Técnicas de demonstração

Prof. Adriano Barbosa

02/10/2024

Prova direta

Em matemática os resultados usualmente aparecem na forma

$$p \to q$$

ou

$$p \leftrightarrow q$$

Prova direta

Em matemática os resultados usualmente aparecem na forma

$$p \to q$$

ou

$$p \leftrightarrow q$$

Para provar $p \to q$, assumimos que p é verdadeira e usamos axiomas, definições, regras lógicas e resultados provados anteriormente para concluir q.

Prova direta

Exemplo: Se n é par, então n^2 é par.

1. Hipótese: n é um número par.

Prova direta

Exemplo: Se n é par, então n^2 é par.

1. Hipótese: n é um número par.
2. Definição de número par: $\exists k \in \mathbb{Z}$ tal que $n = 2k$.

Prova direta

Exemplo: Se n é par, então n^2 é par.

1. Hipótese: n é um número par.
2. Definição de número par: $\exists k \in \mathbb{Z}$ tal que $n = 2k$.
3. Definição de quadrado de um número: $n^2 = n \cdot n$.

Prova direta

Exemplo: Se n é par, então n^2 é par.

1. Hipótese: n é um número par.
2. Definição de número par: $\exists k \in \mathbb{Z}$ tal que $n = 2k$.
3. Definição de quadrado de um número: $n^2 = n \cdot n$.
4. Juntando 2 e 3: $n^2 = (2k)(2k)$, com $k \in \mathbb{Z}$.

Prova direta

Exemplo: Se n é par, então n^2 é par.

1. Hipótese: n é um número par.
2. Definição de número par: $\exists k \in \mathbb{Z}$ tal que $n = 2k$.
3. Definição de quadrado de um número: $n^2 = n \cdot n$.
4. Juntando 2 e 3: $n^2 = (2k)(2k)$, com $k \in \mathbb{Z}$.
5. Associatividade dos números inteiros: $n^2 = 2(k2k)$.

Prova direta

Exemplo: Se n é par, então n^2 é par.

1. Hipótese: n é um número par.
2. Definição de número par: $\exists k \in \mathbb{Z}$ tal que $n = 2k$.
3. Definição de quadrado de um número: $n^2 = n \cdot n$.
4. Juntando 2 e 3: $n^2 = (2k)(2k)$, com $k \in \mathbb{Z}$.
5. Associatividade dos números inteiros: $n^2 = 2(k2k)$.
6. $k2k$ é inteiro: $n^2 = 2m$, com $m \in \mathbb{Z}$.

Prova direta

Exemplo: Se n é par, então n^2 é par.

1. Hipótese: n é um número par.
2. Definição de número par: $\exists k \in \mathbb{Z}$ tal que $n = 2k$.
3. Definição de quadrado de um número: $n^2 = n \cdot n$.
4. Juntando 2 e 3: $n^2 = (2k)(2k)$, com $k \in \mathbb{Z}$.
5. Associatividade dos números inteiros: $n^2 = 2(k2k)$.
6. $k2k$ é inteiro: $n^2 = 2m$, com $m \in \mathbb{Z}$.
7. Definição de número par: n^2 é par.

Prova direta

Exemplo: Se n é par, então n^2 é par.

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

$$n^2 = n \cdot n = (2k)(2k) = 2(k2k) = 2m, \text{ onde } m = k2k$$

Como $2, k \in \mathbb{Z}$, $m = k2k \in \mathbb{Z}$. Portanto, $n^2 = 2m$, para algum $m \in \mathbb{Z}$, ou seja, n^2 é par.

Prova pela contrapositiva

$\sim q \to \sim p$ é dita a forma contrapositiva de $p \to q$.

Prova pela contrapositiva

$\sim q \to \sim p$ é dita a forma contrapositiva de $p \to q$.

$$p \to q \equiv \sim q \to \sim p$$

p	q	$p \to q$	$\sim p$	$\sim q$	$\sim q \to \sim p$
V	V	V	F	F	V
V	F	F	F	V	F
F	V	V	V	F	V
F	F	V	V	V	V

Prova pela contrapositiva

$\sim q \to \sim p$ é dita a forma contrapositiva de $p \to q$.

$$p \to q \equiv \sim q \to \sim p$$

p	q	$p \to q$	$\sim p$	$\sim q$	$\sim q \to \sim p$
V	V	V	F	F	V
V	F	F	F	V	F
F	V	V	V	F	V
F	F	V	V	V	V

Assumimos $\sim q$ verdadeira e usamos definições, axiomas, resultados já provados para concluir $\sim p$.

