11 Teoremas

Sumário da Aula

11.1 Introdução

Demonstração é um argumento válido que estabelece a veracidade de uma sentença. Em outras palavras, é um instrumento usado para convencer alguém de que uma determinada afirmação é verdadeira.

As técnicas de demonstração são fundamentais na matemática e na ciência da computação e podem ser aplicadas, por exemplo, para verificar se programas de computadores estão corretos, estabelecer se os sistemas de operações são seguros e fazer inferência em inteligência artificial. Uma correpondência entre teorema e algoritmo, verifica-se quando um teorema pode ser usado para verificar se uma implementação está correta ao analisar se a implementação realmente funciona [4, 6].

As regras de dedução natural das lógicas proposicional e de predicados também são aplicadas na

demonstração de teoremas matemáticos, onde cada passo da prova deve ser justificado pela regra de inferência usada. Uma **prova** é uma sequência de passos usadas para verificar que um teorema é verdadeiro, ou seja, é uma argumentação que mostra, de maneira indiscutível, que uma afirmação é verdadeira.

Nas próximas seções serão apresentadas um conjunto de técnicas usadas para a demonstração de teoremas em um contexto matemático, onde os principais passos e o raciocínio usado podem ser esboçados usando uma linguagem do dia-a-dia e menos formal que o procedimento usado nas lógicas de proposiçAo e de predicados. As demonstrações serão feitas usando as hipóteses do teorema; definições e propriedades conhecidas; axiomas assumidos com verdadeiros; teoremas já provados anteriormente e todas as regras de inferência estudadas na lógica formal.

11.2 Teorema

Uma afirmação matemática, que acredita-se ser verdadeira, é chamada de:

- **teorema**, quando for possível provar sua veracidade;
- **conjectura**, quando a veracidade não é garantida; e
- **erro**, quando se trata de uma afirmação falsa.

Um teorema é uma declaração matemática para qual existe uma prova, ou ainda, uma sentença matemática que pode ser demonstrada por meio de operações e argumentos matemáticos. O termo teorema foi introduzido por Euclides de Alexandria (c.325 a.C. - c.265 a.C) no livro "Os Elementos" para especificar uma afirmação que pode ser provada.

Como alguns teoremas são mais importantes que outros, existem designações alternativas para serem usadas no lugar da palavra teorema, sendo que cada uma delas deve ser empregada com uma contação diferente. "A palavra teorema tem uma conatação de importância e generalidade"[8]. Por exemplo, são teoremas as afirmações "**o quadrado da hipotenusa é igual à soma dos quadrados dos catetos**"; "**o quadrado de todo número inteiro par também é par**" e "**2+2=4**". Mas, apenas a primeira afirmação, devido a sua importância, merece ser chamada de teorema (Teorema de Pitágoras).

Observação

É importante não confundir os significados das palavras TEOREMA e TEORIA. Um teorema é uma afirmação específica que pode ser demonstrada, enquanto teoria envolve um conjunto mais amplo de ideias sobre um tema em particular.

Considere algumas palavras alternativas para ser usadas no lugar da palavra teorema e a orientação quanto ao uso:

Resultado: é uma expressão modesta e genérica para um teorema.

Fato: um teorema de importância bastante limitada, como por exemplo "2+2=4".

Proposição: um teorema de importância secundária. É mais importante que um fato, mas não possui tanto prestígio quanto um teorema.

Axioma: também chamado de **postulado**, é uma sentença assumida verdadeira. O axioma é usado como base para a demonstração de outros teoremas.

Lema: é um teorema usado para ajudar a provar outro teorema mais importante. O lema é uma afirmação que deve ser provada e que normalmente é usada como parte, ou instrumento, durante a demonstração mais complicada de um teorema.

Corolário: é consequência direta de um teorema, cuja demonstração é relativamente simples.

Chama-se de **Conjectura**, uma sentença proposta, inicialmente como verdadeira, mas que ainda não foi provada. É considerada previamente verdadeira baseada em alguma evidência parcial, argumento heurístico ou intuição de um perito. Para mostrar a veracidade de uma conjectura é necessário construir uma prova e, quando demonstrada, se transforma em um **teorema**.

