12 Estratégia de Prova

Sumário da Aula

12.1 Prova por Exaustão

Embora provar que uma conjectura é falsa a partir de um contraexemplo **sempre funcione**, provar que uma conjectura é verdadeira por um exemplo **quase nunca funciona**. Um exceção ocorre quando a conjectura é uma afirmação sobre uma coleção finita. E, neste caso, a prova é realizada verificando a conjectura para cada um dos elementos do universo de discurso.

Este tipo de demonstração é chamada de **prova por exaustão** e consiste em um tipo especial de demonstração que **verifica a validade do teorema para cada elemento do universo do discurso** quando este representa uma **coleção finita**.

Exemplo 12.1. Prove que se n é um inteiro positivos com $n \leq 4$, então $(n+1)^3 \geq 3^n$.

Prova: Para provar a conjectura, é preciso verificar que a inequação $(n+1)^3 \geq 3^n$ é verdadeira para todos os elementos do universo de discurso.
Como existe uma quantidade finita de casos,, ou seja, $n = 1,\ 2,\ 3$ e 4, a conjectura pode ser verificada mostrando que ela é verdadeira para todos os casos possíveis. Seja:

n	$(n+1)^3$	3^n	$(n+1)^3 \geq 3^n$
1	$(1+1)^3 = 8$	$3^1 = 3$	T
2	$(2+1)^3 = 27$	$3^2 = 9$	T
3	$(3+1)^3 = 64$	$3^3 = 27$	T
4	$(4+1)^3 = 125$	$3^4 = 81$	T

Verifica-se por exaustão que, para as quatro possibilidades, a inequação $(n+1)^3 \geq 3^n$ é verdadeira.
Portanto, pode-se afirmar que se n é um número inteiro positivo e $n \leq 4$, então é válida a inequação $(n+1)^3 \geq 3^n$. ■

Exemplo 12.2. Prove a conjectura: "**Se um número inteiro entre 1 e 20 for divisível por 6, então ele também é divisível por 3**".

Prova: Sabe-se pela definição de divisibilidade, que um número é divisível por 6 se, e somente se, ele é um múltiplo de 6.
De forma análoga, um número é divisível por 3 se, e somente se, for múltiplo de 3.
Para provar a conjectura, como existe uma quantidade finita de casos (o universo de discurso é uma coleção finita), pode-se construir uma tabela e verificar que a conjectura é verdadeira para todos os casos (números inteiros entre 1 e 20). Veja:

Número	Divisível por 6	Divisível por 3
1	não	
2	não	
3	não	
4	não	
5	não	
6	sim: $6 = 1 \times 6$	sim: $6 = 2 \times 3$
7	não	
8	não	
9	não	
10	não	

Número	Divisível por 6	Divisível por 3
11	não	
12	sim: $12 = 2 \times 6$	sim: $12 = 4 \times 3$
13	não	
14	não	
15	não	
16	não	
17	não	
18	sim: $18 = 3 \times 6$	sim: $18 = 6 \times 3$
19	não	
20	não	

Logo, pode-se concluir que se um inteiro entre 1 e 20 for divisível por 6, então ele também será divisível por 3. ■

12.2 Prova Direta

Em geral, quando a demonstração por exaustão não funciona, para provar que uma sentença na forma $P \to Q$ é verdadeira, pode-se aplicar uma **demonstração direta** em que se pressupõe verdadeira a hipótese P e deduz a conclusão Q.

A prova direta segue o mesmo raciocínio das demonstrações realizadas na lógica proposicional: a partir da suposição da veracidade das hipóteses e, através de uma sequência de passos (axiomas, definições, teoremas já demonstrados e regras de inferência), infere-se a conclusão. Os passos e a escrita da prova direta consistem em:

1. Escrever o teorema que deve ser provado.
2. Expressar o teorema como uma fórmula da lógica de predicados (essa etapa pode ser feita mentalmente ou na etapa anterior).
3. Identificar cada variável usada na prova juntamente com o seu tipo (ex: Seja m um número inteiro).
4. Entender o enunciado e identificar o que são as hipóteses e a conclusão.
5. Marcar o início da demonstração com a palavra **PROVA**.
6. Começar a prova supondo que x é um elemento específico, mas escolhido arbitrariamente, do domínio para o qual a hipótese é verdadeira (ex: Seja $x \in \mathbb{U}$ tal que $P(x)$).
7. Construir passo a passo da prova **apresentando uma justificativa**.
8. Terminar a prova com a dedução da conclusão.

