

# O que é uma prova?

Paulo Feofiloff

<http://www.ime.usp.br/~pf/amostra-de-prova/>

Em matemática, uma prova é uma argumentação precisa que procura convencer o leitor de que uma certa proposição, previamente enunciada, está correta.

Que “cara” tem uma prova? Uma prova é uma sequência de afirmações organizada da seguinte maneira: cada afirmação é consequência simples das afirmações anteriores e das hipóteses da proposição em discussão; a última afirmação é a proposição que se deseja provar.

## Exemplo 1

Considere a configuração do jogo *Mine Hunt* indicada ao lado. Cada “B” representa uma bomba. As posições em branco não têm bombas. As posições marcadas com “?” podem ou não ter bombas. Uma posição marcada com um número  $k$  não tem bomba mas é vizinha de exatamente  $k$  bombas.

Cada posição do tabuleiro é especificada por suas coordenadas. Assim, por exemplo, o extremo superior esquerdo do tabuleiro tem coordenadas  $(1, 1)$  e o cruzamento da primeira linha com a segunda coluna tem coordenadas  $(1, 2)$ .

?	?	1	1	B
?	?	2	2	B
?	?	3	B	
?	?	B	2	
?	?	2	1	
?	?	3	1	
2	B	B	1	
2	3	3	1	

**Proposição:** Não há bomba na posição  $(1, 2)$  da configuração acima.

**Prova,** por contradição:

Suponha, por um momento, que há uma bomba em  $(1, 2)$ .

A posição  $(2, 3)$  é vizinha de duas bombas e há uma bomba em  $(3, 4)$ ;

logo, as posições  $(2, 2)$  e  $(3, 2)$  não têm bomba alguma.

Portanto, o “3” na posição  $(3, 3)$  garante que há uma bomba em  $(4, 2)$ .

Agora, o “2” na posição  $(5, 3)$  garante que não há bomba em  $(5, 2)$  nem em  $(6, 2)$ .

Mas isso é inconsistente com o “3” na posição  $(6, 3)$ .

Esta contradição mostra que  $(1, 2)$  não pode conter bomba.

## Exemplo 2

**Proposição:** A raiz quadrada de 2 é irracional, ou seja, não existem números inteiros positivos  $p$  e  $q$  tais que  $p/q = \sqrt{2}$ .

**Prova,** por contradição:

Suponha que existem números inteiros positivos  $p$  e  $q$  tais que  $(p/q)^2 = 2$ .

Escolha  $p$  e  $q$  de modo que eles não tenham divisor comum, ou seja, de modo que não exista um número inteiro maior que 1 que divida  $p$  e  $q$ .

O número  $p^2$  é par (pois  $p^2 = 2q^2$ ).

O número  $p$  é par (pois o produto de quaisquer dois números ímpares é ímpar).

Seja  $s$  o número  $p/2$ .

O número  $q^2$  é par (pois  $q^2 = p^2/2 = (2s)^2/2 = 2s^2$ ).

O número  $q$  é par.

Os números  $p$  e  $q$  são divisíveis por 2.

Isso contradiz a maneira como escolhemos  $p$  e  $q$ .

A contradição mostra que a raiz quadrada de 2 é irracional.

## Exemplo 3

**Proposição:** Para qualquer número natural não nulo  $n$  tem-se  $1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{1}{6}n(n+1)(2n+1)$ .

**Prova,** por indução em  $n$ :

Base da indução:  $n = 1$ .

Nesse caso, os dois lados da identidade valem 1 e portanto são iguais.

Passo da indução:  $n > 1$ .

Por hipótese de indução,  $1^2 + 2^2 + \dots + (n-1)^2 = \frac{1}{6}(n-1)n(2n-1)$ .

$$\begin{aligned} \text{Portanto, } 1^2 + 2^2 + \dots + n^2 &= \\ &= 1^2 + 2^2 + \dots + (n-1)^2 + n^2 \\ &= \frac{1}{6}(n-1)n(2n-1) + n^2 \\ &= \frac{1}{6}n((n-1)(2n-1) + 6n) \\ &= \frac{1}{6}n(2n^2 - 3n + 1 + 6n) \\ &= \frac{1}{6}n(2n^2 + 3n + 1) \\ &= \frac{1}{6}n(n+1)(2n+1), \text{ como queríamos provar.} \end{aligned}$$

**Mau exemplo.** Eis uma maneira *feia* de organizar a indução:

Base da indução:

Se  $n = 1$  então os dois lados da identidade valem 1 e portanto são iguais.

