Métodos de Prova

Antonio Alfredo Ferreira Loureiro

loureiro@dcc.ufmg.br

http://www.dcc.ufmg.br/~loureiro

Introdução

- Objetivo: ter precisão de pensamento e linguagem para obter a certeza matemática a respeito de um determinado problema.

- Métodos de prova:
  - Prova direta
  - Contra-exemplo
  - Divisão em casos
  - Prova por contradição
  - Prova por contraposição

Prova direta: Definições

- É importante saber o significado de cada termo na afirmação matemática.

- Definição de par e ímpar:
  - n é par $\Leftrightarrow \exists$ um inteiro k tal que $n = 2k$
  - n é ímpar $\Leftrightarrow \exists$ um inteiro k tal que $n = 2k + 1$

- Exemplos:

  (a) 0 é par?

  Sim. $0 = 2 \times 0$.

  (b) -301 é ímpar?

  Sim. $-301 = 2 \times (-151) + 1$.

  (c) Se a e b são inteiros, $6a^2b$ é par? Por que?

  $6a^2b = 2 \times (3a^2b)$

  O conjunto dos números inteiros é "fechado" para as operações de $+$, $-$ e $\times$. Logo, $3a^2b$ é um número inteiro e, consequentemente, o seu dobro.

  (d) Se a e b são inteiros, então $10a + 8b + 1$ é ímpar. Por que?

  Sim. $10a + 8b + 1 = 2 \times (5a + 4b) + 1$.

  (e) Todo número inteiro é par ou ímpar.

Prova direta: Definições

- Definição de primo e número composto:
  - n é primo $\Leftrightarrow$
    $\forall$ inteiros positivos r e s, se $n = r \times s$, $n > 1$, então $r = 1$ ou $s = 1$.
  - n é composto $\Leftrightarrow$
    $\exists$ inteiros positivos r e s tal que $n = r \times s$, e $r \neq 1$ e $s \neq 1$.

- Questão: $\forall$ inteiro n, $n \geq 2$, n é um número primo ou um número composto?
  Sim. Uma definição é a negação da outra.

Provando proposições existenciais

- $\exists\, x \in D$ tal que $Q(x) = V$ sse $Q(x)$ é V para pelo menos um x em D.

- Possíveis métodos de prova:
  (a) Ache/apresente x em D que faz $Q(x)$ verdadeiro.
  (b) Mostre como achar x que faz $Q(x)$ verdadeiro.
  ➜ Métodos de prova construtiva de existência.

- Exemplo:
  Prove: $\exists$ um inteiro par n que pode ser escrito de duas formas diferentes como a soma de dois números primos.

$$n = 10 = 5 + 5 = 7 + 3$$

- Exemplo:
  Sejam r e s inteiros.
  Prove: $\exists$ um inteiro k, expresso em termos de r e s, tal que $22r + 18s = 2k$.

$$22r + 18s = 2 \times (11r + 9s) = 2k$$

Prova não-construtiva de existência

- Consiste em mostrar que:
  (a) A existência de um valor x, que faz com que $Q(x)$ seja verdadeiro, é garantida por um axioma ou teorema; ou
  (b) A suposição que não existe um valor x leva a uma contradição.

- Desvantagem deste tipo de prova:
  – Pode não dar uma "pista" de como ou onde x pode ser encontrado.

- Tendência em computação devido ao acesso a computadores cada vez mais rápidos em ambientes paralelos e distribuídos:
  – Busca de uma prova construtiva através de um programa de computador.
  – Exemplo ligado à teoria de CC: Michael R. Fellows & Michael A. Langston. *Nonconstructive tools for proving polynomial-time decidability*, Journal of the ACM (JACM), 35(3):727–739, July 1988.
  – Veja https://en.wikipedia.org/wiki/Non-constructive_algorithm_existence_proofs

Provando afirmações universais

- A maioria das afirmações em matemática são universais da forma:

$$\mathcal{A}\text{: } \forall x \in D, \text{ se } P(x) \text{ então } Q(x).$$

- Qual é uma possível forma de provar $\mathcal{A}$ no caso de D ser finito ou existir um número finito de valores x que satisfazem $P(x)$?
  - Método da exaustão.

- Método da exaustão:
  $\forall n \in \mathbb{Z}$, se n é par e $4 \leq n \leq 30$, então n pode ser escrito como a soma de dois números primos.

