Técnicas de Prova

Mário S. Alvim
(msalvim@dcc.ufmg.br)

Matemática Discreta

DCC-UFMG
(2016/02)

Técnicas de prova: Introdução

- 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.
- Nesta seção vamos nos focar em provas 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:
  1. correção de programas;
  2. análise de complexidade de algoritmos;
  3. propriedades de segurança de sistemas;
  4. ...

Introdução às provas

Terminologia

- Um **axioma (ou postulado)** é afirmação assumida como verdadeira sem a necessidade de uma prova; axiomas são considerados "verdades auto-evidentes".
- Um **teorema** é uma afirmação que se pode demonstrar ser verdadeira. Um teorema é um resultado considerado interessante em si mesmo.
- Uma **proposição** é também uma afirmação que se pode demonstrar verdadeira, mas considerada um teorema "de menor interesse".
- Um **lema** é uma afirmação auxiliar a ser provada, geralmente para quebrar a prova de um teorema grande em pedaços menores.
- Uma **prova (ou demonstração)** é um argumento que mostra que uma afirmação (teorema, proposição ou lema) segue de um conjunto de premissas.
- Um **corolário** é afirmacão derivável facilmente a partir de um teorema já provado. Colorários são consequências imediatas de outros resultados.
- Uma **conjectura** é suposição bem fundada, porém (ainda) sem prova. Uma vez provada, uma conjectura se torna um teorema ou uma proposição.

Evidência versus prova

- 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!

Evidência versus prova

- 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 1987, Noam Elkies proveu um contra-exemplo, mostrando que

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

  Logo, esta conjectura também é falsa. ◁

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

Evidência versus prova: uma piadinha ;-)

- **Conjectura:** Todos os números ímpares maiores que 1 são primos.

  Como cada profissional "prova" esta conjectura acima?

  - **Matemático**: *"3 é primo, 5 é primo, 7 é primo, mas* $9 = 3^2$ *não é primo, logo a conjectura é falsa."*
  - **Físico**: *"3 é primo, 5 é primo, 7 é primo, 9 não é primo, 11 é primo, 13 é primo. Assim o número* 9 *deve ser um erro experimental, e a conjectura é verdadeira."*
  - **Advogado**: *"Senhoras e senhores do júri: não há duvida de que números ímpares são todos primos. A evidência é clara: 3 é primo, 5 é primo, 7 é primo, 9 é primo, e assim por diante!"*
  - **Professor**: *"3 é primo, 5 é primo, 7 é primo, ... O restante fica para os alunos resolverem na lista de exercícios."*

Técnicas de prova

- 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, técnicas que são úteis para provar uma grande quantidade de afirmações.

  Neste capítulo os seguintes técnicas de prova:

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

- Outras técnicas de prova (e.g., prova por indução matemática) serão vistas mais adiante no curso.

Como escrever uma prova

- 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 □, ou
  - a abreviação **Q.E.D.** (do latim *"quod erat demonstrandum"*), ou
  - sua tradução em português, **C.Q.D.** (*"conforme queríamos demonstrar"*).
- Escreva a prova 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.

Como escrever uma prova

- 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 o leitor de que o resultado (teorema, proposição, lema) é verdadeiro.

  Não basta que você mesmo esteja convencido!

  Certifique-se de que está sendo conciso, mas claro.

Prova direta

- Forma geral:
  1. Expresse a afirmação a ser provada na forma:

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

     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 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.

Prova direta

- Exemplo 3: 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. Queremos mostrar que $\forall n : (P(n) \to Q(n))$, onde $P(n)$ é o predicado *"n é um inteiro ímpar"*, e $Q(n)$ é o predicado *"n^2 é ímpar"*.

  Para produzir uma 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. □

Prova direta

- Exemplo 4: 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 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 prova é mostrar que mn será um quadrado perfeito quando m e n o forem. Para ver isto, podemos calcular

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

  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. □

Prova direta

- Exemplo 5: 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 $s = t/u$.

Prova direta

- Exemplo 5: (Continuação)

  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. □

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.

Prova por contraposição

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

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

Para produzir uma prova por contraposição, vamos demonstrar que $\forall n \in \mathbb{N} : (\neg Q(n) \rightarrow \neg P(n))$. 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 $k \in \mathbb{N}$. 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. □

Prova por contraposição

- Exemplo 7: 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 sempre que a conclusão da implicação é falsa, sua hipótese também é falsa.

A conclusão da implicação pode ser escrita como $(a \leq \sqrt{n}) \vee (b \leq \sqrt{n})$.

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 $n \neq ab$.

Prova por contraposição

- Exemplo 7: (Continuação)

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. □

Prova por contradição

- A prova por contradição se baseia no fato de que se partindo de uma premissa p, e aplicando regras de infererência corretamente, chegamos a uma conclusão falsa, então a premissa p deve ser necessariamente falsa.
- Equivalentemente, se ao tomarmos como premissa a negação $\neg p$ de uma afirmação chegamos a um absurdo (contradição), então a afirmação p deve ser necessariamente 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

$$\neg p \rightarrow F.$$

Prova por contradição

- Exemplo 8: 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. □

Prova por contradição

- Exemplo 9: 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. □

Prova por contradição

- Exemplo 10: 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. □

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.