Passo da indução:

Suponha que a identidade vale para  $n$ .

Vamos provar a identidade para  $n + 1$ :

$$\begin{aligned} 1^2 + 2^2 + \dots + n^2 + (n + 1)^2 &= \\ &= \frac{1}{6} n(n + 1)(2n + 1) + (n + 1)^2 \\ &= \frac{1}{6} (n + 1) (n(2n + 1) + 6(n + 1)) \\ &= \frac{1}{6} (n + 1) (2n^2 + 7n + 6) \\ &= \frac{1}{6} (n + 1) (n + 2)(2n + 3) \\ &= \frac{1}{6} (n + 1)(n + 2)(2(n + 1) + 1), \text{ como queríamos provar.} \end{aligned}$$

## Exemplo 4

**Proposição:** Em qualquer grafo  $(V, E)$ , a soma dos graus dos vértices é igual ao dobro do número de arestas, ou seja,  $\sum_{v \in V} d(v) = 2|E|$ .

**Prova,** por indução em  $|E|$ :

Base da indução:  $|E| = 0$ .

Nesse caso,  $d(v) = 0$  para todo vértice  $v$  e portanto  $\sum_v d(v) = 2|E|$ .

Passo da indução:  $|E| > 0$ .

Hipótese de indução: a identidade vale em qualquer subgrafo próprio de  $(V, E)$ .

Seja  $xy$  uma aresta do grafo.

Seja  $F$  o conjunto  $E - \{xy\}$ .

Seja  $d_F(v)$  o grau de  $v$  no grafo  $(V, F)$ .

Por hipótese de indução,  $\sum_v d_F(v) = 2|F|$ .

Temos  $d(x) = 1 + d_F(x)$ ,  $d(y) = 1 + d_F(y)$  e  $d(v) = d_F(v)$  para todo  $v$  diferente de  $x$  e  $y$ .

Portanto,  $\sum_v d(v) = 1 + 1 + \sum_v d_F(v) = 2 + 2|F|$ .

Mas  $2 + 2|F| = 2|E|$ , e portanto  $\sum_v d(v) = 2|E|$ , como queríamos demonstrar.

**Errado.** Eis uma versão errada da indução:

Base da indução:  $|E| = 0$ .

Nesse caso,  $d(v) = 0$  para todo vértice  $v$  e portanto  $\sum_v d(v) = 2|E|$ .

Passo da indução: Vamos supor que  $\sum_v d(v) = 2|E|$  para um certo grafo  $(V, E)$ .

Acrescente ao grafo uma nova aresta  $xy$ .

Seja  $E'$  o novo conjunto de arestas e

denote por  $d'$  os graus dos vértices no novo grafo.

Temos  $d'(x) = 1 + d(x)$ ,  $d'(y) = 1 + d(y)$  e

$d'(v) = d(v)$  para todo  $v$  diferente de  $x$  e  $y$ .

Portanto,  $\sum_v d'(v) = 1 + 1 + \sum_v d(v) = 2 + 2|E|$ .

Mas  $2 + 2|E| = 2|E'|$ , e assim  $\sum_v d'(v) = 2|E'|$ .

## Exemplo 5

**Proposição:** Em qualquer grafo, todo vértice não isolado é saturado por um emparelhamento máximo.

**Prova:**

Seja  $G$  um grafo e  $u$  um vértice não isolado de  $G$ .

Seja  $M$  um emparelhamento máximo em  $G$ .

Se  $M$  satura  $u$  então nada mais temos que provar.

Suponha agora que  $M$  não satura  $u$ .

Seja  $uv$  qualquer uma das arestas que incidem em  $u$ .

O emparelhamento  $M$  satura  $v$  (pois é máximo).

