Universidade Federal de Ouro Preto
Departamento de Computação
Matemática Discreta I- BCC101

Notas de Aula: Técnicas de Demonstração de Teoremas

Prof[a]. Dayanne G. Coelho

Ouro Preto - MG
2017

.

Prefácio

Esta apostila consiste em notas de aulas da disciplina Matemática Discreta I para o curso de Ciência da Computação da Universidade Federal de Ouro Preto. Todo o material, bem como o conjunto de exercícios, foram baseados nas seguintes fontes bibliográficas:

1. Book of Proof, Hammack [1].
2. Fundamentos Matemáticos para a Ciência da Computação: Matemática Discreta e suas Aplicações, Gersting [2].
3. Notas de aulas do professor prof. Dr. Rodrigo Geraldo Ribeiro, DECOM- UFOP [3].
4. Matemática Discreta para a Computação e Informática, Menezes [4].
5. Fundamentos da Matemática Discreta, Hunter [5].
6. Discrete Mathematics With Applications, Epp [6].

Ouro Preto, 2018

Dayanne Coelho

Aula 14: Teoremas

BCC101- Matemática Discreta I

DECOM/UFOP

1.1 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 computador estão corretos, estabelecer se os sistemas de operações são seguros e fazer inferência em inteligência artificial. Fazendo uma analogia entre teorema e algoritmo, temos que um teorema pode ser usado para verificar se uma implementação está correta ao analisar se a implementação realmente funciona [2, 3].

As regras de dedução natural das lógicas proposicional e de predicados podem ser usadas para demonstrar teoremas matemáticos, onde cada passo da prova deve ser justificando por uma regra de inferência. Nas próximas seções vamos estudar um conjunto de técnicas 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. As demonstrações serão feitas usando as hipóteses do teorema; axiomas assumidos com verdadeiros; teoremas já provados e todas as regras de inferência estudadas na lógica formal.

Considere as seguintes terminologias:

Axiomas: também chamados de **postulados**, são sentenças assumidas verdadeiras, ou seja, são as premissas do teorema e teoremas previamente provados. Os axiomas são usados como base para a demonstração de teoremas. Veja mais detalhes na seção 1.1.2.

Conjecturas: são sentenças propostas, inicialmente, como verdadeiras, mas que ainda não foram provadas. Quando uma conjectura é demonstrada ela se torna uma teorema. Veja mais detalhes na seção 1.1.1.

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

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 pode ser aplicado em outras definições. Veja mais detalhes na seção 1.1.2.

Demonstração: ou **prova** é uma sequência de passos para verificar que o teorema é verdadeiro, ou seja, é uma argumentação que mostra, de maneira indiscutível, que uma afirmação é verdadeira.

Lemas: são teoremas cujo principal objetivo é ajudar a provar outro teorema mais importante. Os lemas são as partes, ou instrumentos, usados para elaborar uma demonstração mais complicada.

Proposições: são sentenças que podem ser demonstradas e possui demonstração simples. É um teorema de importância secundária.

Teorema: é 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.

Neste capítulo estudaremos um conjunto de técnicas pra determinar a verdade ou falsidade de uma afirmação matemática. Para tanto, vamos considerar afirmações que envolvem as propriedades dos números inteiros (teoria dos números), números racionais (frações inteiras) e os números reais. A nível de curiosidade, a seção 1.1.2 apresenta um conjunto de definições e axiomas que será usado para a demonstração dos exemplos apresentados neste material.

1.1.1 Conjecturas

Conjecturas são afirmações para as quais ainda não existem provas. Porem são consideradas previamente verdadeiras baseadas 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, ela se transforma em um teorema.

Exemplo 1.1 Conjecturas famosas demonstradas recentemente:

- **CONJECTURA 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.” Esta conjectura hoje é conhecida como **o último teorema de Fermat** e foi provada em 1995 pelo matemático inglês Andrew Wiles.

- **Conjectura 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.

A prova da falsidade de uma conjectura é dada apresentando um **contraexemplo**. Um único contra-exemplo 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 1.2 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 se devemos prová-la ou procurar um contraexemplo. Enquanto a conjectura não for provada ou verificada falsa, dizemos que ela está aberta.

Exemplo 1.3 Conjecturas abertas:

- **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 sabemos 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 $\$1.000.000,00$.

1.1.2 Propriedades

Nesta seção são apresentadas algumas definições e axiomas relacionados aos conjuntos dos números inteiros e reais.

Definições

(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.

Axiomas

A seguir são apresentados alguns axiomas [1] decorrentes da definição dos números reais e da inclusão das operações binárias da "adição" e " multiplicação" entre os elementos desses conjuntos. Dados $a, b, c \in \mathbb{R}$:

- o conjunto dos números reais é fechado em relação as operações da adição e multiplicação:
  1. o resultado da soma dos elementos a e b, denotado por $a + b$, é um número real.
  2. 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:
  1. $a = a$;
  2. se $a = b$, então $b = a$; e
  3. 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 $5/3$

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

e não é um número inteiro e $3 \div 0$ 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 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.

1.1.3 Exercícios

1. Use as Definições e os Axiomas para responder as perguntas.
   (a) 0 é par?
   (b) -51 é ímpar?
   (c) Seja k um número inteiro, $2k-1$ é ímpar?
   (d) Se a e b são inteiros, $2a+4b$ é par?
   (e) Se a e b são inteiros, $2a+4b+3$ é ímpar?
   (f) Se a e b são inteiros, $10ab+7$ é ímpar?
   (g) Se a e b são inteiros, $6a+4b^2+3$ é par?
   (h) 1 é primo?
   (i) A propriedade $(a+b)^2=a^2+b^2$ é verdadeira para todos os inteiros.
   (j) A propriedade $-a^n=(-a)^n$ é verdadeira para alguns números inteiros.
   (k) $5/3$ é um número racional?
   (l) 0 é um número racional?
   (m) $1,75$ é um número racional?

1.2 Teoremas

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

1.2.1 Declarações Universais

Os teoremas no formato de declarações universais são representados formalmente por

$$\forall x, [P(x) \to Q(x)]$$

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

OBSERVAÇÕES:

- a sentença informal $P(x) \to Q(x)$ só é falsa quando $P(x)$ é verdadeira e $Q(x)$ é falsa.
- para mostrar que $P(x) \to Q(x)$ é verdadeira, basta supor que $P(x)$ é verdadeira e mostrar que $Q(x)$ também é.
- para provar $\forall x, P(x) \to Q(x)$ 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 $Q(x)$.
- chamamos a sentença $P(x)$ 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, podemos 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, dizemos que a afirmação é verdadeira **por vacuidade**.

Exemplo 1.4 Prove que todos os pares primos maiores que dois são quadrados perfeitos.

Prova: A afirmação é verdadeira por vacuidade. Veja que não existem números primos pares maiores que dois. ■

- Se a afirmação $\forall x, P(x) \to Q(x)$ for falsa, para demonstrar este fato, bastar provar que sua negação é verdadeira, ou seja, provar a sentença equivalente $\exists x, P(x) \land \neg Q(x)$.

> Para refutar uma afirmação do tipo $\forall x, P(x) \to Q(x)$ basta encontrar um valor de x para o qual $P(x)$ é verdadeiro e $Q(x)$ é falso. 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**.

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 1.5 Prove a sentença "**Todo inteiro positivo é a soma dos quadrados de dois inteiros**".
A sentença é falsa!
Para contestar a sentença precisamos apresentar um contraexemplo: procuramos por 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 $1^2 = 1$. Dessa forma, temos que é impossível obter 3 da soma desses dois quadrados usando apenas dois termos.
Portanto, para o contraexemplo $x = 3$, verifica-se que a sentença é falsa.

Exemplo 1.6 Prove que $\forall a, b \in \mathbb{R}$ se $a^2 = b^2$ então $a = b$.
A sentença, pode ser escrita como $\forall a, b \in \mathbb{R}, (a^2 = b^2) \rightarrow (a = b)$, é falsa. Considere como contraexemplo $a = 1$ e $b = -1$.

1.2.2 Declarações Existenciais

As sentenças matemáticas 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 provar a veracidade dos teoremas que aparecem escritos como $\exists x, P(x)$ basta:
  Prova Construtiva: encontrar um valor para $a \in D$ tal que $P(a)$ seja verdadeira.
  Prova Não Construtiva: mostrar que a afirmativa $\exists x, P(x)$ pode ser provada de outra maneira, mesmo sem exibir explicitamente um valor a tal que $P(a)$ 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 1.7 Mostre que existem três números inteiros positivos, tais que $x^2 + y^2 = z^2$.

Prova: (**Prova Construtiva**) Sejam $x = 3$, $y = 4$ e $z = 5$. Temos que

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

Logo, podemos concluir que a afirmação é verdadeira. ■

Exemplo 1.8 Mostre que existe um inteiro positivo que pode ser escrito como a soma de dois cubos de duas maneiras diferentes.

Prova: (Prova Construtiva) Após uma exaustiva busca (neste caso, computacionalmente) é possível obter um exemplo que torne a sentença verdadeira. Seja:

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

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

1.2.3 Exercícios

1. Prove que se um inteiro é simultaneamente um quadrado perfeito e primo, então ele é negativo.
2. Apresente contraexemplos para as proposições.
   (a) Toda figura geométrica com quatros ângulos retos é um quadrado.
   (b) Se um número real não for positivo, terá que ser negativo.
   (c) Todas as pessoas com cabelo ruivo têm olhos verdes ou são altas.
   (d) Se $n^2 > 0$ então $n > 0$
   (e) Se n for um número par, então $n^2 + 1$ será um número primo.
   (f) Se n for um número positivo, então $n^3 > n!$.
   (g) A diferença entre dois números ímpares é ímpar.
   (h) O Produto de um número inteiro e o seu quadrado é par.
   (i) Se o inteiro x é primo, então x é ímpar.
   (j) 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.
3. Prove que existe um numero real x tal que $x^2 < \sqrt{x}$.
4. Prove que existe um número primo entre 90 e 100.