Observações:

São justificativas (Passo 7) aceitáveis em uma prova: pela hipótese; pelo axioma; pelo teorema x provado anteriormente; pela definição; pelo passo y (um passo anterior do argumento); pela regra z da lógica formal.

Exemplo 12.3. Considere a seguinte conjectura: **A soma de dois números pares é um número par.**
Observações:

- A conjectura pode ser reescrita como **"se n e m são dois números pares quaisquer, então $n + m$ é um número par"**.
- Possui a forma simbólica igual a $P_1 \wedge P_2 \to Q$, onde:
  - Hipóteses P_1: "n é número par qualquer" e P_2: "m é número par qualquer"
  - Conclusão Q: "$n + m$ é um número par".
- Definição de número par para seguir com as etapas da prova da conjectura:
  (Definição de Número Par): n é par $\Leftrightarrow \exists$ um inteiro k tal que $n = 2k$.

Prova: (da conjectura: "A soma de dois números pares é um número par".)

1. **Das hipóteses do teorema, sejam n e m dois números números pares quaisquer.**
2. **Então, pela definição de número par, existem números r e $s \in \mathbb{Z}$ tais que $n = 2r$ e $m = 2s$. Provar que $n + m$ é par.**
3. **A soma $n + m = 2r + 2s = 2(r + s)$.**
4. **Por definição, a operação soma é fechada no conjunto dos inteiros, assim, $r + s = t \in \mathbb{Z}$.**
5. **Então, existe um $t \in \mathbb{Z}$, tal que $t = r + s$.**
6. **Dessa forma, $n + m = 2t$.**
7. **Portanto, pela definição de número par, concluí-se que $m + n$ também é par.**

■

A demonstração anterior pode ser reescrita de uma forma mais simples, como apresentada a seguir.

Prova: Sejam n e m dois números pares. Pela definição de número par, existem números $r, s \in \mathbb{Z}$ tais que $n = 2r$ e $m = 2s$. Deseja-se provar que $m + n$ é par.
A soma $n+m = 2r+2s = 2(r+s)$. A operação soma é fechada no conjunto dos inteiros, então segue que $r + s$ também é um número inteiro. Assim, vale dizer que $n+m = 2t$, onde $t = r+s$ e $t \in \mathbb{Z}$.
Portanto, pode-se concluir que $n + m$ também é um número par. ■

Observação

O símbolo ■ que aparece no final da prova pode ser substituído por □ ou c.q.d e indica que a demonstração do teorema foi concluída. O termo c.q.d é a abreviação de "como se queria demonstrar".

Exemplo 12.4. Prove que **Se n é um número inteiro ímpar, então n^2 é ímpar.**
Observações:

- O teorema está escrito na forma $P \to Q$.
- Hipótese: P é "n é um número inteiro ímpar".
- Conclusão: Q é "n^2 é ímpar".

Prova: (Se n é um número inteiro ímpar, então n^2 é ímpar.)
Seja n um número inteiro ímpar. Então, pela definição de número ímpar, $n = 2k + 1$ para algum $k \in \mathbb{Z}$. Queremos mostrar que n^2 também é ímpar.
Elevando ambos os membros da equação $n = 2k + 1$ ao quadrado:

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

As operações da soma e multiplicação são fechadas no conjunto dos números inteiros, então segue que $2k^2 + 2k = t$ para algum $t \in \mathbb{Z}$. Assim, da definição de número ímpar e do resultado $n^2 = 2t + 1$, pode-se concluir que n^2 também é ímpar. ∎

Exemplo 12.5. Prove que **"Se m e n são ambos quadrados perfeitos, então $m.n$ também é um quadrado perfeito.'"**
Dados:

- O teorema está escrito na forma $P_1 \wedge P_2 \to Q(x)$.
- Hipóteses: P_1 : "m é um quadrado perfeito" e P_2 : "n é um quadrado perfeito".
- Conclusão: Q : "$m.n$ é um quadrado perfeito".
- Definição necessária para a prova:
  (Quadrado Perfeito) Um número n é um **quadrado perfeito** se, existe $k \in \mathbb{Z}$ tal que $n = k^2$.

