Técnicas de Demonstração

Prof. Eanes Torres Pereira

FMCC-2

Roteiro

Introdução

- Os números primos são infinitos?
- A soma de dois números pares é um número par?
- Como saber que um programa está correto?
- Para um positivo inteiro $n \geq 3$, não existem inteiros positivos x, y e z que satisfaçam a equação $x^n + y^n = z^n$ (Último Teorema de Fermat).

Introdução

- Uma prova estabelece a verdade de afirmações matemáticas.
- Um **teorema** é uma afirmação que pode ser mostrada verdadeira.
- Um **lemma** é normalmente um teorema auxiliar utilizado para provar outros teoremas.
- Um **corolário** é um teorema que pode ser estabelecido diretamente de um teorema que foi provado.
- Uma **conjectura** é uma afirmação sendo proposta como verdade, mas que precisa ser provada para virar teorema.

Forma dos Teoremas

Muitos teoremas são apresentados na forma condicional $p \to q$.

Exemplo 1: "Se $x > y$, no qual x e y são números reais positivos, então $x^2 > y^2$".

O que esse teorema realmente significa é:

$$\forall x, y \, (P(x, y) \to Q(x, y))$$

onde

$$P(x, y) \text{ denota } x > y$$
$$Q(x, y) \text{ denota } x^2 > y^2$$

Forma dos Teoremas

- Teoremas também aparecem na forma bi-condicional.
- A implicação deve ser demonstrada nas duas direções.

Preliminares

Considere as definições a seguir para os exemplos que seguem.

Paridade de Números Inteiros

Um inteiro n é *par* se existe um inteiro k tal que $n = 2k$, e n é ímpar se existe um inteiro k tal que $n = 2k + 1$.

Preliminares

Considere as definições a seguir para os exemplos que seguem.

Paridade de Números Inteiros

Um inteiro n é *par* se existe um inteiro k tal que $n = 2k$, e n é ímpar se existe um inteiro k tal que $n = 2k + 1$.

Números Racionais

Um número real r é dito racional se existem inteiros p e q com $q \neq 0$ tal que $r = p/q$. Um número que não é racional é chamado irracional.

Preliminares

Considere as definições a seguir para os exemplos que seguem.

Paridade de Números Inteiros

Um inteiro n é *par* se existe um inteiro k tal que $n = 2k$, e n é ímpar se existe um inteiro k tal que $n = 2k + 1$.

Números Racionais

Um número real r é dito racional se existem inteiros p e q com $q \neq 0$ tal que $r = p/q$. Um número que não é racional é chamado irracional.

Potência Perfeita

Um número inteiro n é dito uma potência perfeita se existem números inteiros $b > 1$ e $k > 1$ tais que $n = b^k$.

Roteiro

Demonstração Exaustiva e por Contra-Exemplo

- Verifica-se a verdade da conjectura para todos os elementos da coleção.
- Para provar a falsidade da conjectura, basta achar um contra-exemplo.

Exemplo 2

Prove a conjectura "Para todo inteiro positivo n, $n! \leq n^2$".

Solução: A conjectura é falsa pois não é verdade para todo n: é falsa para $n = 4$.

n	$n!$	n^2	$n! \leq n^2$
1	1	1	sim
2	2	4	sim
3	6	9	sim
4	24	16	não

Exemplo 3

Prove a conjectura "Para qualquer inteiro positivo menor ou igual a 5, o quadrado do inteiro é menor ou igual à soma de 10 mais 5 vezes o inteiro".

Solução: A conjectura é verdadeira pois

n	n^2	$10+5n$	$n^2 \leq 10+5n$
1	1	15	sim
2	4	20	sim
3	9	25	sim
4	16	30	sim
5	25	35	sim

Exercícios

Exercício 1: Mostre que a afirmação "Todo número inteiro positivo é a soma dos quadrados de dois inteiros" é falsa.

Exercício 2: Mostre que os únicos inteiros positivos consecutivos não excedendo 100 que são potências perfeitas são 8 e 9.

Demonstração por Casos

Uma prova por casos deve cobrir todos os casos possíveis que aparecem em um teorema.