Exemplo 11.1. Conjecturas famosas que foram demonstradas recentemente:

- **Último Teorema de Fermat:** proposta pelo matemático Pierre de Fermat (1601-1665). Esta conjectura diz que "se $n > 2$, a equação $x^n + y^n = z^n$ não tem soluções inteiras positivas." Foi provada em 1995 pelo matemático inglês Andrew Wiles.
- **Teorema das quatros cores:** enunciada em 1852 por Francis Guthrie (1831-1899). Diz que "todo mapa pode ser pintado com no máximo quatro cores, de modo que países vizinhos tenham cores distintas." Esta conjectura foi provada em 1976 por Kenneth Appel e Wolfgang Haken utilizando um computador.

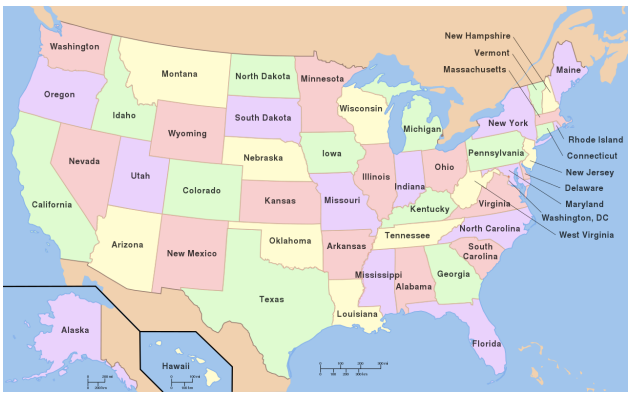

Figura 11.1: Mapa dos Estados Unidos colorido utilizando quatro cores. Veja que até em estados que fazem fronteira com mais de três estados, como por exemplo o Corolado, as cores não coindem. Imagem: File:Map of USA with state names.svg

A prova da falsidade de uma conjectura é dada por meio da apresentação de um **contraexemplo**. Um único contraexemplo é suficiente para provar que a conjectura é falsa! Mas é preciso ter cuidado nesta busca, pois, o fato de não encontrar um contraexemplo não significa que a conjectura seja verdadeira.

Exemplo 11.2. Conjecturas falsas:

- Todos os animais que vivem no oceano são peixes.
  Contraexemplo: baleia.

- Todo número primo menor do que 10 é maior do que 5.
  Contraexemplo: número 2.

Diante de uma conjectura, não é trivial decidir pela demonstração ou pela procura de um contraexemplo. Uma conjectura em aberto é aquela que ainda não foi provada ou verificada falsa.

Exemplo 11.3. Conjecturas em aberto:

- **CONJECTURA DE GOLDBACH:** proposta em 1742 pelo matemático alemão Christian Goldbach (1690 - 1764) que diz "todo número par maior que 2 pode ser representado pela soma de dois números primos." Esta conjectura foi verificada, em 2010, por um programa de computador para números até 2.10^{18}, mas isso não implica que a conjectura seja verdadeira. Como até hoje não foi apresentada uma prova ou um contraexemplo, ainda não se sabe se a Conjectura de Goldbach é verdadeira ou falsa.

- **CONJECTURA DE BEAL:** é uma generalização do último teorema de Fermat. Foi proposta em 1993 pelo empresário Andrew Beal e diz o seguinte: "se $A^x + B^y = C^z$, onde A, B, C, x, y, z são inteiros positivos com $x, y, z > 2$, então A, B, C possui um fator primo em comum". Para esta demonstração é oferecido o Premio Beal no valor de $\$1.000.000,00$.

Nas aulas seguintes será apresentado um conjunto de técnicas usadas pra determinar a verdade ou falsidade de afirmações matemáticas. Para tanto, devem ser consideradas algumas afirmações que envolvem propriedades e definições dos números inteiros (Teoria dos Números), números racionais e os números reais.

Definição é um enunciado que descreve o significado de um termo. A definição precisa especificar todas as propriedades que identificam o conceito de cada termo do enunciado. Uma vez bem definido este conceito, o mesmo poderá ser aplicado em outras definições e nas provas de teoremas. Considere algumas definições importantes que serão usadas durante todo o tópico de técnicas de demonstração.

Definições Úteis

Número par: Seja $n \in \mathbb{Z}$. n é **par**, se existe um $k \in \mathbb{Z}$ tal que $n = 2k$.