Prova: Sejam m e n ambos quadrados perfeitos. Pela definição (Quadrado Perfeito), existem números $a, b \in \mathbb{Z}$, tais que $m = a^2$ e $n = b^2$.
Queremos provar que $m.n$ também é um quadrado perfeito.
Das propriedades do produto e potenciação:

$$m.n = a^2.b^2 = (a.b)^2$$

Dado que $m.n$ é o quadrado de $a.b$ e dado que $a.b \in \mathbb{Z}$, pode-se concluir que $m.n$ também é um quadrado perfeito. ∎

Exemplo 12.6. Prove que **"Se a soma de dois números inteiros é par, então a sua diferença também é par".**

Prova: Sejam m e n números inteiros tais que a soma $m + n$ é par.
Por definição de número par, $m + n = 2k$, para algum inteiro k.
Queremos provar que $m - n$ também é par.
Subtraindo n dois lados da equação $m + n = 2k$, obtém-se $m = 2k - n$.
Veja a diferença entre m e n, é:

$$\begin{aligned} m - n = \ & (2k - n) - n \ \textbf{ substituindo } \ m = 2k - n \\ & 2k - 2n \\ & 2(k - n) \end{aligned}$$

As operações da soma e multiplicação são fechadas no conjunto dos inteiros. Assim, dados que k e n são ambos números inteiros, a expressão $2(k - n)$ também é um número inteiro. Portanto, como $m - n$ é um múltiplo de dois, pode-se concluir que $m - n$ é par. ■

Exemplo 12.7. Prove que para todo $n \in \mathbb{Z}$, se n é ímpar então $3n + 9$ é par.

Exemplo 12.8. Sejam $a, b \in \mathbb{R}$. Se $0 \leq a < b$ então $a^2 < b^2$.

12.2.1 Erros comuns em demonstração

É preciso ter cuidado em cada passo de uma demonstração matemática para que erros básicos de aritmética e álgebra não sejam cometidos. Cada passo realizado precisa estar correto e a conclusão precisa seguir logicamente os passos que a precedem. Vários erros podem ser cometidos durante uma demonstração, os mais comuns são:

1. **Usar a mesma letra para representar duas coisas diferentes.**

2. **Argumentar a partir de exemplos.**

Teorema: Se a soma de dois números inteiros é par, então a sua diferença também é par.
Prova:
Caso 1: Considere $m = 8$ e $n = 2$ números pares. Então, segue que $m + n = 10$ é par e $m - n = 6$ também é par.
Caso 2: Considere $m = 7$ e $n = 3$ números ímpares. Então, segue que $m + n = 10$ é par e $m - n = 4$ também é par.
Portanto, o teorema é verdadeiro, c.q.d.

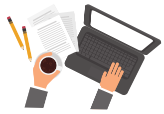
3. **Pular direto para a conclusão.**

Teorema: Se a soma de dois números inteiros é par, então a sua diferença também é par.
Prova:
Suponha m e n números inteiros e que $m+n$ é par. Por definição de número par, $m+n = 2k$ para $k \in \mathbb{Z}$.
Segue que $m = 2k - n$. Portanto, $m - n$ é par.

4. Assumir como verdadeiro o que deve ser provado:

Teorema: Se $m.n$ é ímpar, então m e n são ambos ímpares.
Prova:
Se $m.n$ é ímpar, então por definição $m.n = 2k+1$ para algum $k \in \mathbb{Z}$. Suponha também que m e n são números ímpares. Por definição de números ímpares, $m = 2a + 1$ e $n = 2b + 1$.
Então, $m.n = (2a + 1)(2b + 1) = 2k + 1$ que é ímpar, c.q.d.