4 = 2 + 2	6 = 3 + 3	8 = 3 + 5	10 = 5 + 5
12 = 5 + 7	14 = 11 + 3	16 = 5 + 11	18 = 7 + 11
20 = 7 + 13	22 = 5 + 17	24 = 5 + 19	26 = 7 + 19
28 = 11 + 17	30 = 11 + 19		

  ➜ Este método é pouco prático porque em geral os domínios não são finitos ou são muito grandes.

Provando afirmações universais

- Método da generalização de um elemento específico genérico:

  Para mostrar que cada elemento de um domínio satisfaz uma certa propriedade, suponha que x é um elemento específico mas escolhido arbitrariamente de um domínio e mostre que x satisfaz a propriedade.

- Como mostrar que x satisfaz uma propriedade da forma

  se $P(x)$ então $Q(x)$?

  - A única forma para a sentença $P(x) \rightarrow Q(x)$ ser falsa é $P(x)$ ser V e $Q(x)$ ser F.
  - Para mostrar que $P(x) \rightarrow Q(x)$ é V suponha que $P(x)$ é V e mostre que $Q(x)$ também deve ser V.
  - Para provar que $\forall x \in D, P(x) \rightarrow Q(x)$, deve-se supor que x é um elemento específico mas escolhido arbitrariamente do domínio D que satisfaz $P(x)$, e deve-se provar que x satisfaz $Q(x)$.

  ➜ **Prova direta**.

Prova direta

1. Expresse a afirmação a ser provada na forma $\forall x \in D, P(x) \rightarrow Q(x)$. [Geralmente feito mentalmente]
2. Comece a prova supondo que x é um elemento específico de D mas escolhido arbitrariamente para o qual a hipótese $P(x)$ é V. [Normalmente abreviado para "Suponha $x \in D$ e $P(x)$"]
3. Mostre que a conclusão é V usando definições, resultados anteriores e as regras de inferência lógica.

- Como x é escolhido arbitrariamente:
  - ele pode ser generalizado para todos os elementos de D, e
  - não depende de nenhuma suposição especial sobre x

Prova direta: Exemplo

- **Teorema**:
  - Se a soma de dois números inteiros é par, então a sua diferença também é par. [Linguagem natural]
  - $\forall$ inteiros m e n, se $m + n$ é par então $m - n$ é par. [Linguagem formal]

- Prova:
  - Suponha m e n são inteiros [específicos mas escolhidos arbitrariamente] tal que $m + n$ é par.

  ➜ Deve-se mostrar que $m - n$ é par.
  - Pela definição de par, $m + n = 2k$ para algum inteiro k.
  - Subtraindo n dos dois lados, m pode ser expresso como: $m = 2k - n$
  - A diferença entre m e n pode ser expressa como

$$\begin{aligned} m - n &= (2k - n) - n \quad \text{substituindo } m \text{ pelo valor acima} \\ &= 2k - 2n \\ &= 2(k - n) \end{aligned}$$

  - A expressão $k - n$ é um número inteiro que multiplicado por 2 é um inteiro par. [O que devia ser mostrado.]

Regras para escrever provas de afirmações universais

- Escreva o teorema a ser provado.

- Marque o início da prova com a palavra PROVA.

- Escreva a prova de tal forma que ela seja auto-contida.
  - Identifique cada variável usada na prova juntamente com o seu tipo.

    Exemplos: Seja x um número real maior que 2.

    Suponha que m e n são inteiros.

  ➜ Similar a declaração de variáveis e seus tipos numa linguagem de programação.

- Escreva provas em linguagem natural usando sentenças completas.

Erros comuns

- Argumentar a partir de exemplos:
  - Exemplo incorreto da prova do teorema:
    Se $m = 14$ e $n = 6$ então $m + n = 20$ que é par e $m - n = 8$ que também é par.

- Usar a mesma letra para representar duas coisas diferentes

- Pular para uma conclusão:
  - Alegar a verdade de alguma coisa sem dar uma razão adequada.
  - Exemplo: 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.