Seja  $vw$  a aresta de  $M$  que incide em  $v$ .

O conjunto  $(M \cup \{uv\}) - \{vw\}$  é um emparelhamento.

Esse emparelhamento é máximo (pois tem o mesmo tamanho que  $M$ ).

Esse emparelhamento satura  $u$ , como queríamos provar.

## Observação final

É claro que você não precisa seguir fielmente o formato dos exemplos acima: o texto da prova pode ser complementado com comentários e observações que tornem a leitura mais fácil e agradável.

A propósito, veja o artigo de Reuben Hersh — “[Math Lingo vs. Plain English: Double Entendre](#)”, *The American Mathematical Monthly*, v.104 (1997), pp. 48-51 — sobre o jargão da matemática.

## Exercícios

1. Prove, por indução em  $k$ , que  $2^0 + 2^1 + \dots + 2^k = 2^{k+1} - 1$ .
2. [D.E. Knuth, *Fundamental Algorithms*] Seja  $a$  um número positivo qualquer. Afirimo que para todo inteiro positivo  $n$  tem-se

$$a^{n-1} = 1.$$

Eis a prova (por indução em  $n$ ): Se  $n = 1$  então  $a^{n-1} = a^0 = 1$  e portanto a afirmação está correta nesse caso. Agora tome  $n > 1$  e suponha, a título de hipótese de indução, que  $a^{k-1} = 1$  quando  $k = n - 1, n - 2, \dots, 1$ . Temos então

$$a^{n-1} = a^{n-2} \cdot a^1 = a^{n-2} \cdot \frac{a^{n-2}}{a^{n-3}} = 1 \cdot \frac{1}{1} = 1.$$

Portanto, a afirmação está correta para todo inteiro positivo  $n$ , como queríamos provar. Onde está o erro da prova?

3. [D.E. Knuth, *Fundamental Algorithms*] Afirimo que para todo número inteiro positivo  $n$  tem-se

$$\sum_{i=1}^{n-1} \frac{1}{i \cdot (i+1)} = \frac{3}{2} - \frac{1}{n}. \quad (1)$$

Eis a prova (por indução em  $n$ ): Para  $n = 1$ , ambos os lados de (1) valem  $1/2$  e portanto a afirmação está correta nesse caso. Agora tome  $n > 1$  e suponha, como hipótese de indução, que  $\sum_{i=1}^{n-2} \frac{1}{i \cdot (i+1)} = \frac{3}{2} - \frac{1}{n-1}$ . Teremos então

$$\begin{aligned} \sum_{i=1}^{n-1} \frac{1}{i \cdot (i+1)} &= \sum_{i=1}^{n-2} \frac{1}{i \cdot (i+1)} + \frac{1}{(n-1) \cdot n} \\ &= \frac{3}{2} - \frac{1}{n-1} + \frac{1}{(n-1) \cdot n} \\ &= \frac{3}{2} - \frac{1}{n-1} + \frac{1}{n-1} - \frac{1}{n} \\ &= \frac{3}{2} - \frac{1}{n}, \end{aligned}$$

como queríamos demonstrar. Onde está o erro da prova? Alguma coisa deve estar errada, pois quando  $n = 6$  o lado esquerdo de (1) vale  $5/6$  enquanto o lado direito vale  $4/3$ .

4. [M. Blum] Imagine uma dessas barras de chocolate retangulares que consiste em quadradinhos dispostos em linhas e colunas. Uma tal barra pode ser quebrada ao longo de uma linha ou de uma coluna produzindo assim duas barras menores. Qual o número mínimo de quebras necessário para reduzir uma barra com  $m$  linhas e  $n$  colunas aos seus quadradinhos constituintes?
5. [M. Blum] Imagine uma jarra contendo um certo número de bolas brancas e bolas pretas. Suponha também que você tem um suprimento ilimitado de bolas brancas fora da jarra. Agora repita o seguinte procedimento enquanto ele fizer sentido: Retire duas bolas da jarra; se as duas tiverem a mesma cor, coloque uma bola branca na jarra; se as duas tiverem cores diferentes, coloque uma bola preta na jarra. Qual a cor da última bola a sobrar na jarra?