Aula 15: Técnicas de Prova: Prova por Exaustão e Prova Direta

BCC101- Matemática Discreta I

DECOM/UFOP

2.1 Prova por Exaustão

A prova por exaustão é um tipo especial de demonstração que verifica a validade do teorema para cada elemento do universo do discurso quando este representa uma coleção finita. Em outras palavras verifica-se o teorema para todos casos possíveis.

Exemplo 2.1 Prove que se n é um inteiro positivos com $n \leq 4$, então $(n+1)^3 \geq 3^n$.

Prova: Precisamos verificar que a inequação $(n+1)^3 \geq 3^n$ é verdadeira quando $n = 1,\ 2,\ 3$ e 4.

Como existe uma quantidade finita de casos, a conjectura pode ser verificada mostrando que ela é verdadeira para todos os casos possíveis. Seja:

n	$(n+1)^3$	3^n	$(n+1)^3 \geq 3^n$
1	$(1+1)^3 = 8$	$3^1 = 3$	**T**
2	$(2+1)^3 = 27$	$3^2 = 9$	**T**
3	$(3+1)^3 = 64$	$3^3 = 27$	**T**
4	$(4+1)^3 = 125$	$3^4 = 81$	**T**

Usando o método de demonstração por exaustão, verifica-se para as quatro possibilidades, que a inequação $(n+1)^3 \geq 3^n$ é verdadeira.

Portanto, temos que se n é um número inteiro positivo e $n \leq 4$, então é válida a inequação $(n+1)^3 \geq 3^n$. ■

Exemplo 2.2 Prove a conjectura: "**Se um número inteiro entre 1 e 20 for divisível por 6, então ele também é divisível por 3**".

Prova: Sabe-se que um número é divisível por 6 somente se ele é um múltiplo de 6.

Para provar que o número é divisível por 3, precisamos provar que ele também é múltiplo de 3.

Como existe uma quantidade finita de casos, esta conjectura pode ser verificada mostrando que ela é verdadeira para todos esses casos (números inteiros entre 1 e 20):

Número	**Divisível por 6**	**Divisível por 3**
1	não	
2	não	
3	não	
4	não	
5	não	
6	sim: $6 = 1 \times 6$	sim: $6 = 2 \times 3$
7	não	
8	não	
9	não	
10	não	

Número	**Divisível por 6**	**Divisível por 3**
11	não	
12	sim: $12 = 2 \times 6$	sim: $12 = 4 \times 3$
13	não	
14	não	
15	não	
16	não	
17	não	
18	sim: $18 = 3 \times 6$	sim: $18 = 6 \times 3$
19	não	
20	não	

Como verificado pelo método de demonstração por exaustão, temos que se um inteiro entre 1 e 20 for divisível por 6, então ele também é divisível por 3. ■

2.1.1 Exercícios

1. Prove cada uma das proposições seguintes:
   (a) Se $n = 25, 100$ ou 169, então n é um quadrado perfeito e é a soma de dois quadrados perfeitos.
   (b) Se n for um inteiro par tal que $4 \leq n \leq 12$, então n será uma soma de dois números primos.
   (c) Para qualquer inteiro positivo n menor ou igual a 3, temos que $n! < 2^n$.
   (d) Para $2 \leq n \leq 4$, temos que $n^2 \leq 2^n$.

2.2 Prova Direta

Chamamos de **prova direta** uma demonstração que pressupõe verdadeira a hipótese e, a partir desta, prova-se ser verdadeira a tese.

A prova direta segue o mesmo raciocínio das demonstrações realizadas na lógica proposicional: supor a veracidade das hipóteses e através de uma sequência de passos (axiomas, definições, teoremas já demonstrados e regras de inferência) deduzir a conclusão. Os passos e a escrita da prova direta consistem em:

1. Escrever o teorema que deve ser provado.
2. Expressar o teorema como uma fórmula da lógica de predicados (essa etapa pode ser feita mentalmente ou na etapa anterior).
3. Identificar cada variável usada na prova juntamente com o seu tipo (ex: Seja m um número inteiro).
4. Entender o enunciado e identificar o que são as hipóteses e a conclusão.
5. Marcar o início da demonstração com a palavra **PROVA**.
6. Começar a prova supondo que x é um elemento específico, mas escolhido arbitrariamente, do domínio para o qual a hipótese é verdadeira (ex: Seja $x \in \mathbb{U}$ tal que $P(x)$).
7. Construir passo a passo da prova apresentando uma justificativa.
8. Terminar a prova com a dedução da conclusão.

SÃO JUSTIFICATIVAS (PASSO 7) ACEITÁVEIS EM UMA PROVA:

- Pela hipótese $\cdots$
- Pelo axioma $\cdots$
- Pelo Teorema $\cdots$ provado anteriormente
- Pela definição $\cdots$
- Pelo passo $\cdots$ (um passo anterior do argumento) $\cdots$ Pela regra $\cdots$ da lógica.

Considere o seguinte teorema:

A soma de dois números pares é um número par.

OBSERVAÇÕES:

- O teorema pode ser reescrito como **"se n e m são dois números pares quaisquer, então $n+m$ é um número par"**.
- Possui a forma simbólica igual a $P(x) \rightarrow Q(x)$.
- Antes de verificar a veracidade do enunciado é preciso identificar e distinguir as hipóteses da conclusão:
  - Hipótese ($P(x)$): "n e m são dois números pares quaisquer".
  - Conclusão ($Q(x)$): "$n+m$ é um número par".
- Precisamos da definição de número par para seguir com as etapas da prova do teorema:
  (Definição de Número Par): n é par $\Leftrightarrow \exists$ um inteiro k tal que $n = 2k$.

Prova: (**Teorema:** A soma de dois números pares é um número par.)

1. Da hipótese do teorema, sejam n e m dois números números pares quaisquer.
2. Então, pela definição de número par, existem números r e $s \in \mathbb{Z}$ tais que $n = 2r$ e $m = 2s$.
3. Queremos provar que $n+m$ é par.
4. Da propriedade algébrica da distributividade, temos que a soma $n+m = 2r+2s = 2(r+s)$.
5. Por definição, temos que a soma $r+s \in \mathbb{Z}$.
6. Então, temos que existe um $t \in \mathbb{Z}$, tal que $t = r+s$.
7. Dessa forma, temos que $n+m = 2t$.
8. Portanto, pela definição de número par, podemos deduzir que $m+n$ também é par.

■

A demonstração anterior pode ser reescrita de forma mais simples, como apresentado a seguir.

Prova: (**Teorema:** A soma de dois números pares é um número par.)

Suponham n e m dois números pares. Pela definição de número par, existem números $r,s \in \mathbb{Z}$ tais que $n = 2r$ e $m = 2s$.
Queremos provar que $m+n$ é par.
Da propriedade algébrica da distributividade, podemos escrever a soma $n+m = 2r+2s = 2(r+s)$. Segue que a soma de dois números inteiros $r+s$ também é um número inteiro. Assim, vale dizer que $n+m = 2t$, onde $t = r+s$ e $t \in \mathbb{Z}$.
Portanto, podemos concluir que $n+m$ também é um número par. ■

O símbolo ■ que aparece no final da prova pode ser substituído por □ ou **c.q.d** e indica que a demonstração do teorema foi concluída. O termo **c.q.d** é a abreviação de "como se queria demonstrar".

Exemplo 2.3 Considere o seguinte teorema:

Se n é um número inteiro ímpar, então n^2 é ímpar.

OBSERVAÇÕES:

- O teorema está escrito na forma $P(x) \rightarrow Q(x)$.
- Hipótese: $P(x)$ é "n é um número inteiro ímpar".
- Conclusão: $Q(x)$ é "n^2 é ímpar".

Para provar o teorema vamos assumir que a hipótese é verdadeira.

Prova: (**Teorema:** Se n é um número inteiro ímpar, então n^2 é ímpar.)
Seja n um número inteiro ímpar. Então, pela definição de número ímpar, $n = 2k+1$ para algum $k \in \mathbb{Z}$.
Queremos mostrar que n^2 também é ímpar.

Elevando ambos os membros da equação $n = 2k+1$ ao quadrado, temos:

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Por definição de número ímpar e do resultado $n^2 = 2(2k^2+2k)+1$, podemos concluir que n^2 também é ímpar. ■

Exemplo 2.4 Considere o teorema:

Se m e n são ambos quadrados perfeitos, então $m.n$ também é um quadrado perfeito.

Dados:

- O teorema está escrito na forma $P(x) \to Q(x)$.
- Hipótese: $P(x)$ é "m e n são ambos quadrados perfeitos".
- Conclusão: $Q(x)$ é "$m.n$ também é um quadrado perfeito".
- Definição necessária para a etapa de prova:
  (Quadrado Perfeito) Um número n é um **quadrado perfeito** se existe $k \in \mathbb{Z}$ tal que $n = k^2$.

Prova: (**Teorema:** Se m e n são ambos quadrados perfeitos, então $m.n$ também é um quadrado perfeito.)
Sejam m e n ambos quadrados perfeitos. Pela definição **(Quadrado Perfeito)**, existem números $a, b \in \mathbb{Z}$, tais que $m = a^2$ e $n = b^2$.
Queremos provar que $m.n$ também é um quadrado perfeito.
Das propriedades do produto e potenciação, podemos escrever $m.n$ como:

$$m.n = a^2.b^2 = (a.b)^2$$

Portanto, como $m.n$ é o quadrado de $a.b$ e sabendo que $a.b \in \mathbb{Z}$, podemos concluir que $m.n$ também é um quadrado perfeito. ■

Exemplo 2.5 Considere o seguinte teorema:

Se a soma de dois números inteiros é par, então a sua diferença também é par.

OBSERVAÇÕES:

- O teorema está escrito na forma $P(x) \to Q(x)$.
- Pode ser reescrito, usando uma linguagem formal, como **Para todo inteiro m, n, se $m+n$ é par então $m-n$ é par**.
- Hipótese: $P(x)$ é "Para m, n inteiros $m+n$ é par".
- Conclusão: $Q(x)$ é "$m-n$ é par".

