# Métodos de Prova

Mário S. Alvim e Sebastián Urrutia

DCC - UFMG

2014/02

# Provas matemáticas

- Uma **prova** é uma demonstração matemática da certeza a respeito de uma afirmação.
- O nível de detalhamento de uma prova 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.
- Neste curso vamos nos focar em provas formais, utilizando o rigor matemático esperado de um profissional em nível de graduação na área de ciências exatas.
- Provas são importantes em várias áreas da Ciência da Computação:
  - correção de programas;
  - análise de complexidade de algoritmos;
  - propriedades de segurança de sistemas;
  - ...

- **Axioma (ou postulado)**: afirmação assumida como verdadeira sem a necessidade de uma prova; axiomas são considerados “verdades evidentes”.
- **Teorema (ou proposição)**: afirmação a ser provada; teoremas são resultados considerados de interesse em si mesmos.
- **Lema**: afirmação auxiliar a ser provada, geralmente para quebrar a prova de um teorema grande em pedaços menores.
- **Prova (ou demonstração)**: argumento que mostra que uma afirmação (teorema ou lema) é verdadeira.
- **Corolário**: afirmacão derivável facilmente a partir de um teorema já provado; colorários são consequências imediatas de outros resultados.
- **Conjectura**: suposição bem fundada, porém (ainda) sem prova.

- $\boxed{\text{Exemplo 1:}}$

  Seja a fórmula $p(n) = n^2 + n + 41$.

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

  - Evidência de que a conjectura está certa:

    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 |

    *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.

- **Evidência não é o mesmo que prova!**

- $\boxed{\text{Exemplo 2:}}$

  Em 1769, Euler (1707–1783) 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 1987, Noam Elkies proveu um contra-exemplo, mostrando que

    $$95800^4 + 217519^4 + 414560^4 = 422481^4.$$

  - Logo, esta conjectura também é falsa.

- **Ausência de prova não o mesmo que prova de ausência!**

- Construir uma prova é uma arte.

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

- Existem, entretanto, métodos que são úteis para provar uma grande quantidade de afirmações.

  Neste capítulo os seguintes métodos de prova:

  A. prova por contra-exemplo;

  B. prova direta;

  C. prova por contraposição;

  D. prova por divisão em casos;

  E. prova por contradição (ou prova por redução ao absurdo).

- Outros métodos de prova (e.g., prova por indução matemática) serão vistos mais adiante no curso.

- Escreva claramente qual a afirmação que se deseja provar.

  (É comum preceder a afirmação com a palavra **Teorema** ou **Lema**.)

- Delimite claramente o escopo da prova.
  - Indique o início da prova com a palavra **Prova.**
  - Indique o fim da prova com um marcador. Pode-se usar um quadradinho: $\Box$, ou quando a afirmação é a ser provada no fim da demonstração, a abreviação **Q.E.D.** (*quod erat demonstrandum*) ou sua tradução em português, **C.Q.D.** (*conforme queríamos demonstrar*).

- Escreva a prova de tal forma que ela seja auto-contida. Use linguagem natural (português) de forma clara, empregando sentenças completas e bem estruturadas. Podem-se utilizar fórmulas matemáticas, equações, etc., quando necessário.

- Identifique cada variável usada na prova juntamente com seu tipo. Exs.:
  1. Seja $x$ um número real maior que 2.
  2. Suponha que $m$ e $n$ sejam inteiros sem divisores comuns.

- **Importante:** o objetivo principal de uma prova é convencer <u>o leitor</u> de que a afirmação é válida. Não basta que <u>você mesmo</u> esteja convencido, então certifique-se de que está sendo conciso, mas claro.

# Prova por contra-exemplo

- Provas por contra-exemplos funcionam para provar que afirmações são falsas.
- Forma geral:
  1. Expresse a afirmação a ser provada na forma:
  $$\forall x \in D : P(x)$$
  Esta etapa às vezes é feita mentalmente.
  2. Encontre um $x \in D$ tal que $P(x)$ seja falso.

- $\boxed{\text{Exemplo 3:}}$

  Seja $p(n) = n^2 + n + 41$. Prove que a afirmação "$\forall n \in \mathbb{N} : p(n)$ é primo" é falsa.

  **Prova.** Tome o contra-exemplo $n = 40$. Neste caso temos $p(n) = 1681 = 41 \cdot 41$, que não é primo.

  Logo a afirmação é falsa. □

- $\boxed{\text{Exemplo 4:}}$

  Mostre que a afirmação "Todo inteiro positivo pode ser escrito como a soma do quadrado de dois inteiros" é falsa.

