que, por hipótese, q e u são diferentes de zero e, portanto, $qu \neq 0$.

Consequentemente $r + s$ pode ser expresso como a razão de dois inteiros ($pu + qt$ e qu, com $qu \neq 0$) e, portanto, $r + s$ satisfaz a definição de número racional.

Logo a afirmação é verdadeira. $\square$

Demonstração por contraposição

- Forma geral:

  1. Expresse a afirmação a ser demonstrada na forma:

  $$\forall x \in D : (\, P(x) \;\rightarrow\; Q(x)\,)$$

     Esta etapa às vezes é feita mentalmente.

  2. Encontre a afirmação contrapositiva da afirmação a ser demonstrada:

  $$\forall x \in D : (\, \neg Q(x) \;\rightarrow\; \neg P(x)\,)$$

  3. Comece a demonstração supondo que x é um elemento específico do domínio D, mas escolhido arbitrariamente, para o qual a conclusão $Q(x)$ é falsa.
  4. Mostre que a hipótese $P(x)$ é falsa utilizando definições, resultados anteriores e as regras de inferência lógica.

- Importante: Como $x \in D$ é escolhido arbitrariamente,
  - ele não depende de nenhuma suposição especial sobre x, e,
  - portanto, ele ser generalizado para todos os elementos de D.

- **Exemplo 6** Mostre que se n é um inteiro e $3n + 2$ é ímpar, então n é ímpar.

Demonstração. Queremos mostrar que $\forall n \in \mathbb{Z} : (P(n) \rightarrow Q(n))$, onde $P(n)$ é *"$3n + 2$ é ímpar"*, e $Q(x)$ é *"n é ímpar"*.

Para produzir uma demonstração por contraposição, vamos demonstrar que $\forall n \in \mathbb{Z} : (\neg Q(n) \rightarrow \neg P(n))$. Ou seja, vamos mostrar que se um número inteiro n não é ímpar, então $3n + 2$ também não é ímpar.

Se n não é ímpar, é porque n é par e, pela definição de número par, $n = 2k$ para algum $k \in \mathbb{Z}$. Portanto podemos derivar

$$\begin{aligned} 3n + 2 &= 3(2k) + 2 \\ &= 6k + 2 \\ &= 2(3k + 1), \end{aligned}$$

de onde concluímos que $3n + 2$ satisfaz a definição de número par.

Como mostramos que sempre que a conclusão da implicação é falsa, a hipótese também é falsa, concluímos com sucesso a demonstração por contraposição . $\square$

- $\boxed{\text{Exemplo 7}}$ Mostre que se $n = ab$ onde a e b são inteiros positivos, então $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$.

Demonstração. Em primeiro lugar, note que o resultado que queremos demonstrar pode ser formalizado como

$$\forall n, a, b \in \mathbb{Z}^+ : \left(n = ab \ \to \ a \leq \sqrt{n} \vee b \leq \sqrt{n}\right) \ .$$

Para produzir uma demonstração por contraposição, vamos demonstrar que sempre que a conclusão da implicação é falsa, sua hipótese também é falsa.

A conclusão da implicação é $(a \leq \sqrt{n}) \vee (b \leq \sqrt{n})$, logo por De Morgan, sua negação é

$$\begin{aligned} \neg((a \leq \sqrt{n}) \vee (a \leq \sqrt{n})) &\equiv \neg(a \leq \sqrt{n}) \wedge \neg(b \leq \sqrt{n}) \\ &\equiv (a > \sqrt{n}) \wedge (b > \sqrt{n}). \end{aligned}$$

Já a hipótese da implicação é $n = ab$, e sua negação é $n \neq ab$.

- $\boxed{\text{Exemplo 7}}$ (Continuação)

  Queremos mostrar a contrapositiva da proposição original, ou seja, que para todos inteiros positivos a, b, n se $(a > \sqrt{n}) \wedge (b > \sqrt{n})$ então $n \neq ab$.

  Para isto, note que se $(a > \sqrt{n}) \wedge (b > \sqrt{n})$ podemos derivar o seguinte

$$
\begin{aligned}
ab &> \sqrt{n} \cdot b && (\text{pois } a > \sqrt{n}) \\
&> \sqrt{n} \cdot \sqrt{n} && (\text{pois } b > \sqrt{n}) \\
&= n \, ,
\end{aligned}
$$

  de onde se conclui que $ab > n$ e, portanto, $ab \neq n$.

  Como mostramos que sempre que a conclusão da implicação é falsa, a hipótese também é falsa, a demonstração por contraposição é concluída com sucesso. $\square$

Demonstração por contradição

- Para demonstrar p, assumimos $\neg p$ e mostramos que isso leva a uma contradição. Como $\neg p \to \mathbf{F}$ é verdadeira, concluimos que $\neg p$ é falsa e portanto que p é verdadeira.
- De outra forma, para provar $p \to q$, basta mostrar $p \land \neg q \to \mathbf{F}$, pois $(p \land \neg q \to \mathbf{F}) \to (p \to q)$ é uma tautologia (verifique isso).