Prova pela contrapositiva

Exemplo: Se n^2 é par, então n é par.

Contrapositiva: Se n não é par, então n^2 não é par.
Versão melhor: Se n é ímpar, então n^2 é ímpar.

Prova pela contrapositiva

Exemplo: Se n^2 é par, então n é par.

Contrapositiva: Se n não é par, então n^2 não é par.
Versão melhor: Se n é ímpar, então n^2 é ímpar.

Se n é ímpar, existe $k \in \mathbb{Z}$ tal que $n = 2k + 1$. Assim,

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

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

$$= 2m + 1, \text{ onde } m = 2k^2 + 2k.$$

Como $2, k \in \mathbb{Z}$, $m \in \mathbb{Z}$. Portanto, $n^2 = 2m + 1$, com $m \in \mathbb{Z}$, ou seja, n^2 é ímpar.

Prova por absurdo

$$p \to q \equiv p \wedge \sim q \to c$$

p	q	$p \to q$	$\sim q$	$p \wedge \sim q$	$p \wedge \sim q \to c$
V	V	V	F	F	V
V	F	F	V	V	F
F	V	V	F	F	V
F	F	V	V	F	V

Prova por absurdo

$$p \to q \equiv p \wedge \sim q \to c$$

p	q	$p \to q$	$\sim q$	$p \wedge \sim q$	$p \wedge \sim q \to c$
V	V	V	F	F	V
V	F	F	V	V	F
F	V	V	F	F	V
F	F	V	V	F	V

Assumimos p e $\sim q$ verdadeiras e usamos definições, axiomas, resultados já provados para obter uma contradição.

Prova por absurdo

Exemplo: Se n^2 é ímpar, então n é ímpar.

$p : n^2$ é ímpar, $\quad q : n$ é ímpar
$p : n^2$ é ímpar, $\quad \sim q : n$ é par

Prova por absurdo

Exemplo: Se n^2 é ímpar, então n é ímpar.

$p : n^2$ é ímpar, $\quad q : n$ é ímpar
$p : n^2$ é ímpar, $\quad \sim q : n$ é par

Suponha n^2 ímpar e n par, então existe $k \in \mathbb{Z}$ tal que $n = 2k$. Assim,

$$n^2 = n \cdot n = (2k)(2k) = 2(k2k) = 2m, \text{ onde } m = k2k.$$

Como $2, k \in \mathbb{Z}$, $m \in \mathbb{Z}$. Portanto, n^2 é par, um absurdo, pois assumimos n^2 é ímpar.

Exercícios

Sejam m e n inteiros. Se $m+n$ é par, então m e n são ambos pares ou ímpares.

Exercícios

Sejam m e n inteiros. Se $m+n$ é par, então m e n são ambos pares ou ímpares.

Contrapositiva: $m, n \in \mathbb{Z}$. Se m e n não são ambos pares nem ambos ímpares, então $m+n$ não é par.
Forma alternativa: $m, n \in \mathbb{Z}$. Dados m e n, um par e outro ímpar, então $m+n$ é ímpar.

Exercícios

Sejam m e n inteiros. Se $m+n$ é par, então m e n são ambos pares ou ímpares.

Contrapositiva: $m, n \in \mathbb{Z}$. Se m e n não são ambos pares nem ambos ímpares, então $m+n$ não é par.
Forma alternativa: $m, n \in \mathbb{Z}$. Dados m e n, um par e outro ímpar, então $m+n$ é ímpar.