  **Prova.** Tome o contra-exemplo 3, que é um inteiro que não pode ser escrito como a soma dos quadrados de dois inteiros.

  Para ver isto, basta ver que os únicos quadrados menores que 3 são 0 e 1, e as somas possíveis destes quadrados são $0 + 0 = 0$, $0 + 1 = 1$, e $1 + 1 = 2$, nenhuma das quais se iguala a 3.

  Logo 3 é um contra-exemplo e a afirmação é falsa. □

# Prova direta

- Forma geral:

  1. Expresse a afirmação a ser provada na forma:

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

     Esta etapa às vezes é feita mentalmente.

  2. Comece a prova 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 válido".

  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 $D$.

- Exemplo 5:

Mostre que se $n$ é um inteiro ímpar, então $n^2$ é ímpar.

(**Obs.** Um inteiro $n$ é par sse existe um inteiro $k$ tal que $n = 2k$. Um inteiro $n$ é ímpar sse existe um inteiro $k$ tal que $n = 2k + 1$.)

**Prova.** Podemos reescrever a afirmação formalmente como $\forall n : P(n) \rightarrow Q(n)$, onde $P(n)$ é a proposição "$n$ é um inteiro ímpar", e $Q(n)$ é "$n^2$ é ímpar".

Para prover uma prova direta desta afirmação, assumimos que a hipótese da implicação, $P(n)$, é verdadeira, ou seja, que $n$ é um inteiro ímpar. Então, pela definição de número ímpar, existe um inteiro $k$ tal que $n = 2k + 1$.

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

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

Logo, pela definição de número ímpar, $n^2$ também é ímpar. $\square$

- Exemplo 6:

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

  (**Obs:** Um inteiro $a$ é um quadrado perfeito se existe um inteiro $b$ tal que $a = b^2$.)

  **Prova.** Para provar este teorema, 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 prova é mostrar que $mn$ será um quadrado perfeito quando $m$ e $n$ o forem. Para ver isto, podemos calcular

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

  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 prova de que a afirmação é verdadeira. $\square$

- Exemplo 7:

Mostre que a soma de dois números racionais é um número racional.

(**Obs:** Um número $n$ é racional quando existem inteiros $p$ e $q$, com $q \neq 0$, tais que $n = p/q$.)

**Prova.** 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 prova 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 $s = t/u$.

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

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

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. $\square$

# Prova por contraposição

- Forma geral:

    1. Expresse a afirmação a ser provada 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 provada:

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

    3. Comece a prova 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 8:

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

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

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

Se $n$ não é ímpar, é porque $n$ é par e, pela definição de número par, $n = 2k$ para algum $k \in \mathbb{N}$. 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, a prova por contraposição é concluída com sucesso. $\square$

- Exemplo 9:

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

  **Prova.** Para produzir uma prova por contraposição, vamos demonstrar que quando a conclusão da implicação é falsa, sua hipótese também deve ser falsa.

  A conclusão da implicação pode ser escrita como $(a \leq \sqrt{n}) \vee (a \leq \sqrt{n})$. Logo, por de Morgan, a negação da conclusão 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 pode ser escrita como $n = ab$, e sua negação é $n \neq ab$.

  Queremos mostrar que 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

$$ab \quad > \quad \sqrt{n}\sqrt{n} \quad = \quad n,$$

  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 prova por contraposição é concluída com sucesso. $\square$

- A prova por contradição se baseia no fato de que se uma afirmação nos leva a concluir um absurdo (contradição), a afirmação necessariamente é falsa.
- Em outras palavras, se a negação de uma afirmação nos leva a concluir um absurdo (contradição), a afirmação necessariamente é verdadeira.
- Forma geral:
  1. Para provar que a afirmação $p$ é verdadeira, assuma que sua negação $\neg p$ é verdadeira.
  2. Mostre que $\neg p$ leva a uma contradição, ou seja, que

$$\neg p \rightarrow F.$$

- $\boxed{\text{Exemplo 10:}}$

  Mostre que em um grupo de 22 dias, ao menos 4 dias caem no mesmo dia da semana.