Prova: (**Teorema:** Se a soma de dois números inteiros é par, então a sua diferença também é par.)
Sejam m e n números inteiros tais que $m+n$ é par. Por definição de número par, temos que $m+n=2k$, para algum inteiro k.
Queremos provar que $m-n$ também é par.
Subtraindo n dois lados da equação $m+n=2k$, obtemos $m=2k-n$.
Veja que a diferença entre m e n, pode então ser escrita como:

$$\begin{aligned} m-n = \; & (2k-n)-n \\ & 2k-2n \\ & 2(k-n) \end{aligned}$$

Como k e n são ambos números inteiros, a expressão $k-n$ também é um número inteiro que, ao ser multiplicada por dois, torna-se um inteiro par.
Portanto, como $m-n$ é um múltiplo de dois, temos que $m-n$ é par. ■

Exercício: Prove os teoremas:

a) Para todo $n \in \mathbb{Z}$, se n é ímpar então $3n+9$ é par.
Prova:

b) Sejam $a,b \in \mathbb{R}$. Se $0 \leq a < b$ então $a^2 < b^2$.
Prova:

Erros Comuns em Demonstrações

É preciso ter cuidado em cada passo de uma demonstração matemática para que erros básicos de aritmética e álgebra não sejam cometidos. Cada passo realizado precisa estar correto e a conclusão precisa seguir logicamente os passos que a precedem. Vários erros podem ser cometidos durante uma demonstração, os mais comuns são:

1. Usar a mesma letra para representar duas coisas diferentes.

2. Argumentar a partir de exemplos:

> **Teorema:** Se a soma de dois números inteiros é par, então a sua diferença também é par.
> **Prova:**
> Caso 1: Considere $m = 8$ e $n = 2$ números pares. Então, segue que $m+n = 10$ é par e $m-n = 6$ também é par.
> Caso 2: Considere $m = 7$ e $n = 3$ números ímpares. Então, segue que $m+n = 10$ é par e $m-n = 4$ também é par.
> Portanto, o teorema é verdadeiro, c.q.d.

3. Pular para a conclusão:

> **Teorema:** Se a soma de dois números inteiros é par, então a sua diferença também é par.
> **Prova:**
> Suponha m e n números inteiros e que $m+n$ é par. Por definição de número par, $m+n = 2k$ para $k\mathbb{Z}$.
> Segue que $m = 2k-n$. Portanto, $m-n$ é par.

4. Assumir como verdadeiro o que deve ser provado:

> **Teorema:** Se $m.n$ é ímpar, então m e n são ambos ímpares.
> **Prova:**
> Se $m.n$ é ímpar, então por definição $m.n = 2k+1$ para algum $k \in \mathbb{Z}$. Suponha também que m e n são números ímpares. Por definição de números ímpares, $m = 2a+1$ e $n = 2b+1$.
> Então, $m.n = (2a+1)(2b+1) = 2k+1$ é ímpar, c.q.d.

2.2.1 Exercícios

1. Prove que se x é um inteiro impar, então x^3 é ímpar.
2. Suponha $x, y \in \mathbb{Z}$. Prove que se x e y são impares, então xy é impar.
3. Prove que se a soma de dois inteiros é par, então sua diferença também é par.
4. Prove que se n e m são quadrados perfeitos, então $(n.m)$ é um quadrado perfeito.
5. Prove que se a e b são números racionais, então $(a+b)$ é um número racional.
6. Sejam $a, b, c \in \mathbb{Z}$. Prove que se $a|b$ e $a|c$ então $a|(b+c)$.

7. Prove que, para quaisquer inteiros a,b,c, se $a|b$ e $b|c$ então $a|c$
8. Prove que, para todo $n \in \mathbb{Z}$, temos que $5n^2 + 3n + 7$ é impar.
9. Prove que para todos os números inteiros, se $a|b$ então $a^2|b^2$.
10. O que está errado na suposta "prova" da afirmação de que $1 = 2$?

    Prova:

1.	$a = b$	Sejam a e b dois números inteiros positivos iguais.
2.	$a^2 = ab$	Multiplicando ambos os membros de (1) por a.
3.	$a^2 - b^2 = ab - b^2$	Subtraindo b^2 de ambos os lados de (2).
4.	$(a-b)(a+b) = b(a-b)$	Fatorando ambos os membros de (3).
5.	$a + b = b$	Dividindo ambos os lados de (4) por $(a-b)$.
6.	$2b = b$	Substituindo a por b em (5), pois $a = b$ e simplificando.
7.	$2 = 1$	Dividindo ambos os membros de (6) por b.

11. O que está errado na suposta "prova" do teorema: "**Se n^2 é positivo, então n é positivo.**"

    Prova:

    1. Suponha que n^2 é positivo.
    2. A sentença condicional "se n é positivo, então n^2 é positivo" é verdadeira.
    3. Então, podemos concluir que n é positivo.

Aula 16: Técnicas de Prova: Prova por Contraposição

BCC101- Matemática Discreta I

DECOM/UFOP

3.1 Prova por Contraposição

Em uma prova direta, parte-se da veracidade das hipóteses e através de uma sequência de passos (axiomas, definições, teoremas já demonstrados e regras de inferência) deduzir a conclusão. Porém, por mais simples que pareçam a demonstração de algumas sentenças por prova direta não é uma tarefa simples. Para estes casos, uma boa estratégia é aplicar uma estratégia de prova indireta.

A **prova por contraposição** é um tipo de prova indireta que baseia-se na seguinte equivalência lógica:

$$P \to Q \equiv \neg Q \to \neg P \ \{\text{Contrapositivo}\}$$

que significa que toda sentença condicional é equivalente a sua contrapositiva.

Dessa forma, se não for possível provar que uma sentença condicional $(P(x) \to Q(x))$ é verdadeira, então basta mostrar que a sua contrapositiva é verdadeira. Os passos desta técnica de prova consistem em:

1. Dada a sentença do tipo $P(x) \to Q(x)$ escreva a contrapositiva equivalente a ela: $\neg Q(x) \to \neg P(x)$.
2. Tome como hipótese a sentença $\neg Q(x)$ (que é a negação da conclusão da sentença original).
3. Comece a demonstração com uma frase da forma: “Seja x um elemento do domínio, e suponha $\neg Q(x)$ verdadeira”.
4. Aplique na hipótese os axiomas, definições, teoremas demonstrados ou regras de inferência disponíveis.
5. Deduza $\neg P(x)$ (ou seja, mostre que a hipótese da sentença original é falsa).

6. Diante do fato de que a negação da conclusão implica na falsidade da hipótese, conclua que a sentença original é verdadeira.

A prova por contraposição é uma sequência de deduções justificadas, de forma que partindo de $\neg Q(x)$ conclui-se $\neg P(x)$.

Exemplo 3.1 Considere o seguinte teorema:

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

Primeiro vamos considerar a demonstração do teorema aplicando a prova direta.

Prova: **(Prova Direta)**

1. Seja $n \in \mathbb{Z}$.
2. Por hipótese, $3n+2$ é ímpar.
3. Pela definição de números ímpares, $3n+2 = 2k+1$, para algum $k \in \mathbb{Z}$.
4. Precisamos provar que n é ímpar.
   Temos um problema a partir daqui:
   Note que da equação $3n+2 = 2k+1$ é possível verificar que $3n+1 = 2k$ (é par). Porém, não conseguimos de forma direta concluir que n é ímpar.

■

A prova direta falhou para este teorema! Considere então a prova por contraposição.

- O teorema "se n é um inteiro e $3n+2$ é ímpar, então n é ímpar" é escrito como $P(x) \rightarrow Q(x)$.
- A contrapositiva equivalente é $\neg Q(x) \rightarrow \neg P(x)$, ou seja, "se n é par, então $3n+2$ é par."

Prova: **(Prova por Contraposição)**

1. Seja $n \in \mathbb{Z}$ um número par. Assumindo como verdadeira a negação da conclusão da sentença condicional original, ou seja, $\neg Q(x)$:
2. Pela definição de número par $n = 2k$ para algum $k \in \mathbb{Z}$.
3. Vamos provar que $3n+2$ é par (negação da hipótese da sentença condicional original $\neg P(x)$).
4. Substituindo $2k$ em n temos:

$$3n+2 = 3(2k)+2 = 6k+2 = 2(3k+1)$$

5. Do passo anterior, como $3n+2$ é múltiplo de 2 podemos concluir que é par. (negação da hipótese do teorema original)
6. Como a negação da conclusão implica na negação da hipótese, podemos afirmar que a sentença original é verdadeira.
7. Logo, temos que se n é um inteiro e $3n+2$ é ímpar, então n é ímpar.

■

Exemplo 3.2 Prove o teorema: **Para todo $n \in \mathbb{Z}$, se n^2 é par, então n é par.**

Ao invés de provar a condicional (n^2 é par $\rightarrow$ n é par) vamos provar a contrapositiva (n é ímpar $\rightarrow$ n^2 é ímpar).

Prova: **(Por Contraposição)**
Seja $n \in \mathbb{Z}$ e suponha que n é ímpar. Então, $n = 2k+1$ para algum $k \in \mathbb{Z}$.
Precisamos provar que n^2 também é ímpar.
Temos que:

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

Do resultado $n^2 = 2(2k^2+2k)+1$ temos que n^2 é ímpar.
Logo, provado a contrapositiva, podemos concluir que se n^2 é par, então n é par. ∎

Exemplo 3.3 Prove que se $n+1$ senhas diferentes forem distribuídas para n alunos, então algum aluno receberá um número maior ou igual a 2 senhas.

Para realizar a prova, considere:

- O argumento possui como hipótese "$n+1$ senhas diferentes foram distribuídas para n alunos" e como conclusão "algum aluno receberá um número ≥ 2 de senhas".
- A conclusão é do tipo $\exists x, Q(x)$. E sua negação $\neg[\exists x, Q(x)]$ é equivalente a $\forall x, \neg Q(x)$.
- O teorema é escrito na forma simbólica por $P(x) \rightarrow \exists x, Q(x)$.
- A contrapositiva do teorema original é:
  - Simbolicamente: $\forall x, \neg Q(x) \rightarrow \neg P(x)$
  - "Se todo aluno receber um número < 2 de senhas, então não foram distribuídas $n+1$ senhas para os n alunos."