Número ímpar: Seja $n \in \mathbb{Z}$. n é **ímpar**, se existe um $k \in \mathbb{Z}$ tal que $n = 2k + 1$.

Número Primo: n é um número primo se, e somente se, $\forall k, s \in \mathbb{Z}^+$, se $n = ks$, então $k = 1$ e $s = n$ ou $k = n$ e $s = 1$.

Número Composto: n é um número composto, se e somente se, $\exists k, s \in \mathbb{Z}^+$ tais que $n = ks$ e $1 < k < n$ e $1 < s < n$, ou seja, $k \neq 1$ e $s \neq 1$.

Quadrado Perfeito: Um número n é um **quadrado perfeito**, se existe $k \in \mathbb{Z}$ tal que $n = k^2$.

Cubo Perfeito: Um número n é um **cubo perfeito**, se existe $k \in \mathbb{Z}$ tal que $n = k^3$.

Número Racional: Seja $r \in \mathbb{R}$. r é **racional** se existem $p, q \in \mathbb{Z}$ tais que $r = p/q$ e $q \neq 0$. Caso contrário, dizemos que r é irracional.

Mínimo Múltiplo Comum: O **Mínimo Múltiplo Comum** de dois inteiros a e b, denotado como $mmc(a, b)$, é o menor inteiro que é múltiplo tanto de a quanto de b.

Máximo Divisor Comum: O **Máximo Divisor Comum** de dois inteiros a e b, denotado como $mdc(a, b)$, é o maior inteiro que divide tanto a quanto b.
Observações:
1. $mdc(a, 0) = mdc(0, a) = |a|$ se $a \neq 0$;
2. $mdc(0, 0) = \infty$.

Módulo: O **Valor Absoluto** ou **Módulo** de um número x, denotado por $|x|$, é igual a :

$$|x| = \begin{cases} x, & \text{se } x \geq 0 \\ -x, & \text{se } x < 0 \end{cases}$$

Números Negativos: Os símbolos $<, >, \leq$ e $\geq$ e os números reais negativos são definidos em termos dos números reais positivos. Dados $a, b \in \mathbb{R}$:

- $a < b$ significa que $b + (-a)$ é positivo;
- $a \leq b$ significa que $a < b$ ou $a = b$;
- Se $a < 0$, dizemos que a é um número negativo;
- Se $a \geq 0$, dizemos que a é um número não-negativo.

Os **axiomas** são usados como base para a demonstração de outros teoremas. Considere os axiomas[1] seguintes decorrentes da definição dos números reais e da inclusão das operações binárias da "adição" e " multiplicação" entre os elementos destes conjuntos. Dados $a, b, c \in \mathbb{R}$:

- **O conjunto dos números reais é fechado em relação as operações da adição e multiplicação**:

  I. o resultado da soma dos elementos a e b, denotado por $a + b$, é um número real.

[1]Retirados e adaptados de Epp, S. S. (2011). *Discrete mathematics with applications*. Boston, MA: Cengage Learning, pp A-1 - A-3.

II. o resultado do produto dos elementos a e b, denotado por $a \cdot b$ ou ab, também é um número real.

- **Valem as propriedades de igualdade**:

I. $a = a$;

II. se $a = b$, então $b = a$; e

III. se $a = b$ e $b = c$, então $a = c$.

- **A maioria dos quocientes de números inteiros não são inteiros**. Por exemplo, $5 \div 3$ é igual a $5/3$ e não é um número inteiro, já $3 \div 0$ não é nem mesmo um número.

- **Não existe um número inteiro entre 0 e 1.**

Os axiomas dos números reais estão divididos em três grupos: axiomas de corpo, de ordem e do supremo. A seguir são apresentados os axiomas dos dois primeiros grupos.

Axiomas Úteis

Axiomas de Corpo: Sejam $a, b, c \in \mathbb{R}$, são válidas as seguintes propriedades:

A1. **(Comutatividade):** $a + b = b + a$ e $ab = ba$.

A2. **(Associatividade):** $(a + b) + c = a + (b + c)$ e $(ab)c = a(bc)$.

A3. **(Distributividade):** $a(b + c) = ab + ac$ e $(b + c)a = ba + ca$

A4. **(Elemento Neutro):** Existe um único elemento neutro para a adição e para a multiplicação, de forma que: $a + 0 = a$ e $a.1 = a$.