  **Prova.** Seja $p$ a proposição "Em um grupo de 22 dias, ao menos 4 dias caem no mesmo dia da semana".

  Suponha que $\neg p$ é verdadeiro, ou seja, que "Em um grupo de 22 dias, no máximo 3 dias caem no mesmo dia da semana". Neste caso, no máximo 21 dias podem ser escolhidos para fazer parte de um grupo (já que há apenas 7 dias na semana). Mas isso contradiz a premissa de que o grupo tem 22 dias.

  Em outras palavra, se $r$ é a proposição "22 dias são escolhidos", teríamos $\neg p \rightarrow (r \wedge \neg r)$, ou seja, $\neg p \rightarrow F$.

  Logo, $\neg p$ não pode ser verdadeiro, ou seja, $p$ é verdadeiro. $\square$

- $\boxed{\text{Exemplo 11:}}$

Mostre que se $3n + 2$ é ímpar, então $n$ é ímpar.

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

Para provar por contradição, vamos assumir que $p \rightarrow q$ é 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. $\square$

- Exemplo 12:

Vamos revisitar o exemplo da primeira aula de MD (recordar é viver!) e mostrar que $\sqrt{2}$ é irracional.

**Prova.** Suponha o contrário do que queremos provar, ou seja, que $\sqrt{2}$ é 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. $\square$

# Prova por divisão em casos

- Utilizada geralmente para provar que $p \to q$.
- A prova divide $p$ em casos, e mostra que $q$ segue de qualquer caso possível.
- Forma geral:

  1. Para mostrar que $p \to q$, primeiro mostre que
  $$p \equiv p_1 \vee p_2 \vee \ldots \vee p_n$$
  2. Mostre, separadamente, cada uma das implicações
  $$\begin{aligned} p_1 &\to q \\ p_2 &\to q \\ \ldots &\to \ldots \\ p_n &\to q \end{aligned}$$

- $\boxed{\text{Exemplo 13:}}$

  Mostre que, dados dois números reais $x$, $y$, $min(x, y) + max(x, y) = x + y$.

  **Prova.** 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, podemos concluir que sempre teremos $min(x, y) + max(x, y) = x + y$. $\square$

- $\boxed{\text{Exemplo 14:}}$

  Mostre que $\lfloor \frac{n}{2} \rfloor + \lceil \frac{n}{2} \rceil = n$.

  **Prova.** Só há duas possibilidades para $n$: ou ele é par, ou é ímpar. Vamos analisar cada caso separadamente.

  - Se $n$ é par, então $\lfloor \frac{n}{2} \rfloor + \lceil \frac{n}{2} \rceil = \frac{n}{2} + \frac{n}{2} = n$
  - Se $n$ é ímpar, então $\lfloor \frac{n}{2} \rfloor + \lceil \frac{n}{2} \rceil = \frac{n-1}{2} + \frac{n+1}{2} = n$

  Logo, podemos concluir que a afirmação é sempre verdadeira. □

## Prova de equivalências

- É muito comum termos que mostrar que um conjunto de afirmações são todas equivalentes.
- Forma geral:
  1. Para mostrar que $p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n$, mostre, separadamente, cada uma das implicações

$$\begin{aligned} p_1 &\to p_2 \\ p_2 &\to p_3 \\ \ldots &\to \ldots \\ p_n &\to p_1 \end{aligned}$$

- **Importante:** A prova não está completa se não se fechar o ciclo de implicações, provando que a última proposição implica de volta na primeira: $p_n \to p_1$.
- **Caso especial:** Para provar que $p_1 \leftrightarrow p_2$ podemos mostrar, separadamente, que $p_1 \to p_2$ e que $p_2 \to p_1$.

# Erros comuns em provas

- Argumentar a partir de exemplos.

  **Teorema:** "Se $m + n$ é par então $m - n$ é par."

  **Prova incorreta:** Se $m = 14$ e $n = 6$ então $m + n = 20$ que é par e $m - n = 8$ que também é par. $\square$

- Usar a mesma letra para representar duas coisas diferentes.

- Pular para uma conclusão; ou alegar a verdade de alguma coisa sem dar uma razão adequada.

  **Teorema:** "Se $m + n$ é par então $m - n$ é par."

  **Prova incorreta:** Suponha que $m$ e $n$ sejam inteiros e que $m + n$ é par. Pela definição de par, $m + n = 2k$ para algum inteiro $k$. Então $m = 2k - n$ e assim $m - n$ é par. $\square$

- Exercício: Corrija as provas acima, provando corretamente a afirmação "Se $m + n$ é par então $m - n$ é par".

- Todas as falácias que vimos na aula sobre inferência lógica são erros comuns em provas.