Sem perda de generalidade, suponha m par e n ímpar, então existem $r, s \in \mathbb{Z}$ tais que $m = 2r$ e $n = 2s+1$. Assim,

$$m + n = 2r + (2s+1) = 2(r+s) + 1 = 2t + 1, \text{ onde } t = r + s.$$

Como $r, s \in \mathbb{Z}$, $t \in \mathbb{Z}$. Portanto, $m+n = 2t+1$, para algum $t \in \mathbb{Z}$, ou seja, $m+n$ é ímpar.

Exercícios

Se n é um inteiro ímpar, então $5n-3$ é par.

Prova direta:

Exercícios

Se n é um inteiro ímpar, então $5n - 3$ é par.

Prova direta:
Se n é ímpar, existe $k \in \mathbb{Z}$ tal que $n = 2k + 1$, logo

$5n-3 = 5(2k+1)-3 = 10k+5-3 = 10k+2 = 2(5k+1) = 2m, m \in \mathbb{Z}.$

Portanto, $5n - 3$ é par.

Exercícios

Se n é um inteiro ímpar, então $5n - 3$ é par.

Prova pela contrapositiva:

Exercícios

Se n é um inteiro ímpar, então $5n - 3$ é par.

Prova pela contrapositiva:
Supondo $5n - 3$ ímpar, existe $k \in \mathbb{Z}$ tal que $5n - 3 = 2k + 1$.
Mostremos que n é par.

$n = 5n-4n = 5n-4n+3-3 = 5n-3-4n+3 = 2k+1-4n+3$

$= 2k - 4n + 4 = 2(k - 2n + 2) = 2m, m \in \mathbb{Z}.$

Portanto, n é par.

Exercícios

Se n é um inteiro ímpar, então $5n - 3$ é par.

Prova por absurdo:

Exercícios

Se n é um inteiro ímpar, então $5n - 3$ é par.

Prova por absurdo:
Supondo n ímpar e $5n - 3$ ímpar, existe $k \in \mathbb{Z}$ tal que $n = 2k + 1$.
Logo,

$5n-3 = 5(2k+1)-3 = 10k+5-3 = 10k+2 = 2(5k+1) = 2m, m \in \mathbb{Z}$.

Assim, $5n - 3$ á par, um absurdo!

Exercícios

Seja p um número primo. Mostre que $\sqrt{p}$ é irracional.

Exercícios

Seja p um número primo. Mostre que $\sqrt{p}$ é irracional.

Suponha $\sqrt{p} \in \mathbb{Q}$, logo existem $m \in \mathbb{Z}$ e $n \in \mathbb{N}$ tais que $\sqrt{p} = \frac{m}{n}$ é irredutível. Assim,

$$\sqrt{p} = \frac{m}{n} \Rightarrow p = \frac{m^2}{n^2} \Rightarrow m^2 = pn^2.$$

A decomposição em primos de m^2 e n^2 têm número par de fatores p, mas pn^2 número ímpar de fatores p, logo m^2 não pode ser igual a $2n^2$.

Exercícios

Sejam $x, y \in \mathbb{R}$ tais que $y^3 + yx^2 \leq x^3 + xy^2$. Prove que $y \leq x$.

Exercícios

Sejam $x, y \in \mathbb{R}$ tais que $y^3 + yx^2 \leq x^3 + xy^2$. Prove que $y \leq x$.

Suponha que $y > x$. Vamos mostrar que $y^3 + yx^2 > x^3 + xy^2$.

Exercícios

Sejam $x, y \in \mathbb{R}$ tais que $y^3 + yx^2 \leq x^3 + xy^2$. Prove que $y \leq x$.

Suponha que $y > x$. Vamos mostrar que $y^3 + yx^2 > x^3 + xy^2$. Como $y > x$, temos que $y - x > 0$.

$$\begin{aligned} y^3 + yx^2 - x^3 - xy^2 &= (y^3 - x^3) + (x^2y - xy^2) \\ &= (y - x)(y^2 + yx + x^2) + xy(x - y) \\ &= (y - x)(y^2 + yx + x^2) - xy(y - x) \\ &= (y - x)[(y^2 + yx + x^2) - xy] \\ &= (y - x)(y^2 + x^2). \end{aligned}$$

Sabemos que $x^2, y^2 \geq 0$, logo $y^2 + x^2 \geq 0$. Mas, $y^2 + x^2 = 0 \Rightarrow y^2 = x^2 = 0 \Rightarrow y = x = 0$. Entretanto, estamos suponto $y > x$. Portanto, $y^2 + x^2 > 0$ e, como $y - x > 0$, temos

$$y^3 + yx^2 - x^3 - xy^2 = (y - x)(y^2 + x^2) > 0$$
$$\Rightarrow y^3 + yx^2 > x^3 + xy^2.$$

Exercícios

Mostre que existe um número infinito de números primos.