12.3 Exercícios



E. 1. Prove as proposições seguintes.

a) Se $n = 25, 100$ ou 169, então n é um quadrado perfeito e é a soma de dois quadrados perfeitos.

b) Se n for um inteiro par tal que $4 \leq n \leq 12$, então n será uma soma de dois números primos.

c) Para qualquer inteiro positivo n menor ou igual a 3, temos que $n! < 2^n$.

d) Para $2 \leq n \leq 4$, temos que $n^2 \leq 2^n$.

E. 2. Prove que se x é um inteiro impar, então x^3 é ímpar.

E. 3. Suponha $x, y \in \mathbb{Z}$. Prove que se x e y são impares, então xy é impar.

E. 4. Prove que se a soma de dois inteiros é par, então sua diferença também é par.

E. 5. Prove que se n e m são quadrados perfeitos, então $(n.m)$ é um quadrado perfeito.

E. 6. Prove que se a e b são números racionais, então $(a + b)$ é um número racional.

E. 7. Sejam $a, b, c \in \mathbb{Z}$. Prove que se $a|b$ e $a|c$ então $a|(b + c)$.

E. 8. Prove que, para quaisquer inteiros $a, b, c,$ se $a|b$ e $b|c$ então $a|c$

E. 9. Prove que, para todo $n \in \mathbb{Z}$, temos que $5n^2 + 3n + 7$ é impar.

E. 10. Prove que para todos os números inteiros, se $a|b$ então $a^2|b^2$.

E. 11. O que está errado na suposta "prova" da afirmação de que $1 = 2$?

Prova:

1.	$a = b$	Sejam a e b dois números inteiros positivos iguais.
2.	$a^2 = ab$	Multiplicando ambos os membros de (1) por a.
3.	$a^2 - b^2 = ab - b^2$	Subtraindo b^2 de ambos os lados de (2).
4.	$(a - b)(a + b) = b(a - b)$	Fatorando ambos os membros de (3).
5.	$a + b = b$	Dividindo ambos os lados de (4) por $(a - b)$.
6.	$2b = b$	Substituindo a por b em (5), pois $a = b$ e simplificando.
7.	$2 = 1$	Dividindo ambos os membros de (6) por b.

E. 12. O que está errado na suposta "prova" do teorema: "Se n^2 é positivo, então n é positivo."

Prova:

1. Suponha que n^2 é positivo.
2. A sentença condicional "se n é positivo, então n^2 é positivo" é verdadeira.
3. Então, podemos concluir que n é positivo.

Referências Bibliográficas

1 HAMMACK, R. H. *Book of Proof*. 2ª. ed. Virginia: Richard Hammack, 2013. v. 1.

2 EPP, S. S. *Discrete Mathematics With Applications*. Fourth. Boston - USA: Cengage Learning, 2010. ISBN 978-0-495-39132-6.

3 HUNTER, D. J. *Fundamentos da Matemática Discreta*. Rio de Janeiro: LTC, 2011.

4 GERSTING, J. L. *Fundamentos Matemáticos para a Ciência da Computação: Matemática Discreta e suas Aplicações*. 7ª. ed. Rio de Janeiro: LTC, 2017.

5 MENEZES, P. B. *Matemática Discreta para a Computação e Informática*. 4ª. ed. Porto Alegre: Bookman, 2013.

6 RIBEIRO, R. G. *Notas de Aula de Matemática Discreta*. [S.l.]: Universidade Federal de Ouro Preto, 2016.

7 BISPO, C. A. F.; CASTANHEIRA, L. B.; FILHO, O. M. S. *Introdução à Lógica Matemática*. São Paulo: CENGAGE Learning, 2011.

8 SCHEINERMAN, E. R. *Matemática Discreta:Uma Introdução.* 2. ed. São Paulo: Cengage Learning., 2016.

9 DAGHLIAN, J. *Lógica e Álgebra de Boole*. 4ª. ed. São Paulo: atlas, 2016.

10 FILHO, E. de A. *Iniciação à Lógica Matemática*. São Paulo: Nobel, 2002.

11 ROSEN, K. H. *Matemática Discreta e Suas Aplicações*. 6ª. ed. Porto Alegre: Mc Graw Hill, 2010.