Prova: **(Por Contraposição)**
Suponha que todo aluno receba uma quantidade "menor que 2" de senhas.
Então, cada um dos n alunos possui, no máximo, 1 senha.
Do passo anterior, temos que o número total de senhas distribuídas é no máximo igual a n. (negando a hipótese de que $n+1$ senhas foram distribuídas.)
Portanto, temos que se $n+1$ senhas diferentes forem distribuídas para n alunos, então algum aluno receberá um número maior ou igual a 2 de senhas. ∎

Exercício: Sejam $a,b,c \in \mathbb{R}$ e $a > b$. Prove que, se $ac \leq bc$, então $c \leq 0$

3.1.1 Exercícios

1. Prove que se x é um número irracional, então $\sqrt{x}$ é um número irracional.
2. Sejam $a,b \in \mathbb{Z}$. Prove que se $a^2(b^2-2b)$ é impar, então a e b são ambos ímpares.
3. Suponha $x \in \mathbb{R}$. Prove que se $x^2+5x < 0$ então $x < 0$.
4. Prove que para todo número inteiro se n^2 não é divisível por 5, então n não é divisível por 5.
5. Prove que o negativo de todo número irracional também é um número irracional.
6. Considere $x \neq 0$. Prove que se $1/x$ é um número irracional então x também é irracional.
7. Prove que para todos os inteiros a,b e c, se a não divide bc então a não divide b.
8. Para todos os inteiros m e n, se $m+n$ é par, então m e n são pares ou m e n são ambos ímpares.
9. Para todos os inteiros m e n, se mn é par, então m é par ou n é par.

Aula 17: Técnicas de Prova: Prova por Contradição

BCC101- Matemática Discreta I

DECOM/UFOP

4.1 Prova por Contradição

A **prova por contradição** é um tipo de prova indireta que baseia-se no fato de que uma afirmação é verdadeira ou é falsa, mas não ambas. Então, se for possível mostrar que a suposição de que uma determinada afirmação não verdadeira, leva logicamente a uma contradição (ou absurdo)então essa suposição só pode ser falsa e, portanto, a afirmação dada deve ser verdadeira. Esta técnica de prova, que também é conhecida por **prova por redução ao absurdo**, é uma das ferramentas mais poderosas na matemática. De um modo geral, neste tipo de prova assumimos que a tese é falsa e, mostramos que esta suposição leva a uma **contradição** ou **absurdo**.

A argumentação por contradição também ocorre em outros contextos. Por exemplo, se um homem acusado de roubar um banco puder provar que ele estava em algum outro lugar no momento em que o crime foi cometido, então ele certamente será inocentado. A lógica de sua defesa é a seguinte: suponha que eu tenha cometido o crime. Então, no momento do crime, eu deveria que estar no local do crime. Porém, no momento do crime eu estava em uma reunião com 20 pessoas, longe da cena do crime, e todas elas irão testemunhar a meu favor. Isso contradiz a suposição de que eu teria cometido o crime, já que é impossível estar em dois lugares ao mesmo tempo. Portanto, a suposição (o homem cometeu um crime) é falsa.

Os passos para a prova por contradição de um teorema na forma $P(x) \rightarrow Q(x)$ são:

1. Assuma a sentença $P(x)$ verdadeira.
2. Suponha que a afirmação que deve ser provada é falsa, ou seja, negue a conclusão ($\neg Q(x)$). Faça isso, iniciando sua demonstração com a seguinte frase: **Suponha, por contradição, que** $\neg Q(x)$.
3. Construa o passo a passo da prova aplicando as definições, teoremas já demonstrados e regras de inferência.
4. Argumente cada passo como se estive aplicando a prova direta, até alcançar uma sentença que você saiba que é falsa (uma contradição ou um absurdo).
5. Como a negação da conclusão resulta em um absurdo, conclua que a afirmação a ser provada ($Q(x)$) é verdadeira.

Exemplo 4.1 Prove o seguinte teorema:

$$\sqrt{2} \textbf{ é um número irracional}$$

Prova: **(Por Contradição)**

1. Suponha por contradição que $\sqrt{2}$ é um número racional (negação da conclusão).

2. Pela definição de número racional, $\sqrt{2} = a/b$ para $a, b \in \mathbb{Z}$ e $b \neq 0$.

3. Vamos supor, sem perda de generalidade, que a/b é uma fração irredutível. Então, a e b são primos entre si ($mdc(a,b) = 1$).

4. Elevando a igualdade do passo 2 ao quadrado, temos:

$$(a/b)^2 = (\sqrt{2})^2 = 2 \Rightarrow a^2/b^2 = 2 \Rightarrow a^2 = 2b^2$$

5. Do passo (4), temos que a^2 é par.

6. Do exemplo (3.2) temos que a também é par. Então, $a = 2k$ para algum $k \in \mathbb{Z}$.

7. Segue que:

$$a^2 = 2b^2 \Rightarrow b^2 = a^2/2 = (2k)^2/2 = 2k^2$$

8. Do passo anterior, b^2 também é par. Portanto b também é par.

9. Isso é um absurdo! Pois contradiz o fato de que a e b são primos entre si e que a/b é uma fração irredutível.

10. Portanto, concluímos que $\sqrt{2}$ é irracional. ■

Observe que a contradição obtida no passo (9) mostra que a suposição feita no passo (1) é falsa. Desta forma, podemos concluir que o teorema é verdadeiro.

Exemplo 4.2 Prove por contradição que **Se a e b números inteiros, então** $a^2 - 4b \neq 2$.

Prova: **(Por Contradição)**

1. Sejam a e b números inteiros.
2. Queremos provar que $a^2 - 4b \neq 2$.
3. Suponha, por contradição, que $a^2 - 4b = 2$.
4. Segue que:

$$\begin{aligned} a^2 &= 2 + 4b \\ &= 2(1 + 2b) \end{aligned}$$

como a^2 é múltiplo de 2 temos que a^2 é par.

5. Do exemplo (3.2), temos que se a^2 é par, então a também é par.
6. Então, $a = 2k$, para algum $k \in \mathbb{Z}$.
7. Substituindo a por $2k$ na equação do passo (4) temos:

$$(2k)^2 = 2(1 + 2b) \Rightarrow 4k^2 = 2(1 + 2b)$$

8. Dividindo ambos os lados por 2:

$$\begin{aligned} 2k^2 = 1 + 2b \Rightarrow \quad 1 &= 2b - 2k^2 = 2(b - k^2) \\ 1 &= 2(b - k^2) \end{aligned}$$

9. Dados que $b, k \in \mathbb{Z}$, deduzimos que 1 é par. **O que é um absurdo!**
10. Logo, podemos concluir que $a^2 - 4b \neq 2$. ■

Exercício: 1. Prove por contradição que para todo n, se n^2 é par, então n é par.

Prova:

Exercício: Prove por contradição que se $3n+2$ é ímpar, então n é ímpar.

Prova:

4.1.1 Exercícios

1. Prove que $(1+3\sqrt{2})$ é irracional.
2. Prove que se $a,b \in \mathbb{Z}$, então $a^2-4b-2 \neq 0$.
3. Prove que existem infinitos números primos (A prova dessa afirmação foi provada pelo matemático greco Euclides, no século IV A.C.)
4. Suponha $a,b,c \in \mathbb{Z}$. Prove que se $a^2+b^2=c^2$, então a ou b é par.
5. Sejam $a,b \in \mathbb{R}$. Prove que se a é racional e ab é irracional, então b é irracional.
6. Prove que se a e b são números reais positivos, então $a+b \geq 2\sqrt{ab}$.
7. Prove que todo número racional diferente de zero pode ser expresso como o produto de 2 números irracionais.
8. Prove que o negativo de todo número irracional também é um número irracional.

4.2 Particularidades das Declarações Existenciais

4.2.1 Quantificação Existencial

Os teoremas que aparecem escritos como $\exists x, P(x)$ também podem ser demonstrados usando a demonstração não construtiva, ou seja, mostrando que a afirmativa $\exists x, P(x)$ pode ser provada de outra maneira, mesmo sem exibir explicitamente um valor a tal que $P(a)$ seja verdadeira.

Exemplo 4.3 Mostre que existem números irracionais x e y, tal que x^y é racional.

Prova: **(Demonstração não Construtiva)**

Do exemplo 4.1 temos que $\sqrt{2}$ é um número irracional.

Considere então o seguinte número: $\sqrt{2}^{\sqrt{2}}$.

Temos duas situações possíveis: $\sqrt{2}^{\sqrt{2}}$ é racional ou $\sqrt{2}^{\sqrt{2}}$ é irracional.

Diante destes dois casos, temos:

$\sqrt{2}^{\sqrt{2}}$ **é racional:**

Supondo que $\sqrt{2}^{\sqrt{2}}$ é racional e do exemplo 4.1 temos que $x = y = \sqrt{2}$ são irracionais.

Logo, podemos concluir que a sentença é verdadeira.

Caso 1) Caso 2) $\sqrt{2}^{\sqrt{2}}$ **é irracional:**

Sejam $x = \sqrt{2}^{\sqrt{2}}$ e $y = \sqrt{2}$ dois números irracionais.

Logo: $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^{2} = 2$ é racional.

Dessa forma, temos que para x e y irracionais, x^y é racional.

■

OBSERVAÇÕES

- Nesta prova não encontramos um exemplo de números irracionais x e y que valide a afirmação que $x.y$ é racional.
- O que fizemos foi obter dois pares de números ($\sqrt{2}$ e $\sqrt{2}$) ou ($\sqrt{2}^{\sqrt{2}}$ e $\sqrt{2}$) em que um deles possui a propriedade desejada.
- Assim, mesmo não mostrando qual par de números verifica a afirmação, podemos concluir que a afirmação é verdadeira para um deles.

O teorema **"Existem números irracionais x e y, tal que x^y é racional"** também pode ser provado usando a demonstração construtiva.