Erros comuns

- Usando a questão a ser provada:
  Assumir como verdadeiro o que deve ser provado—variação de pular para uma conclusão. Exemplo: Prove que, se m e n são dois inteiros tais que $m \cdot n$ é ímpar então m e n são ambos ímpares.
  - Suponha m e n são números ímpares.
  - Se $m \cdot n$ é ímpar, então $m \cdot n = 2k + 1$ para algum inteiro k.
  - Também pela definição de ímpar, $m = 2a + 1$ e $n = 2b + 1$ para inteiros a e b.
  - Então $m \cdot n = (2a + 1)(2b + 1) = 2k + 1$, que é ímpar por definição.

- Uso incorreto do vocábulo SE.
  - Exemplo: Suponha que p é um número primo. Se p é primo, então p não pode ser escrito como o produto de dois números menores que são inteiro.
  - O vocábulo SE, nesta última sentença, coloca em dúvida se de fato p é primo ou não.

Prova por contra-exemplo

- Para negar uma afirmação da forma

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

ache um valor de x em D para o qual $P(x)$ é V e $Q(x)$ é F. O elemento x é chamado de contra-exemplo.

- Exemplo:
Negue a seguinte afirmação:

$$\forall a, b \in \mathbb{R}, (a^2 = b^2) \rightarrow (a = b).$$

Contra-exemplo:
$a = 1$ e $b = -1$.

Prova e contra-exemplo

- Último Teorema de Fermat:
  - Não existem inteiros positivos x, y, z e $n \geq 3$ tais que $x^n + y^n = z^n$.
  - ➜ "Teorema" (conjectura proposta em 1637), provado em 1994 e publicado em 1995 (358 anos depois); não existe contra-exemplo.

- Conjectura de Goldbach (1690–1764)
  - Todo inteiro maior que 2 pode ser representado como uma soma de dois primos. [Uma das conjecturas mais antigas de teoria dos números.]
  - Conjectura já verificada por um programa de computador para números até $2{\cdot}10^{18}$ (Novembro de 2010). Veja mais informações na página de Tomás Oliveira e Silva da Universidade do Aveiro, Portugal, em `http://www.ieeta.pt/~tos/goldbach.html`.
  - ➜ Não quer dizer que seja verdade para todos os números entre $2{\cdot}10^{18}$ e ∞.

Prova e contra-exemplo

- Seja $p(n) = n^2 + n + 41$.
  - Conjectura: $\forall n \in \mathbb{N}, p(n)$ é primo.
    Evidência:

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, $p(40) = 1681$, que não é primo!

- Em 1769, Euler (1707–1783) conjecturou que $a^4 + b^4 + c^4 = d^4$ não tinha solução no conjunto dos números inteiros positivos.
  - Em 1987, ou 218 anos depois, Noam Elkies provou que $95800^4 + 217519^4 + 414560^4 = 422481^4$.

Conjectura

Escreva

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\ldots+\frac{1}{99\cdot 100}$$

como um fração usando os menores termos.

Somando os primeiros termos e simplificando temos que:

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}=\frac{2}{3}$$

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}=\frac{3}{4}$$

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\frac{1}{4\cdot 5}=\frac{4}{5}$$

o que leva a conjectura que para todos os inteiros positivos n,

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\ldots+\frac{1}{n(n+1)}=\frac{n}{n+1}$$

Conjectura

- Definição:
  - Inferir ou deduzir que algo é provável, com base em presunções, evidências incompletas; hipótese, suposição (Dicionário Houaiss).

➜ Esta conjectura é verdadeira?

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \ldots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

Prova e contra-exemplo

- Hipótese:

$$313(x^3 + y^3) = z^3$$

não tem solução no conjunto $\mathbb{Z}^+$.

➜ Falso, mas o menor contra-exemplo tem mais de 1000 dígitos.

- O computador mais "poderoso" não seria capaz de obter essa solução usando a estratégia baseada na força bruta.

- Por que é importante resolver esse problema?
  - Achar soluções para tais equações é importante na área de curvas elípticas
  - Curvas elípticas são importantes no estudo de fatoração de inteiros "grandes"
  - Fatorar inteiros "grandes" é importante no estudo de sistemas criptográficos

  ➜ Criptografia é a base de todos os sistemas seguros de comunicação atualmente!

Prova com o uso de computador
Coloração de mapas

Proposição: Cada mapa pode ser colorido com quatro cores de modo que regiões adjacentes tenham cores diferentes.

A prova desta proposição é difícil e levou mais de um século para ser aperfeiçoada.