- $\boxed{\text{Exemplo 11}}$ Mostre que se $3n+2$ é ímpar, então n é ímpar.

Demonstração. Queremos mostrar a proposição *"se $3n+2$ é ímpar, então n é ímpar"*. Podemos escrever esta proposição como $p \rightarrow q$.

Para demonstrar por contradição, vamos assumir que $p \rightarrow q$ seja falso. Isso quer dizer que estamos assumindo $p \wedge \neg q$, ou seja, que *"$3n+2$ é ímpar e n não é ímpar"*.

Mas se n não é ímpar, é porque n é par e existe um inteiro k tal que $n = 2k$. Podemos, então, derivar

$$3n+2 \quad = \quad 3(2k)+2 \quad = \quad 6k+2 \quad = \quad 2(3k+1),$$

o que implica que $3n+2$ é par. Mas isto significa que concluímos exatamente que p é falso, o que contradiz a hipótese de que p é verdadeiro.

Logo, não é possível ter $p \wedge \neg q$ sem cair em contradição, e, portanto, se $3n+2$ é ímpar então n é ímpar. □

- $\boxed{\text{Exemplo 12}}$ Vamos revisitar o exemplo da primeira aula deste curso (recordar é viver!) e mostrar que $\sqrt{2}$ é irracional.

Demonstração. Para atingir uma contradição, suponha o contrário do que queremos demonstrar, ou seja, que $\sqrt{2}$ seja racional.

Neste caso, existem $p, q \in \mathbb{Z}$, com $mdc(p, q) = 1$, tais que $\sqrt{2} = p/q$. Elevando os dois lados ao quadrado, obtemos $2 = p^2/q^2$, ou seja, $p^2 = 2q^2$. Note que $2q^2$ é par, portanto pela igualdade acima p^2 também tem que ser par. Isto implica que p deve ser par.

Agora, já que p é par, existe algum $s \in \mathbb{Z}$ tal que $p = 2s$. Isso implica que $2q^2 = p^2 = (2s)^2 = 4s^2$, o que resulta em $q^2 = 2s^2$. Note que então q^2 é par, portanto q deve ser par.

Mas se ambos p e q são pares, isto contradiz a suposição de que o $mdc(p, q) = 1$: encontramos uma contradição.

Logo podemos concluir que não existem $p, q \in \mathbb{Z}$, com $q \neq 0$ e $mdc(p, q) = 1$, tais que $\sqrt{2} = p/q$. Portanto $\sqrt{2}$ é irracional. □

Demonstração por divisão de casos

- Utilizada geralmente para demonstrar que $p \to q$.
- A demonstração divide p em casos exaustivos, e mostra que q segue de qualquer caso possível.
- Forma geral:
  1. Primeiro mostre que
  $$p \equiv p_1 \vee p_2 \vee \ldots \vee p_n$$
  2. Mostre, separadamente, cada uma das implicações
  $$\begin{aligned} p_1 &\to q \\ p_2 &\to q \\ \ldots &\to \ldots \\ p_n &\to q \end{aligned}$$
  3. Conclua que $p \to q$.

- **Definição:** Dado dois números reais x e y, definimos as funções máximo e mínimo, respectivamente, como a seguir

$$\max(x,y) = \begin{cases} x, & \text{se } x \geq y, \\ y, & \text{se } x < y. \end{cases} \qquad \min(x,y) = \begin{cases} x, & \text{se } x \leq y, \\ y, & \text{se } x > y. \end{cases}$$

- $\boxed{\text{Exemplo 16}}$ Mostre que, dados $x, y \in \mathbb{R}$, $\min(x,y) + \max(x,y) = x + y$.

Demonstração. Há somente três possibilidades para x e y:

$$x < y \quad \text{ou} \quad x = y \quad \text{ou} \quad x > y.$$

Vamos analisar cada caso separadamente:

- Se $x < y$, então $\min(x,y) + \max(x,y) = x + y$.
- Se $x = y$, então $\min(x,y) + \max(x,y) = x + y$.
- Se $x > y$, então $\min(x,y) + \max(x,y) = y + x = x + y$.

Logo, sempre teremos $\min(x,y) + \max(x,y) = x + y$. □

Demonstração por divisão de casos

- **Definição:** Dado um número real a, seu **módulo** $|a|$ é definido como

$$|a| = \begin{cases} a, & \text{se } a \geq 0, \\ -a, & \text{se } a < 0. \end{cases}$$

- Exemplo 17 Mostre que $|xy| = |x||y|$, onde x e y são números reais.

Demonstração. Note que podemos identificar cinco casos exaustivos para a combinação de x e y:

1. pelo menos um entre x e y é zero,
2. x e y são ambos positivos,
3. x é positivo e y é negativo,
4. x é negativo e y é positivo, ou
5. x e y são ambos negativos.