Demonstração por Casos

Uma prova por casos deve cobrir todos os casos possíveis que aparecem em um teorema.

Exemplo 4: Prove que se n é um inteiro, então $n^2 \geq n$.

Demonstração por Casos

Uma prova por casos deve cobrir todos os casos possíveis que aparecem em um teorema.

Exemplo 4: Prove que se n é um inteiro, então $n^2 \geq n$.

(i) Quando $n = 0$. Como $0^2 = 0$, então $n^2 \geq n$ é verdadeiro nesse caso.

Demonstração por Casos

Uma prova por casos deve cobrir todos os casos possíveis que aparecem em um teorema.

Exemplo 4: Prove que se n é um inteiro, então $n^2 \geq n$.

(i) Quando $n = 0$. Como $0^2 = 0$, então $n^2 \geq n$ é verdadeiro nesse caso.

(ii) Quando $n \geq 1$. Multiplicando os dois lados da inequação por n, obtemos

$$n \cdot n \geq n \cdot 1$$

Isso implica que $n^2 \geq n$ para $n \geq 1$.

Demonstração por Casos

Uma prova por casos deve cobrir todos os casos possíveis que aparecem em um teorema.

Exemplo 4: Prove que se n é um inteiro, então $n^2 \geq n$.

(i) Quando $n = 0$. Como $0^2 = 0$, então $n^2 \geq n$ é verdadeiro nesse caso.

(ii) Quando $n \geq 1$. Multiplicando os dois lados da inequação por n, obtemos

$$n \cdot n \geq n \cdot 1$$

Isso implica que $n^2 \geq n$ para $n \geq 1$.

(iii) Quando $n \leq -1$. Como $n^2 \geq 0$ segue que $n^2 \geq n$. $\square$

Exercícios

Exercício 3: Mostre que se x ou y forem inteiros pares, então xy é par.

Exercício 4: Mostre que se x e y são números reais, então

$$\max(x, y) + \min(x, y) = x + y$$

Roteiro

Demonstração Direta

A demonstração direta de uma afirmação da forma $p \rightarrow q$:

1. assume que o antecedente p é verdadeiro e daí;
2. deduz a conclusão q.

Normalmente usa-se axiomas, definições, lemmas e teoremas, em conjunto com regras de inferência, para mostrar que q também deve ser verdade.

Exemplo 5

Prove o seguinte teorema:

"se n é um número inteiro ímpar, então n^2 também é ímpar."

Exemplo 5

Prove o seguinte teorema:

"se n é um número inteiro ímpar, então n^2 também é ímpar."

Solução:

1. Como n é ímpar, $n = 2k + 1$ para $k \in \mathbb{Z}$ (pela definição).
2. Elevando os dois lados da igualdade ao quadrado, $n^2 = (2k + 1)^2$, temos

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

3. Portanto concluimos que n^2 também é ímpar.$\square$

Exemplo 6

Prove que o produto de dois números inteiros pares é par.

Exemplo 6

Prove que o produto de dois números inteiros pares é par.

Solução:

1. Como x e y são pares, $x = 2m$ e $y = 2n$ para $m, n \in \mathbb{Z}$ (pela definição).
2. Como
$$xy = (2m)(2n) = 2(2mn)$$
que por definição é um número par, provamos o teorema.

□

Exercícios

- **Exercício 5:** Dê uma demonstração direta ao teorema "Se um inteiro é divisível por 6, então duas vezes esse inteiro é divisível por 4".
- **Exercício 6:** Prove que se m e n são ambos quadrados perfeitos, então nm também é um quadrado perfeito.
- **Exercício 7:** Mostre que o produto de um número ímpar com um número par é um número par.

Roteiro

Demonstração por Contraposição

Uma conjectura da forma $p \rightarrow q$ pode ser provada mostrando-se a sua contrapositiva

$$\neg q \rightarrow \neg p$$

Exemplo 7

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

Exemplo 7

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

Solução: Primeiro assumimos que n é par (a negação que n é ímpar), ou seja, $n = 2k$. Agora basta verificar que $3n + 2$ também é par:

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

$\square$

Exercício 8

Mostre que se $n \in \mathbb{Z}$ e n^2 é ímpar, então n é ímpar.