Nesse período, muitas provas incorretas foram propostos, incluindo uma que foi considerada válida por 10 anos no final do século XIX.

Uma prova extremamente trabalhosa foi finalmente encontrada em 1976 pelos matemáticos Kenneth Appel e Wolfgang Haken, que utilizaram um programa para categorizar os mapas "coloríveis" de quatro cores.

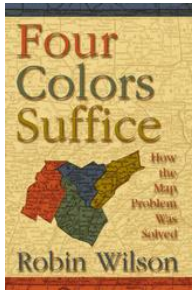
Nota: Duas regiões são adjacentes somente quando elas compartilham um segmento limítrofe de comprimento positivo. Elas não são consideradas adjacentes se seus limites encontram em alguns pontos.

Prova com o uso de computador
Coloração de mapas

O programa deixou alguns milhares de mapas não categorizados, que foram verificados à mão.

Houve muita discussão sobre se esta era uma prova legítima: a prova era grande para ser verificada sem um computador, e ninguém podia garantir que o resultado calculado estava certo nem o trabalho feito à mão.

Na última década, uma prova mais inteligível foi proposta mas ainda foi necessário verificar a coloração de várias centenas de mapas especiais usando um programa.



Four Colors Suffice. How the Map Problem was Solved. Robin Wilson. Princeton Univ. Press, 2003, 276pp. ISBN 0-691-11533-8.

Veja também www.math.gatech.edu/~thomas/FC/fourcolor.html

Prova e hipótese: Humor

Hipótese: todos números ímpares maiores que 1 são primos.

- Matemático:
  - 3 é primo, 5 é primo, 7 é primo, mas $9 = 3 \times 3$, que não é primo, e a hipótese é falsa!
- Estatístico:
  - Tomemos uma amostra de impares: 5, 13, 37, 41 e 53. Ela contém somente números primos. Portanto, todos números impares são números primos.
- Físico:
  - 3 é primo, 5 é primo, 7 é primo, mas 9 não é primo, 11 é primo, 13 é primo. Assim, 9 deve ser um erro experimental, e assim, a hipótese é verdadeira.
- Químico:
  - 3 é primo, 5 é primo, 7 é primo, . . . Já é o suficiente!
- Advogado:
  - Senhores e senhoras do juri: não há dúvida que números ímpares são primos. A evidência é clara: 3 é primo, 5 é primo, 7 é primo, 9 é primo, 11 é primo, e assim por diante!
- Professosr:
  - 3 é primo, 5 é primo, 7 é primo. O restante fica como exercício de casa para os alunos.
- Engenheiro 1:
  - 3 é primo, 5 é primo, 7 é primo, 9 é . . . , 9 é . . . . Vamos usar a aproximação de que 9 é primo!
- Engenheiro 2:
  - 3 é primo, 5 é primo, 7 é primo. A partir deste ponto precisamos fazer um orçamento do trabalho para sabermos quanto isto vai te custar.
- Economista:
  - 2 é primo, 4 é primo, mas na atual conjuntura dos processos de globalização . . .

Definição de racional e irracional

- Um número real r é racional $\Leftrightarrow \exists$ inteiros a e b tal que $r = a/b$ e $b \neq 0$.

- Um número real que não é racional é irracional.

Definição de racional e irracional

Exemplos:

(a) $10/3$ é racional?

Sim. Quociente de inteiros.

(b) 0.281 é racional?

Sim. Número na notação decimal que representa $281/1000$.

(c) Qualquer número representado numa calculadora tradicional é racional?

Sim. O "display" da calculadora é finito e por essa razão todos os números representados são racionais.

(d) $0.121212\ldots$ é racional?

Sim.

Seja $x = 0.121212\ldots$ e $100x = 12.121212\ldots$.

$$\begin{aligned} 100x - x &= 12.121212\ldots - 0.121212\ldots \\ 99x &= 12 \\ x &= 12/99 \end{aligned}$$

Termos num sistema formal

- Axioma ou postulado—do Grego $\alpha\xi\iota o\varsigma$ (áxios): Afirmações que são aceitas como verdadeiras.

- Lema—do Grego $\lambda\alpha\mu\beta\acute{\alpha}\nu\epsilon\iota\nu$ (lambanein): Afirmação que deve ser provada e que normalmente é usada na prova de um teorema.