Exercícios

Mostre que existe um número infinito de números primos.

Suponha que o conjunto dos números primos seja finito.

Exercícios

Mostre que existe um número infinito de números primos.

Suponha que o conjunto dos números primos seja finito.
Seja $P = \{2, 3, 5 \ldots, p\}$ o conjunto dos números primos. Considere o número $n = 2 \cdot 3 \cdot \ldots \cdot p + 1$:

- Ou n é primo, logo temos um primo que não está em P. Absurdo!
- Ou n é composto, logo existe um primo q que divide n. Se $q \in P$, temos que q divide o produto $2 \cdot 3 \cdot \ldots \cdot p$, logo q também divide a diferença $n - 2 \cdot 3 \cdot \ldots \cdot p = 1$, ou seja, $q = 1$. O que não pode acontecer, pois q é primo. Portanto, existe um primo $q \notin P$. Absurdo!

Exercícios

mn é par se, e somente se, m é par ou n é par.

Exercícios

mn é par se, e somente se, m é par ou n é par.

($\Rightarrow$) Mostremos que se m e n são ímpares, então mn é ímpar. Supondo m e n ímpares, existem $r, s \in \mathbb{Z}$ tais que $m = 2r + 1$ e $n = 2s + 1$. Logo,

$mn = (2r+1)(2s+1) = 4rs+2r+2s+1 = 2(2rs+r+s)+1 = 2t+1.$

Como $t = 2rs + r + s \in \mathbb{Z}$, temos que mn é ímpar.

Exercícios

mn é par se, e somente se, m é par ou n é par.

($\Rightarrow$) Mostremos que se m e n são ímpares, então mn é ímpar. Supondo m e n ímpares, existem $r, s \in \mathbb{Z}$ tais que $m = 2r + 1$ e $n = 2s + 1$. Logo,

$mn = (2r+1)(2s+1) = 4rs+2r+2s+1 = 2(2rs+r+s)+1 = 2t+1.$

Como $t = 2rs + r + s \in \mathbb{Z}$, temos que mn é ímpar.

($\Leftarrow$) Sem perda de generalidade, suponha m par, $m = 2k, k \in \mathbb{Z}$.

$$mn = (2k)n = 2(kn) = 2t, t \in \mathbb{Z}.$$

Portanto, mn é par.

Exercícios

Para qualquer $n \in \mathbb{N}$, existe uma sequência de n números naturais consecurivos sem primo algum.

Exercícios

Para qualquer $n \in \mathbb{N}$, existe uma sequência de n números naturais consecurivos sem primo algum.

Seja $x = (n+1)! + 2$. A sequência $x, x+1, x+2, \ldots, x+(n-1)$ é composta por n naturais consegurivos. Observe que

$$x + i = (n+1)! + 2 + i = (n+1) \cdot n \cdot \ldots 3 \cdot 2 + (2+i)$$

$$= (2+i)[(n+1) \cdot n \cdot \ldots \cdot (3+i) \cdot (1+i) \cdot \ldots \cdot 3 \cdot 2 + 1].$$

Portanto, qualquer um dos n números da sequência é divisível por algum $2+i$, $0 \leq i \leq n-1$.

Conjecturas e contraexemplos

Se a divide $b+c$, então a divide b ou a divide c.