Prova por contra-exemplo

- Exemplo 11: 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. □

- Exemplo 12: 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 por divisão em casos

- Utilizada geralmente para provar que $p \rightarrow q$.
- A prova divide p em casos, e mostra que q segue de qualquer caso possível.
- Forma geral:
  1. Para mostrar que $p \rightarrow q$, primeiro mostre que
  $$p \equiv p_1 \vee p_2 \vee \ldots \vee p_n$$
  2. Mostre, separadamente, cada uma das implicações
  $$p_1 \rightarrow q$$
  $$p_2 \rightarrow q$$
  $$\ldots \rightarrow \ldots$$
  $$p_n \rightarrow q$$

Prova por divisão em casos

- 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 $min(x, y) + max(x, y) = x + y$. □

Prova por divisão em casos

- Exemplo 14: Mostre que $|xy| = |x||y|$, onde x e y são números reais.

  (**Obs.** $|a|$ é o módulo do número real a, definido como $|a| = a$ quando $a \geq 0$, e como $|a| = -a$ quando $a<0$.)

  Prova. Note que há quatro casos possíveis para a combinação de x e y:

  - x e y são ambos não-negativos,
  - x é não-negativo e y é negativo,
  - x é negativo e y é não-negativo, ou
  - x e y são ambos negativos.

Prova por divisão em casos

- Exemplo 14: (Continuação)

  Vamos analisar cada caso separadamente:

  - Se x e y são ambos não-negativos, então $xy \geq 0$ e temos
    $$|xy| = xy = |x||y|.$$
  - Se x é não-negativo e y é negativo, então $xy < 0$ e temos
    $$|xy| = -xy = x(-y) = |x||y|.$$
  - Se x é negativo e y é não-negativo, então $xy < 0$ e temos
    $$|xy| = -xy = (-x)y = |x||y|.$$
  - Se x e y são ambos negativos, então $xy \geq 0$ e temos
    $$|xy| = xy = (-x)(-y) = |x||y|.$$

  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
     $$p_1 \rightarrow p_2$$
     $$p_2 \rightarrow p_3$$
     $$\ldots \rightarrow \ldots$$
     $$p_n \rightarrow p_1$$
- Importante: A prova não está completa se não se fechar o ciclo de implicações, provando que a última proposição implica de volta na primeira: $p_n \rightarrow p_1$.
- Caso especial: Para provar que $p_1 \leftrightarrow p_2$ podemos mostrar, separadamente, que $p_1 \rightarrow p_2$ e que $p_2 \rightarrow p_1$.

Prova de existência

- Uma prova de um teorema do tipo $\exists x : P(x)$ é chamada de **prova de existência**.
- Há duas maneiras de se produzir uma prova existencial:
  1. Uma prova **construtiva** produz um elemento a tal que $P(a)$ seja verdadeiro.

     O elemento a é chamado de **testemunha** da prova.
  2. Uma prova **não-construtiva** não produz uma testemunha, mas prova $\exists x : P(x)$ de alguma outra forma.

     Uma maneira é produzir, por exemplo, uma prova por contradição.

Prova de existência: construtiva

- Exemplo 15: Mostre que existe um inteiro positivo que pode ser escrito como a soma de cubos de inteiros positivos de duas maneiras distintas.

  Prova. Após uma busca trabalhosa (por exemplo, usando um programa de computador), encontramos que
  $$1\,729 = 10^3 + 9^3 = 12^3 + 1^3.$$
  □
- A prova acima é construtiva porque ela produz uma testemunha (o número 1 729 junto com suas decomposições) que atesta a existência desejada.

Prova de existência: não-construtiva

- Exemplo 16: Existem números irracionais x e y tais que x^y é racional.

  Prova. Sabemos que $\sqrt{2}$ é irracional (já provamos isto). Considere o número $\sqrt{2}^{\sqrt{2}}$. Há duas possibilidades para este número:

  1. Ele é racional. Neste caso temos dois números irracionais $x = \sqrt{2}$ e $y = \sqrt{2}$ tais que x^y é racional.
  2. Ele é irracional. Neste caso podemos calcular que

  $$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2,$$

  é um número racional. Assim temos dois números irracionais $x = \sqrt{2}^{\sqrt{2}}$ e $y = \sqrt{2}$ tais que x^y é racional. □

- A prova acima é não-construtiva porque ela não produz uma testemunha que atesta a existência desejada. Sabemos que ou $x = \sqrt{2}$ e $y = \sqrt{2}$ ou $x = \sqrt{2}^{\sqrt{2}}$ e $y = \sqrt{2}$ satisfazem a propriedade, mas não sabemos qual destes dois pares é o certo!

Erros comuns em provas

- Argumentar a partir de exemplos.
- Exemplo 17: **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. □
- Pular para uma conclusão; ou alegar a verdade de alguma coisa sem dar uma razão adequada.
- Exemplo 18: **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. □
- Exercício: Corrija as provas acima, provando corretamente a afirmação *"Se $m + n$ é par então $m - n$ é par"*.
- Muitas das falácias que vimos na aula sobre inferência lógica são erros comuns em provas.

O papel de problemas em aberto

- Algumas conjecturas ficam em aberto por muito tempo antes que se consiga provar sua veracidade ou falsidade.
- Mesmo que falhem a provar ou disprovar a conjectura, frequentemente matemáticos fazem muitos avanços importantes ao tentar.
- Exemplos:
  1. **O Último Teorema de Fermat:** Não existem inteiros positivos x, y, z que satisfaçam a equação
  $$x^n + y^n = z^n$$
  para algum $n > 2$.

  Esta conjectura ficou em aberto de 1 621 até 1 994, quando foi resolvida.

  Tentando prová-la, alguns matemáticos criaram o importante campo de teoria dos números algébrica (mas que não resolveu a conjectura).
  2. O maior problema em aberto em ciência da computação é o **Problema de P vs. NP**:

  "Todo problema cuja solução pode ser rapidamente verificada por um computador pode também ser rapidamente resolvido por um computador?"