- Teorema—do Grego $\theta\epsilon o\rho\epsilon\tilde{\iota}\nu$ (theorein): Afirmação que deve ser provada e que normalmente é o resultado principal.
  - Um teorema envolvendo as condições suficiente e necessária, ou seja, se e somente se, é chamado de teorema de caracterização.
    Exemplo: Um paralelogramo é um retângulo se e somente se um dos seus ângulos é reto.

- Corolário—do Latim "corollarium": Um teorema que pode ser derivado de forma natural, imediata ou óbvia de um outro teorema onde a prova do teorema derivado é praticamente desnecessária.

Prova direta: Exemplo

Teorema: A soma de dois números racionais é um número racional.

Prova:

- Suponha que r e s sejam dois números racionais.
- ➜ Deve-se mostrar que $r + s$ é racional.
- Pela definição de racional, $r = a/b$ e $s = c/d$ para inteiros a, b, c e d com $b \neq 0$ e $d \neq 0$.
- Por substituição e álgebra temos que:

$$r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

- Se $p = ad + bc$ e $q = bd$ então p e q são inteiros porque o conjunto dos números inteiros é "fechado" para as operações de $+$ e $\times$ sendo que $q \neq 0$.
- Logo,

$$r + s = \frac{p}{q},$$

ou seja, a soma de $r + s$ é um número racional. [O que devia ser mostrado.]

Definições

- Sejam n e d inteiros e $d \neq 0$.
  - n é **divisível** por d sse $n = d \cdot k$ para algum inteiro k.

- Alternativamente, podemos dizer que:
  - n é **múltiplo** de d, ou
  - d é um **fator** de n, ou
  - d é um **divisor** de n, ou
  - d **divide** n.

- A notação $d|n$ deve ser lida como "d divide n". Simbolicamente, se n e d são inteiros e $d \neq 0$,

$$d|n \Leftrightarrow \exists \text{ um inteiro } k \text{ tal que } n = d \cdot k.$$

Prova direta: Transitividade da divisibilidade

Teorema: Para todos inteiros a, b e c, se a divide b e b divide c, então a divide c.

Prova:

- Suponha que a, b e c são inteiros [específicos mas escolhidos arbitrariamente] tais que a divide b e b divide c.

➜ Deve-se mostrar que a divide c.

- Pela definição de divisibilidade, $b = a \cdot r$ e $c = b \cdot s$ para inteiros r e s.
- Por substituição e álgebra temos que:

$$\begin{aligned} c &= b \cdot s \\ &= (a \cdot r) \cdot s \\ &= a \cdot (r \cdot s) \end{aligned}$$

- Seja $k = r \cdot s$, onde k é um número inteiro.
- Logo,

$$c = a \cdot k,$$

ou seja, a divide c pela definição de divisibilidade. [O que devia ser mostrado.]

Prova direta: Divisibilidade e números primos

Teorema: Todo inteiro $n > 1$ é divisível por um número primo.

Prova:

- Suponha que n é um inteiro [específico mas escolhido arbitrariamente] maior que 1.

➜ Deve-se mostrar que existe um número primo que divide n.

- Se n é primo então n é divisível por um número primo, ou seja, ele próprio e a prova chega ao fim. Se n não é primo então n é composto, e pela definição de número composto

  $n = r_0 \cdot s_0$, onde r_0 e s_0 são inteiros, e

  $1 < r_0 < n$ e $1 < s_0 < n$.

- Pela definição de divisibilidade, $r_0 | n$. Se r_0 é primo, então r_0 é um número primo que divide n e a prova chega ao fim. Se r_0 não é primo então r_0 é composto, e pela definição de número composto

  $r_0 = r_1 \cdot s_1$, onde r_1 e s_1 são inteiros, e

  $1 < r_1 < r_0$ e $1 < s_1 < r_0$.

Prova direta: Divisibilidade e números primos

- Pela definição de divisibilidade, $r_1|r_0$. Mas nós já sabemos que $r_0|n$ e pela transitividade da divisibilidade, $r_1|n$. Se r_1 é primo, então r_1 é um número primo que divide n e a prova chega ao fim. Se r_1 não é primo então podemos continuar o processo acima fatorando r_1 como $r_1 = r_2 \cdot s_2$.
- Pode-se continuar este processo, obtendo fatores sucessivos de n até se obter um fator primo. Este processo tem um número finito de passos já que cada novo fator é menor que o anterior (que é menor que n) e maior que 1, e existem menos que n inteiros entre 1 e n. Desta forma obtém-se a sequência:

$$r_0, r_1, r_2, \ldots, r_k,$$

onde $k \geq 0$, $1 < r_k < r_{k-1} < \ldots < r_1 < r_0 < n$ e $r_i|n$ para cada $i = 0, 1, 2, \ldots, k$. A condição para término é que r_k seja primo, ou seja, r_k é um número primo que divide n. [O que devia ser mostrado.]