A5. **(Elemento Simétrico):** Existe um único elemento inverso para a adição e para a multiplicação, de forma que: $a + (-a) = (-a) + a = 0$ e $a.\left(\frac{1}{a}\right) = \left(\frac{1}{a}\right).a = 1$

Axiomas de Ordem: Considere $\mathbb{R}^+$ um subconjunto de $\mathbb{R}$ cujos elementos são os números reais positivos. Sejam $a, b \in \mathbb{R}^+$, são válidas as seguintes propriedades:

A6. Para quaisquer números reais a e b, se a e b são positivos, então $a + b$ e ab também são.

A7. Para todo número real $a \neq 0$, ou a é positivo ou $-a$ é positivo, mas não ambos. Em outras palavras, qualquer número real diferente de zero é real positivo ou real negativo e nenhum número real e positivo e negativo ao mesmo tempo.

A8. O número 0 não é positivo.

A grande maioria das sentenças matemáticas a serem provadas aparecem na forma de declarações **universais** ou **existenciais**.

11.2.1 Declarações Universais

Os teoremas no formato de declarações universais são representados formalmente por:

$$\forall x[P(x) \rightarrow Q(x)]$$

e discorrem que todos os objetos do universo de discurso que possuem a propriedade $P(x)$ também possuem a propriedade $Q(x)$. Algumas considerações:

- a sentença informal $P(x) \rightarrow Q(x)$ só é falsa quando $P(x)$ é verdadeira e $Q(x)$ é falsa.
- para mostrar que $P(x) \rightarrow Q(x)$ é verdadeira, basta supor que $P(x)$ é verdadeira e mostrar que $Q(x)$ também é.
- para provar $\forall x[P(x) \rightarrow Q(x)]$ é necessário supor que x é um elemento específico do universo do discurso, porém escolhido arbitrariamente, que satisfaz $P(x)$ e provar que x também satisfaz $Q(x)$.
- a sentença $P(x)$ é chamada de **hipótese ou premissa** e a sentença $Q(x)$ de **tese ou conclusão**.

Particularidades na demonstração de sentenças com quantificadores universais:

- Uma vez comprovado que a sentença do tipo $\forall x[P(x)]$ é verdadeira, pode-se afirmar que $P(a)$ é verdadeira para qualquer elemento a do universo de discurso.
- Se o universo do discurso for um conjunto vazio **($\mathbb{D} = \emptyset$)** a afirmação do tipo $\forall x \in \mathbb{D}[P(x)]$ é verdadeira, para qualquer predicado $P(x)$. Neste caso, diz-se que a afirmação é verdadeira por **VACUIDADE**.
- Se a afirmação $\forall x[P(x) \rightarrow Q(x)]$ for falsa, para demonstrar este fato, bastar provar que sua negação é verdadeira, ou seja, provar a seguinte sentença: $\exists x[P(x) \wedge \neg Q(x)]$.
  Assim, para refutar uma afirmação do tipo $\forall x[P(x) \rightarrow Q(x)]$ basta encontrar um valor de x para o qual $P(x)$ é verdadeiro e $Q(x)$ é falso. E, de forma análoga, para negar uma sentença do tipo $\forall x[P(x)]$, basta encontrar um valor para x para o qual $P(x)$ é falsa. O elemento x é chamado de **CONTRAEXEMPLO**.

Exemplo 11.4. Prove que todos os pares primos maiores que dois são quadrados perfeitos.
Prova: A afirmação é verdadeira por vacuidade. Como não existem números primos pares maiores que dois, não é possível encontrar um contraexemplo para refutar a afirmação. ■

Exemplo 11.5. Prove a sentença "**Todo inteiro positivo é a soma dos quadrados de dois inteiros**".
A sentença é falsa!
Para contestar a sentença é preciso apresentar um contraexemplo, ou seja, encontrar um número inteiro positivo que não é a soma dos quadrados de dois números inteiros.
Considere, por exemplo, o número 3. Os quadrados dos números inteiros positivos que não excedem 3 são $0^2 = 0$ e $1^2 = 1$. Veja que é impossível obter 3 a partir da soma desses dois quadrados usando apenas dois termos.
Portanto, dado o contraexemplo $x = 3$, verifica-se que a sentença é falsa.