Prova: **(Demonstração Construtiva)**

Para provar a sentença, precisamos encontrar um valor para x e um valor para y que torne $P(x,y)$ verdadeira.

- Considere $x = \sqrt{2}$ e $y = \log_2^9$.
- Temos que $x^y = \sqrt{2}^{\log_2 9}$.

- Usando as propriedades operatórias dos logaritmos:

$$x^y = \left(\sqrt{2}\right)^{\log_2 9} = \left(\sqrt{2}\right)^{2\log_2^3} = \left(\sqrt{2}^2\right)^{\log_2^3} = 2^{\log_2^3} = 3$$

- Sabendo que $\sqrt{2}$ é irracional e supondo que $\log_2^9$ também seja irracional, temos que x^y é racional.

Para completar a prova, precisamos provar que $\log_2^9$ também é um número irracional.

Prova: Suponha, por **contradição**, que $\log_2^9$ é um número racional.
Então, $\log_2^9 = \frac{a}{b}$, para $a, b \in \mathbb{Z}$ e $b \neq 0$.
Da definição de logaritmo:

$$\log_2^9 = \frac{a}{b} \Leftrightarrow 2^{\left(\frac{a}{b}\right)} = 9.$$

Elevando ambos os lados por b, temos:

$$2^{\left(\frac{a}{b}\right)} = 9 \;\Rightarrow\; \left(2^{\left(\frac{a}{b}\right)}\right)^b = (9)^b \;\Rightarrow\; 2^a = 9^b.$$

Este resultado $2^a = 9^b$ é um absurdo! Pois 2^a é par e 9^b é ímpar, para quaisquer valores de a e b.
Partindo da hipótese que $\log_2^9$ é um número racional chegamos a uma contradição. Logo, podemos concluir que $\log_2^9$ é um número irracional.

Provado que $\log_2^9$ é irracional, podemos concluir que existem números irracionais $x = \sqrt{2}$ e $y = \log_2^9$, tal que x^y é um número racional. ■

4.2.2 Demonstração da Existência e Unicidade

Teoremas no formato

$$\exists! x, P(x)$$

afirmam a existência de um único elemento com uma determinada propriedade. A demonstração deste tipo de sentença é feita mostrando que um elemento com essa propriedade existe e que os demais elementos do domínio não possuem a propriedade.

A demonstração da existência e unicidade é dividida em duas partes:

Existência: Deve ser verificado que existe pelo menos um elemento x que satisfaz $P(x)$ (Nesta parte é provado que $\exists x, P(x)$ é verdadeiro).

Unicidade: Deve ser mostrado que se $y \neq x$, então y não tem a propriedade desejada. (Nesta parte prova-se que a sentença $\forall y, (y \neq x \rightarrow \neg P(y))$ é verdadeira).
De forma sucinta, a prova da unicidade deve ser feita supondo que existe um y que satisfaz $P(y)$ e em seguida prova-se que $y = x$.

Exemplo 4.4 Mostre que se a e b são números reais e $a \neq 0$, então existe um único número real r, tal que $ar + b = 0$

Prova: Sejam $a, b \in \mathbb{R}$ e $a \neq 0$.

Prova da Existência: Seja o número real $r = -\frac{b}{a}$.

Note que o número r é solução da equação $ar + b = 0$, pois

$$a\left(-\frac{b}{a}\right) + b = -b + b = 0$$

Logo, existe um número real r para o qual $ar + b = 0$.

O que prova a primeira parte do teorema, ou seja, que existe um número real r que satisfaz a equação.

Prova da Unicidade: Precisamos provar que r é a única solução da equação.

Sabe-se que $ar + b = 0$ e $r = -b/a$ (primeira parte da prova). Seja s um número real, tal que $as + b = 0$.

Se s também é solução da equação, temos que:

$$ar + b = as + b$$

Subtraindo b em ambos os lados da equação: $ar = as$.

Dividindo ambos os lados por a, com $a \neq 0$, temos: $r = s$.

Isso significa que $as + b = 0$ somente se $s = r$. Ou seja, caso $r \neq s$ a equação $as + b \neq 0$.

Logo, verifica-se a parte da unicidade do teorema.

Portanto, podemos concluir que se a e b são números reais e $a \neq 0$, então existe um único número real r, tal que $ar + b = 0$ ■

Aula 18: Técnicas de Prova: Particularidades

BCC101- Matemática Discreta I

DECOM/UFOP

5.1 Demonstração por Casos

Nas situações em que não é possível comprovar um teorema usando um único argumento que satisfaça todas as possibilidades possíveis, vamos usar uma estratégia de demonstração que divide o teorema em casos cobrindo todas as possibilidades.

Implicação com Hipótese Disjuntiva

Seja uma implicação da forma:

$$(P_1 \vee P_2 \vee \cdots \vee P_n) \rightarrow Q \tag{5.1}$$

onde a hipótese é uma disjunção de várias afirmações. Provar a equação (5.1) é equivalente a provar a seguinte tautologia:

$$(P_1 \rightarrow Q) \wedge (P_2 \rightarrow Q) \wedge (P_3 \rightarrow Q) \wedge \cdots \wedge (P_n \rightarrow Q)$$

Em outras palavras, para demonstrar um teorema com hipótese disjuntiva é necessário provar cada uma das condicionais (que listaremos por casos) separadamente. Este argumento é chamado de **demonstração por casos**.

Mesmo nos casos onde a sentença for uma condicional simples $P \rightarrow Q$, para fazer a prova por casos é necessário usar a disjunção $P_1 \vee P_2 \vee \cdots \vee P_n$ em vez de P como hipótese, desde que P e $P_1 \vee P_2 \vee \cdots \vee P_n$

sejam sentenças equivalentes.

Exemplo 5.1 Prove que para quaisquer inteiros m e n, se m for par ou n for par, então $m.n$ é par.
Precisamos verificar dois casos: quando m é par quando n é par. Dividindo a demonstração nos dois casos listados, temos a seguinte prova:

Prova: Sejam m e n inteiros quaisquer.

caso 1) seja m um inteiro par:

Por definição, existe um inteiro k tal que $m = 2k$.

Neste caso, $m.n = (2k)n = 2(k.n)$ pela propriedade da associatividade da multiplicação.

Como $m.n$ é escrito como múltiplo de 2, temos que $m.n$ é par.

caso 2) seja n um inteiro par:

Por definição, existe um inteiro k tal que $n = 2k$.

Neste caso, $m.n = m(2k) = 2(m.k)$ pela propriedade da associatividade da multiplicação.

Como $m.n$ é escrito como múltiplo de 2, temos que $m.n$ é par.

Portanto, se m é par ou n é par, temos que $m.n$ é par. ■

Exemplo 5.2 Prove que se n é um inteiro, então $n^2 \geq n$.

Prova: Queremos provar que $n^2 \geq n$ para qualquer número inteiro. Para tanto, precisamos considerar três casos distintos: quando $n = 0$, quando $n \geq 1$ e quando $n \leq -1$.

Dividindo a demonstração nos três casos listados, temos:

Caso 1) Seja $n = 0$:

Como $0^2 = 0$, segue que $0^2 \geq 0$.

Logo, $n^2 \geq n$ é verdadeira para o caso 1).

Caso 2) Seja $n \geq 1$:

Considere a inequação $n \geq 1$.

Multiplicando ambos os membros por um inteiro positivo n, obtemos $n.n \geq n.1$.

Tal fato implica que $n^2 \geq n$ é verdadeira para o caso 2).

Caso 3) Seja $n \leq -1$:

Sabe-se que $n^2 \geq 0$ para qualquer $n \in \mathbb{Z}$.

Considerando que $n \leq -1$, segue que $n^2 \geq n$. Logo, $n^2 \geq n$ é verdadeira para o caso 3).

Como a inequação $n^2 \geq n$ é verdadeira para os três casos, podemos concluir que se n é um número inteiro, então $n^2 \geq n$. ■

Implicação com Tese Conjuntiva

Seja um teorema na forma $P \rightarrow (Q_1 \wedge Q_2)$. A demonstração de um teorema neste formato deve feita através da prova da seguinte sentença equivalente:

$$(P \to Q_1) \wedge (P \to Q_2)$$

A demonstração deve ser feita para cada uma das condicionais separadamente!

Exemplo 5.3 Mostre que se 6 divide um inteiro n, então 2 divide n e 3 divide n.

Prova: Seja $n \in \mathbb{Z}$. Se 6 divide n, então existe um $k \in \mathbb{Z}$ tal que $n = 6k$.

Vamos dividir a demonstração em dois casos: Caso 1) 2 divide n e Caso 2) 3 divide n:

Caso 1) 2 divide n:

De $n = 6k$, temos $n = 2(3k)$ e logo 2 divide n.

Caso 2) 3 divide n:

De $n = 6k$, também temos $n = 2(3k) = 3(2k)$ e logo 3 divide n.

Portanto, podemos concluir que se 6 divide um inteiro n, então 2 divide n e 3 divide n. ■

Exercício: Dados dois números quaisquer x, y, prove que $|x+y| \leq |x| + |y|$

Prova:

5.1.1 Exercícios

1. Prove que, se o produto de dois números inteiros (xy) não é divisível por n, então x não é divisível por n e y não é divisível por n.
2. Prove que, para todo $n \in \mathbb{N}$, $n^2 = 2\binom{n}{2} + \binom{n}{1}$

5.2 Demonstração de sentença bicondicional

A demonstração de sentenças na forma $P \leftrightarrow Q$ (P **se e somente se** Q) deve ser feita provando duas sentenças condicionais (na forma "se – então"), ou seja, prova-se separadamente as afirmações $P \to Q$ e $Q \leftarrow P$ da seguinte maneira:

Prova:
Identifique todas as variáveis do teorema e o que precisa ser provado.
($\Rightarrow$) Suponha $P(x)$.
$\ldots$
Conclua $Q(x)$.
($\Leftarrow$) Suponha $Q(x)$.
$\vdots$
Conclua $P(x)$.
Logo, conclua verdadeira a sentença $P(x) \Leftrightarrow Q(x)$.