Exemplo 8

Mostre que se $n = ab$, no qual a e b são inteiros positivos, então $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$.

Exemplo 8

Mostre que se $n = ab$, no qual a e b são inteiros positivos, então $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$.

Solução:

1. Pela contrapositiva temos

$$\neg(a \leq \sqrt{n} \vee b \leq \sqrt{n}) \rightarrow (n \neq ab)$$

2. Por De'Morgan:

$$\neg(a \leq \sqrt{n} \vee b \leq \sqrt{n}) \equiv a > \sqrt{n} \wedge b > \sqrt{n}$$

3. Multiplicando as desigualdades temos:

$$ab > (\sqrt{n})^2 = n$$

4. Como $ab > n \rightarrow ab \neq n$, Q.E.D.

Exercício 9

Prove que o número n é um inteiro ímpar se, e somente se,

$$3n + 5 = 6k + 8$$

para algum inteiro k.

Note que como se trata de uma implicação bicondicional, você deve provar os dois lados da implicação:

i "Se n é um inteiro ímpar, então $3n + 5 = 6k + 8$ para algum inteiro k."

ii "Se $3n + 5 = 6k + 8$ para algum inteiro k, então n é um inteiro ímpar ."

Roteiro

Demonstração por Absurdo

- Para demonstrar p, assumimos $\neg p$ e mostramos que isso leva a uma contradição.
- Para provar $p \to q$, basta mostrar $p \wedge \neg q \to \mathbf{F}$.

Exemplo 9

Mostre que se um número qualquer somado a ele mesmo resulta nele mesmo, então esse número é 0.

Solução:

1. Tentamos mostrar que

$$[(x + x = x) \wedge (x \neq 0)] \rightarrow \mathbf{F}$$

   onde x é um número qualquer.

2. Como $x \neq 0$, então ambos os lados da equação $2x = x$ podem ser divididos por x, dando $2 = 1$, o que é um absurdo.

Exemplo 10

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

Exemplo 10

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

Solução:

- Vamos assumir que $3n + 2$ é ímpar e n é par.
- Vimos no Exemplo 7 que se n é par então $3n + 2$ é par.
- Por contradição n tem que ser ímpar.

$\square$

Exercícios

- **Exercício 8:** Mostre por absurdo que $\sqrt{2}$ é um número irracional.
- **Exercício 9:** Mostre por absurdo que existem infinitos números primos.

Roteiro

Provas de Existência

- Muitos teoremas são da forma $\exists x\, P(x)$.
- Formas de provar:
  - Provas **construtivas:** encontrar elemento a tal que $P(a)$.
  - Provas **não construtivas:** provar que $\exists x\, P(x)$ é verdade de alguma outra forma.

Exemplo 11

Mostre que existe um inteiro positivo que pode ser escrito como a soma de cubos de inteiros positivos de duas formas diferentes.

Solução:

- Após uma busca computacional, descobrimos que:

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

$\square$

Erros em Demonstrações

Há muitos erros comuns na construção de demonstrações, e.g., falácias e erros de aritmética.

Exemplo 12: O que está errado com a prova abaixo?

Passo	**Justificativa**
1. $a = b$	Dados dois inteiros positivos iguais
2. $a^2 = ab$	Multiplica ambos os lados de (1) por a
3. $a^2 - b^2 = ab - b^2$	Subtrai b^2 de ambos os lados de (2)
4. $(a - b)(a + b) = b(a - b)$	Fatoriza ambos os lados de (3)
5. $a + b = b$	Divide ambos os lados de (4) por $a - b$
6. $2b = b$	Substitui a por b em (5) já que $a = b$ e simplifica
7. $2 = 1$	Divide ambos os lados de (6) por b

Referências

- Keneth H. Rosen. Discrete Mathematics and Its Applications. Sexta Edição. McGRAW-HILL International Edition, 2007.
- Judith L. Gersting. Fundamentos Matemáticos para a Ciência da Computação. Quinta Edição. LTC, 2004.
- Leandro Balby Marinho. Slides fornecidos de anos anteriores, 2013.