- Exemplo 17 (Continuação)

Vamos analisar cada caso separadamente:

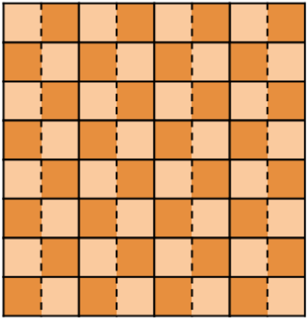
1. Se pelo menos um entre x e y é zero, então $xy = 0$ e pelo menos um entre $|x|$ e $|y|$ é zero e, portanto, temos
$$|xy| = 0 = |x||y|.$$
2. Se x e y são ambos positivos, então $xy > 0$ e temos
$$|xy| = xy = |x||y|.$$
3. Se x é positivo e y é negativo, então $xy < 0$ e temos
$$|xy| = -xy = x(-y) = |x||y|.$$
4. Se x é negativo e y é positivo, então $xy < 0$ e temos
$$|xy| = -xy = (-x)y = |x||y|.$$
5. Se x e y são ambos negativos, então $xy > 0$ e temos
$$|xy| = xy = (-x)(-y) = |x||y|.$$

Logo, podemos concluir que a afirmação é sempre verdadeira. $\square$

- Exemplo 21 É possível cobrir todo o tabuleiro usando peças de dominós?

Solução.

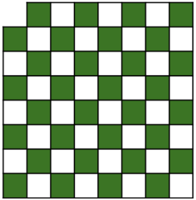
Sim, podemos usar 32 dominós, todos de forma horizontal, como mostra a figura ao lado.



◁

- $\boxed{\text{Exemplo 22}}$ Suponha que um novo tabuleiro seja obtido a partir de um tabuleiro padrão removendo uma de suas quinas.

  É possível cobrir todo este novo tabuleiro usando peças de dominós?



Solução.

Note que ao remover uma quina, novo tabuleiro tem exatamente 63 casas.

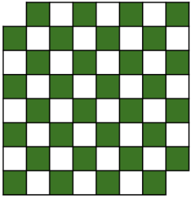
Como cada dominó cobre um número par de casas (2), é impossível cobrir todas as casas do tabuleiro com dominós.

$\triangleleft$

Estratégias de demonstração: tabuleiro de xadrez e dominós

- $\boxed{\text{Exemplo 23}}$ Suponha que um novo tabuleiro seja obtido a partir de um tabuleiro padrão removendo duas quinas opostas.

  É possível cobrir todo este novo tabuleiro usando peças de dominós?



Solução. Por contradição, assuma que haja uma cobertura de dominós para este tabuleiro. Como o tabuleiro tem $64 - 2 = 62$ casas, 31 dominós são usados na cobertura. Como cada dominó cobre exatamente uma casa escura e uma clara, a cobertura cobre exatamente 31 casas claras e 31 casas escuras.

Entretanto, note que ao remover duas quinas opostas, estamos removendo duas casas de mesma cor (ou ambas escuras, ou ambas claras). Logo a cobertura necessariamente cobre 32 casas de um tipo (no nosso exemplo, escuras) e apenas 30 de outro tipo (no nosso exemplo, claras).

Claramente isto é uma contradição, e tal cobertura não pode existir. $\triangleleft$

Erros comuns em demonstrações

- Existem muitos erros comuns na construção de demonstrações matemáticas.

  Aqui vamos brevemente ver alguns deles.

- Entre os erros mais comuns estão os erros aritméticos e básicos álgebra.

  Até mesmo matemáticos profissionais cometem esses erros, especialmente quando trabalham com fórmulas complicadas: atenção nunca é demais!

- Além disso, cada etapa de uma demonstração matemática precisa estar correta, e a conclusão precisa seguir logicamente das etapas que a precedem.

Erros comuns em demonstrações

- Muitos erros resultam da introdução de um passo que não segue logicamente daqueles que o precedem.

- $\boxed{\text{Exemplo 24}}$ Qual o erro na seguinte "demonstração" de que $1 = 2$?

Passo	**Justificativa**
1. $\exists x, y \in \mathbb{R} : x = y$	Premissa
2. $a = b$	Instanciação existencial de (1)
3. $a^2 = ab$	Multiplicando ambos os lados de (2) por a
4. $a^2 - b^2 = ab - b^2$	Subtraindo b^2 de ambos os lados de (3)
5. $(a + b)(a - b) = b(a - b)$	Fatorando ambos os lados de (4)
6. $a + b = b$	Dividindo ambos os lados de (5) por $(a - b)$
7. $2b = b$	Substituindo (2) em (6) e simplificando
8. $2 = 1$	Dividindo ambos os lados de (7) por b

- Outro erro comum em demonstrações é argumentar a partir de exemplos.
- Exemplo 25 **Teorema:** *"Se $m + n$ é par então $m - n$ é par."*

  Demonstração incorreta: Se $m = 14$ e $n = 6$ então $m + n = 20$, que é par, e $m - n = 8$, que também é par.

  Logo se $m + n$ é par então $m - n$ é par. □