OBSERVAÇÃO: As provas da "ida" e da "volta" do teorema devem ser indicadas, respectivamente, pelos símbolos ($\Rightarrow$) e ($\Leftarrow$), para que o leitor consiga identificar cada parte da prova.

Exemplo 5.4 Seja $x \in \mathbb{Z}$. Prove que x é par se, e somente se, $x+1$ é ímpar.

Prova: Seja $x \in \mathbb{Z}$.
Precisamos provar: ($\Rightarrow$) se x é par, então $x+1$ é ímpar e ($\Leftarrow$) se $x+1$ é ímpar, então x é par.

- ($\Rightarrow$) Seja x um número par.
  Por definição, $x = 2k$ para algum $k \in \mathbb{Z}$
  Somando 1 em ambos os membros da equação $x = 2k$, temos:
  $$x+1 = 2k+1$$
  Então, por definição, $x+1$ é ímpar.
- ($\Leftarrow$) Seja $x+1$ um número ímpar.
  Por definição, $x+1 = 2k+1$ para algum $k \in \mathbb{Z}$
  Subtraindo 1 em ambos os membros da equação $x+1 = 2k+1$, temos:
  $$x+1-1 = 2k+1-1 \quad \Rightarrow \quad x = 2k$$
  Então, por definição, x é par.

Portanto, temos que x é par se, e somente se, $x+1$ é ímpar. c.q.d. ■

Exemplo 5.5 Seja $x, y \in \mathbb{Z}$. Então x e y são ambos ímpares se, e somente se, $x.y$ é ímpar.

Prova: Sejam $x, y \in \mathbb{Z}$.
Precisamos provar: ($\Rightarrow$) se x e y são ímpares, então $x.y$ é ímpar e ($\Leftarrow$) se $x.y$ é ímpar, então x e y são ímpares.

- ($\Rightarrow$) Sejam x e y números ímpares.

Então, por definição existem $k, s \in \mathbb{Z}$ tais que $x = 2k+1$ e $y = 2s+1$.

Logo:

$$x.y = (2k+1)(2s+1) = 4ks+2k+2s+1 = 2(2ks+k+s)+1$$

Como $2ks+k+s$ é um número inteiro, por definição, temos que $x.y$ é ímpar.

- ($\Leftarrow$) Seja $x.y$ um número ímpar, então x e y são ambos ímpares.

  Fazendo a prova pela contrapositiva:

  Queremos provar que "se x é par ou y é par, então $x.y$ é par."

  Considere os dois casos abaixo:

  - **Caso 1:** x é par.

    Existe um inteiro k tal que $x = 2k$.

    Portanto, $x.y = (2k)y = 2(k.y)$.

    Como ky é um número inteiro, temos que $x.y$ é par.

  - **Caso 2:** y é par.

    Existe um inteiro r tal que $y = 2r$.

    Portanto, $x.y = x(2r) = 2(x.r)$.

    Como $x.r$ é um número inteiro, temos que $x.y$ é par.

Logo, temos que x e y são ambos ímpares se, e somente se, $x.y$ é ímpar. ■

Exemplo 5.6 Prove que para todo inteiro n, as afirmações seguintes são equivalentes:

(a) n é ímpar.

(b) $(n+1)$ é par.

(c) n^2 é ímpar.

Dados que as três afirmações são equivalentes, precisamos provar que $(a) \Leftrightarrow (b) \Leftrightarrow (c)$.

Vamos usar a seguinte estratégia de prova:

$$(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)$$

Prova: Seja $n \in \mathbb{Z}$. Vamos dividir a prova em três partes:

- **Parte 1:** $(a) \Rightarrow (b)$

  Vamos provar que se "n é ímpar, então $(n+1)$ é par".

  Seja n ímpar. Por definição, existe um $k \in \mathbb{Z}$ tal que $n = 2k+1$.

  Então, $n+1 = (2k+1)+1 = 2k+2 = 2(k+1)$.

  Como $k+1$ é um número inteiro, podemos concluir que $n+1$ é par.

- **Parte 2:** $(b) \Rightarrow (c)$

  Vamos provar que se "$(n+1)$ é par, então n^2 é ímpar" .

  Seja $n+1$ par. Por definição, existe um $k \in \mathbb{Z}$ tal que $n+1 = 2k$.

  Logo, $n = 2k-1$ e $n^2 = (2k-1)^2 = (2k-1)(2k-1) = 4k^2-4k+1 = 2(2k^2-2k)+1$.

  Como $2k^2-2k$ é um número inteiro, podemos concluir que n^2 é ímpar.

- **Parte 3:** $(c) \Rightarrow (a)$

  Vamos provar que se "n^2 é ímpar, então n é ímpar" .

  Essa afirmação é verdadeira e foi provada no exemplo (2).

Portanto, temos que as afirmações (a), (b) e (c) são equivalentes. ■

Exercício: Prove que um número inteiro positivo n é par se, e somente se, n^2 é par.

5.2.1 Exercícios

1. Seja $a \in \mathbb{Z}$. Prove que $a^3 + a^2 + a$ é par se e somente se a é par.
2. Seja $x \in \mathbb{Z}$. Prove que x é ímpar se, e somente se, $3x + 6$ é ímpar.
3. Suponha $x, y \in \mathbb{R}$. Prove que $x^3 + x^2y = y^2 + xy$ se, e somente se, $y = x^2$ ou $y = -x$.

Resumo

A tabela seguinte apresenta um resumo das técnicas de demonstração estudadas.

Prova	**Sentença**	**Prova**
Quantificador Universal	$\forall x, P(x)$	Suponha um x arbitrário. Prove que $P(x)$ é verdadeira.
Quantificador Existencial	$\exists x, P(x)$	**Prova Construtiva:** Encontre um valor a tal que $P(a)$ é verdadeira. **Prova Não Construtiva:** Mostre que $\exists x, P(x)$ pode ser provada de outra maneira sem exibir explicitamente um elemento a que torne a sentença verdadeira.
Quantificador da Existência e Unicidade	$\exists! x, P(x)$	Divida a demonstração em duas partes: **Existência:** Prove que existe um elemento que torne $P(x)$ verdadeira. **Unicidade:** Prove que este elemento é único. Suponha que existe um y que satisfaz $P(y)$ e prove que $y = x$.
Por Exaustão	$P(x) \rightarrow Q(x)$	Prove a sentença para todos os casos possíveis.
Direta	$P(x) \rightarrow Q(x)$ ou $\forall x, P(x) \rightarrow Q(x)$	Suponha $P(x)$ e deduza $Q(x)$. Seja x pertencente ao domínio. Assuma que $P(x)$ é verdadeira e prove $Q(x)$.
Por Contraposição	$P(x) \rightarrow Q(x)$	Suponha $\neg Q(x)$ e deduza $\neg P(x)$. Assuma que $\neg Q(x)$ é verdadeira e prove que $\neg P(x)$ é verdadeira.
Por Contradição	$P(x) \rightarrow Q(x)$	Assuma $\neg Q(x)$ e tente obter uma contradição. Suponha $P(x)$ verdadeira. Suponha que $\neg Q$ também é verdadeira e deduza uma contradição.
Por Casos	$P_1(x) \vee P_2(x) \rightarrow Q(x)$ **Implicação com Hipótese Disjuntiva**	Prove que $(P_1(x) \rightarrow Q(x)) \wedge (P_2(x) \rightarrow Q(x))$ Prove cada das condicionais separadamente
	$P(x) \rightarrow Q_1(x) \wedge Q_2(x)$ **Implicação com Tese Conjuntiva**	Prove que: $(P(x) \rightarrow Q_1(x)) \wedge (P(x) \rightarrow Q_2(x))$ Prove cada das condicionais separadamente
Bicondicional	$P(x) \leftrightarrow Q(x)$	Prove $P(x) \rightarrow Q(x)$ e $Q(x) \rightarrow P(x)$

Propriedades Algébricas

Sejam $a, b, c \in \mathbb{R}$. São válidas as seguintes propriedades derivadas dos axiomas de corpo, axiomas de ordem e das definições:

PAD1. **(Cancelamento da Adição):** Se $a+b=a+c$, então $b=c$.

PAD2. **(Subtração):** Dados a e b, existe exatamente um único x tal que $a+x=b$. x é denotado por $b-a$.

PAD3. $b-a=b+(-a)$.

PAD4. $-(-a)=a$.

PAD5. $a(b-c)=ab-ac$.

PAD6. $0.a=a.0=0$.

PAD7. **(Cancelamento da Multiplicação):** Se $ab=ac$ e $a\neq 0$, então $b=c$.

PAD8. **(Divisão):** Dados a e b com $a\neq 0$. Existe exatamente um inteiro x tal que $b=ax$. Este x, denotado por $a|b$ (b/a), é chamado de quociente de b e a. Dizemos que b é divisível por a.

PAD9. Se $a\neq 0$, então $b/a=b.a^{-1}$.

PAD10. Se $a\neq 0$, então $(a^{-1})^{-1}=a$.

PAD11. Se $ab=0$, então $a=0$ ou $b=0$.

PAD12. **(Regra da multiplicação com sinais negativos):** $(-a)b=a(-b)=-(ab)$, $(-a)(-b)=ab$ e $-\frac{a}{b}=\frac{-a}{b}=\frac{a}{-b}$.

PAD13. **(Equivalência de Frações):** $\dfrac{ac}{bc}=\dfrac{a}{b}$, se $b\neq 0$ e $c\neq 0$.

PAD14. **(Soma de Frações):** $\dfrac{a}{b}+\dfrac{c}{d}=\dfrac{ad+bc}{bd}$, se $b\neq 0$ e $d\neq 0$.

PAD15. **(Multiplicação de Frações):** $\dfrac{a}{b}.\dfrac{c}{d}=\dfrac{ac}{bd}$, se $b\neq 0$ e $d\neq 0$.

PAD16. **(Divisão de Frações):** $\dfrac{\frac{a}{b}}{\frac{c}{d}}=\dfrac{a}{b}.\dfrac{d}{c}=\dfrac{ad}{bc}$, se $b\neq 0$, $c\neq 0$ e $d\neq 0$.