Observação

Uma dica para procurar um contraexemplo é tentar provar a afirmação e, no momento que encontrar alguma dificuldade, determinar qual o problema que impede a continuação da demonstração. A partir desta dificuldade construa o contraexemplo.

Exemplo 11.6. Prove que $\forall a, b \in \mathbb{R}$, se $a^2 = b^2$, então $a = b$.
A sentença pode ser reescrita simbolicamente por $\forall a, b \in \mathbb{R}[(a^2 = b^2) \rightarrow (a = b)]$**.**
A sentença é falsa, considere como contraexemplo $a = 1$ **e** $b = -1$**.**

11.2.2 Declarações Existenciais

As sentenças matemáticas que são representadas formalmente por:

$$\exists x[Q(x)]$$

são verdadeiras se, e somente se, $Q(x)$ é verdadeiro para pelo menos um x pertencente ao universo do discurso D. Para demonstrar a veracidade dos teoremas que aparecem neste formato basta apresentar uma:

Prova Construtiva: encontrar um valor para $a \in D$ tal que $Q(a)$ seja verdadeira.

Prova não Construtiva: mostrar que a afirmativa $\exists x[Q(x)]$ pode ser provada de outra maneira, mesmo sem exibir explicitamente um valor a tal que $Q(a)$ seja verdadeira. **Esta estratégia será melhor detalhada nos próximos capítulos.**

Para mostrar que uma declaração existencial é falsa, basta provar que sua negação (uma afirmação universal) é verdadeira.

Exemplo 11.7. Mostre que existem três números inteiros positivos, tais que $x^2 + y^2 = z^2$.
Prova Construtiva: Sejam $x = 3$**,** $y = 4$ **e** $z = 5$**. Assim:**

$$x^2 + y^2 = (3)^2 + (4)^2 = 25 = (5)^2 = z^2.$$

Logo, é possível concluir que a afirmação é verdadeira. ■

Exemplo 11.8. Mostre que existe um inteiro positivo que pode ser escrito como a soma de dois cubos de duas maneiras diferentes.
Prova Construtiva: Após uma exaustiva busca (neste caso, computacionalmente) é possível obter um exemplo que comprove que a sentença verdadeira. Seja:

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$

Logo, dado o exemplo acima concluí-se que existe um inteiro positivo que pode ser escrito como a soma de cubos de dois modos diferentes. ■

11.3 Exercícios

E. 1. Use as definições e axiomas apresentados para responder as seguintes perguntas:

1. 0 é par?
2. -51 é ímpar?
3. Seja k um número inteiro, $2k - 1$ é ímpar?
4. Se a e b são inteiros, $2a + 4b$ é par?
5. Se a e b são inteiros, $2a + 4b + 3$ é ímpar?
6. Se a e b são inteiros, $10ab + 7$ é ímpar?
7. Se a e b são inteiros, $6a + 4b^2 + 3$ é par?
8. 1 é primo?
9. A propriedade $(a + b)^2 = a^2 + b^2$ é verdadeira para todos os inteiros.
10. A propriedade $-a^n = (-a)^n$ é verdadeira para alguns números inteiros.
11. $5/3$ é um número racional?
12. 0 é um número racional?
13. $1,75$ é um número racional?

E. 2. Prove que se um inteiro é simultaneamente um quadrado perfeito e primo, então ele é negativo.

E. 3. Apresente contraexemplos para as proposições.

1. Toda figura geométrica com quatros ângulos retos é um quadrado.
2. Se um número real não for positivo, terá que ser negativo.
3. Todas as pessoas com cabelo ruivo têm olhos verdes ou são altas.
4. Se $n^2 > 0$ então $n > 0$
5. Se n for um número par, então $n^2 + 1$ será um número primo.
6. Se n for um número positivo, então $n^3 > n!$.
7. A diferença entre dois números ímpares é ímpar.
8. O Produto de um número inteiro e o seu quadrado é par.
9. Se o inteiro x é primo, então x é ímpar.

10. Não existe par de inteiros a e b tais que $mod(a, b) = mod(b, a)$.
    OBS: A função $mod(num, divisor)$ calcula o resto da divisão de um número.

E. 4. Prove que existe um numero real x tal que $x^2 < \sqrt{x}$.

E. 5. Prove que existe um número primo entre 90 e 100.

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.