Divisibilidade e contra-exemplos

- Prove ou "disprove" a seguinte afirmação:
  Para todos inteiros a e b, se $a|b$ e $b|a$ então $a = b$.

- Solução:
  - Suponha que a e b são inteiros [específicos mas escolhidos arbitrariamente] tais que $a|b$ e $b|a$.
  - Pela definição de divisibilidade, as condições $b|a$ e $a|b$ podem ser escritas como

    $$b = k \cdot a \text{ e } a = l \cdot b \text{ para inteiros } k \text{ e } l.$$

  - Por substituição e álgebra temos que:

    $$b = k \cdot a = k \cdot (l \cdot b) = (k \cdot l) \cdot b$$

    Já que $b|a$ e $b \neq 0$, tem-se que

    $$1 = k \cdot l$$

    Em outras palavras, k e l são divisores de 1. Mas os únicos divisores de 1 são 1 e -1. Logo, k e l são ambos 1 ou -1. Se $k = l = 1$ então $a = b = 1$. Mas se $k = l = -1$ então $b = -a$ e assim $a \neq b$.

Divisibilidade e contra-exemplos

- De onde se conclui que a afirmação acima é falsa.
- Comentário: em muitos casos a busca por uma prova ajuda a descobrir um contra-exemplo.
- Por outro lado, um contra-exemplo poderia ser apresentado diretamente. Seja $a = 2$ e $b = -2$. Sabe-se que $a|b$ e $b|a$, mas $a \neq b$. Se restringirmos o dominio ao conjunto dos naturais, então a proposição é verdadeira.

O teorema da fatorização única

Teorema: Dado qualquer inteiro $n > 1$, existem os seguintes números: um inteiro positivo k, números primos distintos $p_1, p_2, \ldots, p_k$ e inteiros positivos $e_1, e_2, \ldots, e_k$ tal que

$$n = p_1^{e_1} \cdot p_2^{e_2} \ldots p_k^{e_k}.$$

Prova: Além do escopo desta matéria

Este resultado é chamado de Teorema Fundamental da Aritmética. No livro "Os Elementos", escrito por Euclídes por volta do ano 300 a.C., possui essencialmente essa afirmação e prova desse resultado. Em 1796, Gauss demonstrou esse teorema usando aritmética modular.

O teorema do quociente–resto

Teorema: Dado qualquer inteiro n e inteiro positivo d, existem inteiros q e r tal que

$$n = d \cdot q + r$$

e $\quad 0 \leq r < d$

Nao veremos a prova deste teorema. Além disso, esta decomposição é única, i.e., não existem diferentes q's e r's, sendo $0 \leq r < d$ com esta propriedade.

Prove que esta fatoração é única. Sugestão: assuma que existam duas fatoracoes e mostre que elas sao idênticas.

O teorema do quociente–resto & Definições

Dado um inteiro não-negativo n e um inteiro positivo d, temos que:

- n div d: quociente inteiro obtido quando n é dividido, por d.
- n mod d: resto inteiro obtido quando n é dividido por d.

Prova direta geométrica: Uma soma

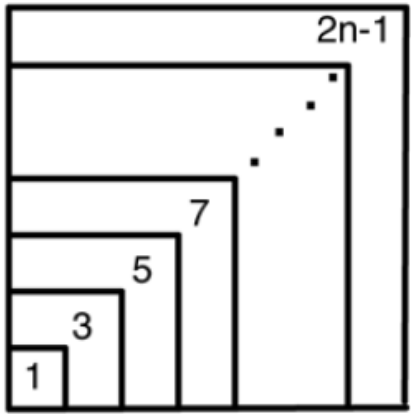
Diferentes técnicas geométricas podem ser usadas para provar fatos, fórmulas e relações.

Prove que

$$P(n) : 1 + 3 + 5 + \ldots + (2n - 1) = n^2$$

para todos inteiros $n \geq 1$.