PAD17. **(Lei da Tricotomia):** Para números reais a e b arbitrários, apenas uma das relações é válida: $a<b$, $a>b$ ou $a=b$.

PAD18. **(Transitividade):** Se $a<b$ e $b<c$, então $a<c$.

PAD19. Se $a<b$, então $a+c<b+c$.

PAD20. Se $a<b$ e $c>0$, então $ac<bc$.

PAD21. Se $a\neq 0$, então $a^2>0$.

PAD22. $1>0$.

PAD23. Se $a<b$ e $c<0$, então $ac>bc$.

PAD24. Se $a<b$, então $-a>-b$. Em particular, se $a<0$, então $-a>0$.

PAD25. Se $ab>0$, então a e b são ambos positivos ou ambos negativos.

PAD26. Se $a<c$ e $b<d$, então $a+b<c+d$.

PAD27. Se $0<a<c$ e $0<b<d$, então $0<ab<cd$.

Referências Bibliográficas

[1] HAMMACK, R. H. *Book of Proof*. 2ª. ed. Virginia: Richard Hammack, 2013. v. 1.

[2] GERSTING, J. L. *Fundamentos Matemáticos para a Ciência da Computação: Matemática Discreta e suas Aplicações*. 7ª. ed. Rio de Janeiro: LTC, 2017.

[3] RIBEIRO, R. G. *Notas de Aula de Matemática Discreta*. [S.l.]: Universidade Federal de Ouro Preto, 2016.

[4] MENEZES, P. B. *Matemática Discreta para a Computação e Informática*. 4ª. ed. Porto Alegre: Bookman, 2013.

[5] HUNTER, D. J. *Fundamentos da Matemática Discreta*. Rio de Janeiro: LTC, 2011.

[6] EPP, S. S. *Discrete Mathematics With Applications*. Fourth. Boston - USA: Cengage Learning, 2010. ISBN 978-0-495-39132-6.

Respostas Dos Exercícios

Aula 14

1.1.3 - Introdução

1. (a) Sim. Pois $0 = 2.0$.
   (b) Sim. Pois $-51 = 2(-25) + 1$.
   (c) Sim, pois $2k - 1 = 2(k - 1) + 1$ e $k - 1$ é inteiro.
   (d) Sim. Pois $2a + 4b = 2(a + 2b)$ e $(a + 2b)$ é inteiro.
   (e) Sim. Pois $2a + 4b = 2(a + 2b + 1) + 1$ e $a + 2b + 1$ é um número inteiro.
   (f) Sim, pois $10ab + 7 = 2(5ab + 3) + 1$ e $5ab + 3$ é um número inteiro.
   (g) Não, pois $6a + 4b^2 + 3 = 2(3a + 2b^2 + 1) + 1$, que por definição é um número ímpar.
   (h) Não. Pois é necessário que o número seja maior que 1 e tenha 2 divisores distintos (1 e ele mesmo).
   (i) Não. A propriedade não é válida para todos os números inteiros. Seja por exemplo $a = 1$ e $b = 2$, temos que $(1 + 2)^2 = 9$ e $1^2 + 2^2 = 5$ e $9 \neq 5$.
   (j) Sim. A propriedade é válida apenas quando n for um número ímpar. Para n par a propriedade falha, seja por exemplo $a = 3$ e $n = 2$, temos que $-3^2 = -9$ e $(-3)^2 = 9$ e $-9 \neq 9$.
   (k) Sim. Pois $5/3$ é o quociente dos números inteiros 5 e 3.
   (l) Sim. Pois 0 é quociente dos números inteiros 0 e 1, ou seja $0/1$.
   (m) Sim, pois $1,75 = 7/4$.

1.2.3 - Teoremas

1. **Prova:** A afirmação é verdadeira por vacuidade. Não existe número que seja simultaneamente primo e quadrado perfeito.
2. (a) **Contraexemplo**: um retângulo.
   (b) **Contraexemplo**: 0.
   (c) **Contraexemplo**: uma pessoa ruiva baixa e com olhos azuis.
   (d) **Contra-Exemplo**: $n = -1$.
   (e) **Contraexemplo**: $n = 8$ é par e $n^2 + 1 = 65$ não é primo.
   (f) **Contraexemplo**: $n = 1$.
   (g) **Contraexemplo**: $9 - 7 = 2$
   (h) **Contraexemplo**: $3 \times 9 = 27$
   (i) **Contraexemplo**: O inteiro 2 é primo, mas é par.
   (j) **Contraexemplo**:Seja $a = b = 2$. Então $mod(a, b) = mod(b, a) = 0$.

3. **Prova:** Tome, por exemplo, $x = 1/4$. Então temos que $x^2 = (1/4)^2 = 1/16 < \sqrt{1/4)} = 1/2$.
4. **Prova:** Temos que $90 < 97 < 100$ e 97 é primo.

Aula 15

2.1.1 - Demonstração por Exaustão

1. Prove cada uma das proposições seguintes:
   (a) Se $n = 25, 100$ ou 169, então n é um quadrado perfeito e é a soma de dois quadrados perfeitos.
   (b) Se n for um inteiro par tal que $4 \leq n \leq 12$, então n será uma soma de dois números primos.
   (c) Para qualquer inteiro positivo n menor ou igual a 3, temos que $n! < 2^n$.
   (d) Para $2 \leq n \leq 4$, temos que $n^2 \leq 2^n$.

2.2.1 - Prova Direta

1. **Prova**: Suponha $n \in \mathbb{Z}$ um número ímpar. Por definição, $n = 2k+1$ para algum $k \in \mathbb{Z}$.
   Assim, $x^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$ Então $x^3 = 2k' + 1$, onde k' é o número inteiro $4k^3 + 6k^2 + 3k$. Portanto, por definição conclui-se que x^3 é ímpar, c.q.d.
2. **Prova**: Sejam $x, y \in \mathbb{Z}$ e suponha x e y números ímpares, isto é, $x = 2k+1$ e $y = 2k'+1$, para $k, k' \in \mathbb{Z}$.
   Assim, temos que $xy = (2k+1)(2k'+1) = 4kk' + 2k + 2k' + 1 = 2(2kk' + k + k') + 1$. Então $xy = 2t + 1$, onde t é o número inteiro $2kk' + k + k'$. Portanto, por definição conclui-se que xy é ímpar, c.q.d.
3. **Prova**: Sejam $n, m \in \mathbb{Z}$ e suponha que a soma $n + m$ é par. Então, por definição, $n + m = 2k$ para algum $k \in \mathbb{Z}$.
   Assim, temos que $n - m = n + (m - 2m) = (n + m) - 2m = 2k - 2m = 2(k - m)$. Então $n - m = 2t$, onde t é o inteiro $k - m$ e, portanto, $n - m$ é par, c.q.d.
   Note que $m - n = -(n - m)$ e, portanto, também é par.
4. **Prova**: Sejam $n, m \in \mathbb{Z}$ e suponha que n e m são ambos quadrados perfeitos. Então, por definição $n = p^2$ e $m = q^2$, onde $p, q \in \mathbb{Z}$.
   Assim, temos que $n.m = p^2 q^2 = (pq)^2$
   Logo, $nm = k^2$, onde $k = pq$ e um número inteiro. Portanto, nm é um quadrado perfeito, c.q.d.
5. **Prova**: Sejam a e b racionais, isto é, $a = n/m$ e $b = p/q$, onde $n, m, p, q \in \mathbb{Z}$ e $m, q \neq 0$. Temos que

   $$a + b = \frac{n}{m} + \frac{p}{q} = \frac{nq + pm}{mq}$$

   Então $a + b = r/s$, onde $r = nq + pm \in \mathbb{Z}$ e $s = mq \in \mathbb{Z}$, já que o produto e a soma de números inteiros também é um número inteiro. Além disso, $s \neq 0$, pois $m \neq 0$ e $q \neq 0$. Portanto, $(a + b)$ é racional c.q.d.
6. **Prova**: Sejam $a, b, c \in \mathbb{Z}$ e suponha $a|b$ e $a|c$. Pela regra da divisão, existem números inteiros x e y tais que $b = xa$ e $c = ya$.
   Assim, $b + c = xa + ya = (x + y)a$.
   Então, $b + c = ta$ onde $t = (x + y) \in \mathbb{Z}$.
   Portanto, temos que $a|(b + c)$, c.q.d.
7. **Prova:** Sejam $a, b, c \in \mathbb{Z}$.

Suponha que $a|b$ e $b|c$. Por definição, temos que $b = n.a$ e $c = m.b$, para $n,m \in \mathbb{Z}$.

Então, $c = m.b = m.(n.a) = (m.n).a$.

Portanto, temos que $a|c$

8. **Prova**:

   Seja $n \in \mathbb{Z}$. Temos os seguintes casos:

   (a) n é par: Então n^2 é par e, portanto, $5n^2$ é par. Além disso, $3n$ é par. Então, $5n^2 + 3n + 7$ é a soma de dois pares e um ímpar, que é ímpar.

   (b) n é impar: Então n^2 é impar e, portanto, $5n^2$ é impar, pois é o produto de dois impares. Do mesmo modo, $3n$ é impar. Então, $5n^2 + 3n + 7$ é a soma de três impares, que é ímpar.

9. **Prova**:

   Sejam $a,b \in \mathbb{Z}$. Suponha $a|b$, isto é $b = k.a$ para algum $k \in \mathbb{Z}$. Temos que$b^2 = (k.a)^2 = k^2.a^2$, ou seja, $b^2 = ma^2$, onde m é o inteiro k^2, e, portanto, $a^2|b^2$.

10. **Solução:** Temos que, exceto o passo 5, todos os passos estão corretos. O que invalida o passo 5 é a divisão de ambos os lados da igualdade por $(a-b)$, pois partindo da sentença inicial de que $a = b$ temos que $a-b$ é igual a zero.

11. **Solução:** Sejam as proposições $P(x) =$ "n^2 é positivo" e $Q(x) =$"n é positivo" , onde $P(x)$ é a hipótese e $Q(x)$ é a conclusão. A sentença "se n é positivo, então n^2 é positivo" é escrita na forma simbólica por $\forall x[Q(x) \to P(x)]$.

    Da hipótese $P(x)$ e da sentença $\forall x[Q(x) \to P(x)]$, não temos uma regra de inferência válida que permite concluir $Q(x)$. Um contraexemplo, que invalida essa demonstração é dado por $n = -1$, para o qual $n^2 = 1$ é positivo, porém n é negativo.

Aula 16

3.1.1 - Prova por Contraposição

1. **Dados:**

   Sejam $P =$ "x é um número irracional" e $Q =$ "$\sqrt{x}$ é um número irracional". A contrapositiva $(\neg Q \to \neg P)$ é a seguinte afirmação "se $\sqrt{x}$ é um número racional, então x é um número racional."

   Prova por Contraposição:

   Seja $\sqrt{x}$ é um número racional. (negação da conclusão)

   Por definição de número racional, $\sqrt{x} = a/b$ para algum $a,b \in \mathbb{Z}$ e com $b \neq 0$.

   Elevando os dois lados da equação ao quadrado: $(\sqrt{x})^2 = (a/b)^2$

   Por propriedades de potenciação temos: $x = a^2/b^2$

   Seja $c = a^2$ e $d = b^2$, para algum $c,d \in \mathbb{Z}$ e $d \neq 0$, (introdução de novas variáveis)

   Temos que $x = c/d$ é um número racional, negando a hipótese original. Logo, podemos concluir que se x é um número irracional, então $\sqrt{x}$ é um número irracional.

2. **Prova por Contraposição:** Suponha que a é par ou b é par. Se a é par, temos que a^2 é par e, portanto $a^2(b^2-2b)$ é par. Por outro lado, se b é par, temos que b^2 é par e, então (b^2-2b) é par, pois é a diferença entre dois números pares. Então, $a^2(b^2-2b)$ é par. Portanto, pela contrapositiva, se $a^2(b^2-2b)$ é ímpar, então a e b são ambos ímpares.

3. **Prova por Contraposição:** Sabemos que $x^2 \geq 0$. Supondo $x \geq 0$, temos que $5x \geq 0$ e, portanto $x^2 + 5x \geq 0$.

Portanto, se $x^2 + 5x < 0$ então $x < 0$.

4. **Prova por Contraposição:** Vamos provar a contrapositiva: Para todo número inteiro, se n é divisível por 5, então n^2 também é divisível por 5.
   Considere n divisível por 5. Pela definição de divisibilidade, $n = 5k$ para algum $k \in \mathbb{Z}$. Então $n^2 = (5k)^2 = 25k^2 = 5(5k^2)$. Como n^2 é um múltiplo de 5, temos pela definição de divisibilidade que n^2 é divisível por 5. Provando a contrapositiva, podemos afirmar que se n^2 não é divisível por 5, então n não é divisível por 5.
5. A sentença pode ser reescrita como "Para todo x, se x é irracional, então $-x$ também é irracional" e possui a seguinte contrapositiva: "Para todo x , se $-x$ não é irracional, então x não é irracional.
   Prova por Contraposição: suponha que $-x$ seja qualquer número racional. Então por definição $-x = a/b$ para $a, b \in \mathbb{Z}$ e $b \neq 0$.
   Queremos mostrar que x também é racional.
   Multiplicando -1 dos dois lados da equação $-x = a/b$, temos:
   $$(-1)(-x) = (-1)(a/b) \Rightarrow x = (-a)/b$$
   Como tanto $-a$ como b são inteiros e $b \neq 0$, podemos concluir pela definição de número racional que x também é racional.
6. **Prova por Contraposição:**
7. **Prova por Contraposição:**
8. **Prova por Contraposição:**
9. **Prova por Contraposição:**

Aula 17

4.1.1 - Prova por Contradição

1. **Prova por Contradição:** Suponha, por contradição, que $(1 + 3\sqrt{2})$ é racional, isto é existem inteiros a e $b \neq 0$ tais que que
   $$1 + 3\sqrt{2} = \frac{a}{b}$$
   Daí obtemos que
   $$\sqrt{2} = \frac{\frac{a}{b} - 1}{3} = \frac{a - b}{3b}$$
   Então, $\sqrt{2} = c/d$ onde c é o inteiro $(a - b)$ e d é o inteiro não nulo $3b$, e, portanto, $\sqrt{2}$ é racional. Mas isso é absurdo, pois contradiz o que já provamos anteriormente, que $\sqrt{2}$ é racional. Portanto $(1 + 3\sqrt{2})$ é irracional.
2. **Prova por Contradição:**
   Sejam $a, b \in \mathbb{Z}$ e suponha, por contradição, que $a^2 - 4b - 2 = 0$. Então $a^2 = 4b + 2 = 2(2b + 1)$, ou seja, a^2 é par, o que implica que a é par, ou seja, $a = 2k$, para algum $k \in \mathbb{Z}$. Então temos: $(2k)^2 = 4b + 2$, o que implica que $4k = 4b + 2$, ou seja, $b = k - 1/2$, isto é, b não é inteiro. Mas isso contradiz a hipótese que de a e b são inteiros. Portanto, se $a, b \in \mathbb{Z}$, então $a^2 - 4b - 2 \neq 0$.
3. **Prova por Contradição:**

Suponha, por contradição, que o conjunto dos números primos é finito. Então podemos listar todos os números primos como $p_1, p_2, p_3, \ldots, p_n$, onde p_n é o maior número primo. Considere o número $a = (p_1 p_2 p_3 \ldots p_n) + 1$, isto é, a é o produto de todos os números primos mais 1. Então, como todo número natural, a possui um menor divisor primo, e isso significa que $p_k | a$ para algum p_k no nosso conjunto de n números primos. Então, existe um número c tal que $a = cp_k$, ou seja:

$$(p_1 p_2 p_3 \ldots p_n) + 1 = cp_k$$

Dividindo ambos os lados da equação acima por p_k, obtemos

$$(p_1 p_2 p_3 \ldots p_{k-1} p_{k+1} \ldots p_n) + \frac{1}{p_k} = c$$

Então

$$\frac{1}{p_k} = c - (p_1 p_2 p_3 \ldots p_{k-1} p_{k+1} \ldots p_n)$$

A expressão do lado direito dessa equação é um inteiro, mas a expressão do lado esquerdo não é um inteiro, o que é um absurdo. Portanto, o conjunto dos números primos não pode ser finito.

4. **Prova por Contradição:**
   Sejam $a, b, c \in \mathbb{Z}$ e suponha $a^2 + b^2 = c^2$. Suponha, por contradição, que a e b são ambos impares, isto é, $a = 2n + 1$ e $b = 2m + 1$, para alguns inteiros n e m. Então temos que $a^2 + b^2 = (2n+1)^2 + (2m+1)^2 = 4(n^2 + n + m^2 + m) + 2$, e, portanto, o resto da divisão de $(a^2 + b^2)$ por 4 é 2. Por outro lado, vemos que $(a^2 + b^2)$ é par e, portanto, c^2 é par e, consequentemente c é par, ou seja, $c = 2k$, para algum $k \in \mathbb{Z}$. Mas então $c^2 = (2k)^2 = 4k^2$ e, portanto, c^2 é divisível por 4. Mas então não podemos ter $a^2 + b^2 = c^2$, contradizendo nossa hipótese. Portanto, concluímos que $a^2 + b^2 = c^2$, então a ou b é par.
5. **Prova por Contradição:**
   Suponha $a \in \mathbb{Q}$ e $ab \notin \mathbb{Q}$. Suponha, por contradição, que $b \in \mathbb{Q}$. Mas então ab seria racional, porque o produto de dois números racionais é um número racional. Mas isso contradiz a hipótese de que ab é irracional. Portanto, concluímos que se a é racional e ab é irracional, então b é irracional.
6. **Prova por Contradição:**
   Sejam a e b reais positivos e suponha, por contradição, que $a + b \leq 2\sqrt{ab}$. Elevando ao quadrado ambos os lados da inequação, obtemos $(a+b)^2 \leq 4ab$, ou seja $a^2 + 2ab + b^2 \leq 4ab$, isto é $a^2 - 2ab + b^2 \leq 0$. Mas isso é uma contradição, pois $a^2 - 2ab + b^2 = (a-b)^2$ e sabemos que o quadrado que qualquer número real é maior ou igual a zero. Portanto, concluímos que se a e b são números reais positivos, então $a + b \geq 2ab$.
7. **Prova por Contradição:**
   Seja $r \neq 0$ racional, ou seja, $r = \frac{a}{b}$, onde $a, b \in \mathbb{Z}$ e $b \neq 0$. Mas r pode também ser expresso como

$$r = \sqrt{2}\,\frac{r}{\sqrt{2}}$$

Sabemos que $\sqrt{2}$ é racional. Portanto, para concluir a prova basta mostrar que $r/\sqrt{2}$ também é irracional. Para mostrar isso, suponha, por contradição, que $r/\sqrt{2}$ é racional, ou seja, existem inteiros $c \neq 0$ e $d \neq 0$ tais que

$$\frac{r}{\sqrt{2}} = \frac{c}{d}$$

Então

$$\sqrt{2} = r\frac{d}{c} = \frac{a}{b}\frac{d}{c} = \frac{ad}{bc}$$

Isso significa que $\sqrt{2}$ é racional, o que é um absurdo. Portanto, $r/\sqrt{2}$ é irracional. Portanto, $\sqrt{2} \cdot (r/\sqrt{2})$ é um produto de dois números irracionais.

8. A sentença pode ser reescrita como "Para todo x, se x é irracional, então $-x$ também é irracional"

   Prova por Contradição: Seja x um número irracional. Suponha por contradição que $-x$ seja racional.

   Pela definição de racional, $-x = a/b$ para $a, b \in \mathbb{Z}$ e $b \neq 0$. Multiplicando ambos os lados por -1 temos que $x = -(a/b) = -a/b$.

   Como $-a$ e b são inteiros (já que a e b também são) e $b \neq 0$, então pela definição de números racionais podemos afirmar que x é racional. Isso é um absurdo! Pois contradiz a suposição de que x é um número irracional.