Prova (geométrica):



Veja o quadrado de comprimento n como formado por vários polígonos: o quadrado de área 1 no canto esquerdo; o 3 em L como três quadrados de área 1; o 5 em L como cinco quadrados de área 1, e assim por diante. Ou seja, a soma de todos os quadrados unitários em cada polígono é dado por $1 + 3 + 5 + \ldots + (2n - 1)$ = a área do quadrado de lado de tamanho n.

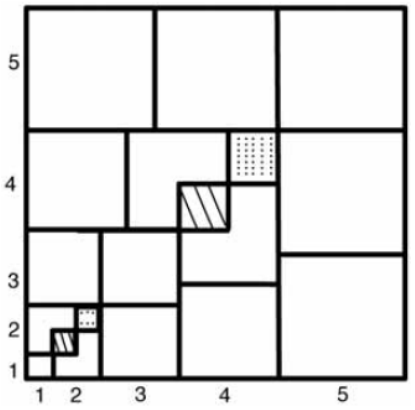
Prova direta geométrica: Duas somas

Prove que

$$P(n) : 1^3 + 2^3 + 3^3 + \ldots + n^3 = (1 + 2 + \ldots + n)^2$$

para todos inteiros $n \geq 1$.

Prova (geométrica):



Na figura, cada quadrado com lado cujo valor é um ímpar k tem area $k \times k$ e existem k deles, i.e., 1 de 1×1, 3 de 3×3, 5 de 5×5, ...

Cada quadrado de lado cujo valor é um par k tem área $k \times k$ e existem k deles. No entanto, há sempre uma parte hachurada comum a dois deles que pode ser rebatida na parte sombreada completando um dos quadrados sobrepostos.

Assim, temos que a area total é $1^3 + 2^3 + 3^3 + 4^3 + 5^3 + \ldots$. Mas a área total é um quadrado de lado igual a $1 + 2 + \ldots + n$.

Divisão em casos: Exemplo I

Teorema: Dois números inteiros consecutivos quaisquer têm paridade (par, ímpar) oposta.

Prova:

- Suponha que dois inteiros consecutivos [específicos mas escolhidos arbitrariamente] são dados. Chame esses números de m e $m + 1$.

➜ Deve-se mostrar que um dos números m e $m + 1$ par e o outro é ímpar.

- Pela definição de par e ímpar, tem-se que ou m é par ou m é ímpar.

➜ Vamos quebrar a prova em dois casos dependendo se m é par ou ímpar.

- Caso 1 (m é par): Neste caso, $m = 2k$ para algum inteiro k e, assim, $m+1 = 2k + 1$, o que é ímpar [Pela definição de ímpar.] Neste caso um dos números m e $m + 1$ é par e o outro é ímpar.
- Caso 2 (m é ímpar): Neste caso, $m = 2k + 1$ para algum inteiro k e, assim, $m+1 = (2k+1)+1 = 2k+2 = 2(k+1)$. Como $m+1$ é igual ao dobro de um número, então $m + 1$ é par. Também neste caso um dos números m e $m + 1$ é par e o outro é ímpar.
- Pode-se concluir que independente de qual caso ocorre para valores específicos de m e $m + 1$ que são escolhidos, um dos números m e $m + 1$ é par e outro é ímpar.

Divisão em casos: Exemplo II

Teorema: O quadrado de qualquer inteiro ímpar tem a forma $8m+1$ para algum inteiro m.

Prova:

– Suponha que n é um inteiro ímpar [específico mas escolhido arbitrariamente]. Pelo teorema do quociente–resto, n pode ser escrito em uma das seguintes formas:

$$4q \quad \text{ou} \quad 4q+1 \quad \text{ou} \quad 4q+2 \quad \text{ou} \quad 4q+3,$$

para algum inteiro q. Como n é ímpar e $4q$ e $4q+2$ são pares, n deve ter uma das duas formas: $4q+1$ ou $4q+3$.

Divisão em casos: Exemplo II

– Caso 1 ($n = 4q + 1$): [Deve-se achar um inteiro m tal que $n^2 = 8m + 1$.] Como $n = 4q + 1$,

$$\begin{aligned} n^2 &= (4q+1)^2 \\ &= 16q^2 + 8q + 1 \\ &= 8(2q^2 + q) + 1 \end{aligned}$$

– Caso 2 ($n = 4q + 3$): [Deve-se achar um inteiro m tal que $n^2 = 8m + 1$.] Como $n = 4q + 3$,

$$\begin{aligned} n^2 &= (4q+3)^2 \\ &= 16q^2 + 24q + 9 \\ &= 8(2q^2 + 3q + 1) + 1 \end{aligned}$$

Método de prova por contradição: Princípios

1. Suponha que a afirmação a ser provada é falsa.
2. Mostre que essa suposição leva logicamente a uma contradição.
3. Conclua que a afirmação a ser provada é verdadeira.

Método de prova por contradição

Teorema: Não existe um inteiro que seja o maior de todos.

Prova:

- Suponha que não. [Supomos que a negação do teorema seja verdadeira.]
- Suponha que exista um inteiro N que seja o maior de todos. [Deve-se deduzir uma contradição.]
- Tem-se então que $N \geq n$ para cada inteiro n. Seja $M = N + 1$, que é um inteiro já que é a soma de inteiros. Tem-se também que $M > N$ já que $M = N + 1$.
- Logo, M é um inteiro que é maior que o maior dos inteiros, o que é uma contradição. [Essa contradição mostra que a suposição é falsa e, desta forma, o teorema é verdadeiro.]

Método de prova por contraposição: Princípios

1. Expresse a afirmação a ser provada na forma

$$\forall x \in D, \text{ se } P(x) \text{ então } Q(x)$$

2. Reescreva a afirmação na forma contrapositiva:

$$\forall x \in D, \text{ se } \neg Q(x) \text{ então } \neg P(x)$$

3. Prove o contrapositivo por uma prova direta:
   (a) Suponha x um elemento específico mas escolhido arbitrariamente de D tal que $\neg Q(x)$ seja V.
   (b) Mostre que $\neg P(x)$ é F.

Método de prova por contraposição

Teorema: Dado qualquer inteiro n, se n^2 é par então n é par.

Prova (pelo contrapositivo):

– Seja n um inteiro que não é par (i.e., é ímpar).

➜ Deve-se mostrar que n^2 não é par (i.e., é ímpar).

– Sabe-se que o produto de dois números ímpares é um número que é ímpar. Desta forma, $n^2 = n \cdot n$ que é ímpar. [O que devia ser mostrado.]

Relação entre prova por contradição e prova por contraposição

- Na prova por contraposição a afirmação

$$\forall x \in D, \text{ se } P(x) \text{ então } Q(x)$$

é provada apresentando uma prova direta da afirmação equivalente

$$\forall x \in D, \text{ se } \neg Q(x) \text{ então } \neg P(x)$$

- Este tipo de prova segue os seguintes passos:
  (a) Suponha que x é um elemento arbitrário de D tal que $\neg Q(x)$.
  (b) Através do raciocínio dedutivo isto leva a
  (c) $\neg P(x)$.

- A prova por contradição é baseada nos seguintes passos:
  (a) Suponha que existe um elemento $x \in D$ tal que $P(x) \wedge \neg Q(x)$.
  (b) Usando o mesmo raciocínio dedutivo isto leva a
  (c) Contradição: $P(x) \wedge \neg P(x)$.

Relação entre prova por contradição e prova por contraposição: Exemplo

Teorema: Para todo n, se n^2 é par então n é par.

Prova (por contradição):

- Suponha que não.
- Suponha que exista um inteiro n tal que n^2 é par e n é ímpar. [Deve-se chegar a uma contradição.]
- Já que n é ímpar, n^2 que é o produto $n \cdot n$ é também ímpar.
- Isto contradiz a suposição que n^2 é par. [Logo, as proposições $P(n) = n^2$ é par e $\neg P(n) = n^2$ é ímpar são verdadeiras ao mesmo tempo, o que é uma contradição.]

Relação entre prova por contradição e prova por contraposição

- Prova por contraposição:
  - + É fácil saber que conclusão deve ser provada: negação da hipótese.
  - + Não é necessário obter a negação da afirmação.
  - − Só pode ser usado para afirmações com quantificadores existencial ou universal.
- Prova por contradição:
  - + A prova termina assim que é achada uma contradição.
  - − A negação da afirmação é mais complexa.
  - − Pode ser mais difícil achar o caminho da prova.