Conjecturas e contraexemplos

Se a divide $b+c$, então a divide b ou a divide c.

$$p : a \text{ divide } b+c, \quad q : a \text{ divide } b, \quad r : a \text{ divide } c$$

$$p \rightarrow (q \vee r)$$

Conjecturas e contraexemplos

Se a divide $b+c$, então a divide b ou a divide c.

$$p : a \text{ divide } b+c, \quad q : a \text{ divide } b, \quad r : a \text{ divide } c$$

$$p \to (q \vee r)$$

O condicional é falso apenas quando p é verdadeira e $q \vee r$ é falsa. Para falsear a afirmação, basta buscar a, b e c tais que p seja verdadeira e $\sim(q \vee r)$ seja falsa ou, equivalentemente, que p e $\sim q \wedge \sim r$ sejam ambas verdadeiras.

Conjecturas e contraexemplos

Se a divide $b+c$, então a divide b ou a divide c.

$$p : a \text{ divide } b+c, \quad q : a \text{ divide } b, \quad r : a \text{ divide } c$$

$$p \to (q \vee r)$$

O condicional é falso apenas quando p é verdadeira e $q \vee r$ é falsa. Para falsear a afirmação, basta buscar a, b e c tais que p seja verdadeira e $\sim(q \vee r)$ seja falsa ou, equivalentemente, que p e $\sim q \wedge \sim r$ sejam ambas verdadeiras.
Tomando $a = 2$, $b = 3$ e $c = 5$, temos que a não divide b, a não divide c e a divide $b+c$. Portanto, a afirmação é falsa.

Conjecturas e contraexemplos

Seja $f(n) = n^2 + n + 41$. Para todo inteiro n, $f(n)$ é um número primo.

Conjecturas e contraexemplos

Seja $f(n) = n^2 + n + 41$. Para todo inteiro n, $f(n)$ é um número primo.

n	$f(n) = n^2 + n + 41$
1	$1^2 + 1 + 41 = 43$
2	$2^2 + 2 + 41 = 47$
3	$3^2 + 3 + 41 = 53$
4	$4^2 + 4 + 41 = 61$
5	$5^2 + 5 + 41 = 71$
6	$6^2 + 6 + 41 = 83$
7	$7^2 + 7 + 41 = 97$

Conjecturas e contraexemplos

Seja $f(n) = n^2 + n + 41$. Para todo inteiro n, $f(n)$ é um número primo.

n	$f(n) = n^2 + n + 41$
1	$1^2 + 1 + 41 = 43$
2	$2^2 + 2 + 41 = 47$
3	$3^2 + 3 + 41 = 53$
4	$4^2 + 4 + 41 = 61$
5	$5^2 + 5 + 41 = 71$
6	$6^2 + 6 + 41 = 83$
7	$7^2 + 7 + 41 = 97$

$f(40) = 1681 = 41^2$ não é primo!

$f(41) = 41^2+41+41 = 41(41+1+1) = 41{\cdot}43$ também não é primo.

Conjecturas antigas

Conjectura de Goldbach (1742): qualquer número par maior do que 2 pode ser escrito como soma de dois primos.

Conjecturas antigas

Conjectura de Goldbach (1742): qualquer número par maior do que 2 pode ser escrito como soma de dois primos.

Número Par	**Soma de Primos**
4	$2 + 2$
6	$3 + 3$
8	$3 + 5$
10	$5 + 5$
12	$5 + 7$
14	$7 + 7$
16	$5 + 11$
18	$7 + 11$
20	$3 + 17$

Conjecturas antigas

Conjectura de Goldbach (1742): qualquer número par maior do que 2 pode ser escrito como soma de dois primos.

Número Par	**Soma de Primos**
4	$2 + 2$
6	$3 + 3$
8	$3 + 5$
10	$5 + 5$
12	$5 + 7$
14	$7 + 7$
16	$5 + 11$
18	$7 + 11$
20	$3 + 17$

Continua sem demonstração, mesmo sendo verificada computacionalmente até, pelo menos, $4 \cdot 10^{14}$.

Conjecturas antigas

Conjectura dos primso gêmeos: existem infinitos pares de primos cuja diferença é 2.

Conjecturas antigas

Conjectura dos primso gêmeos: existem infinitos pares de primos cuja diferença é 2.

$$(3,5),(11,13),(17,19),(29,31),(41,43),(59,61),(71,73),\ldots$$

$$(1319,1321),(1607,1609),\ldots,(4001,4003),(4157,4159),\ldots$$

20 / 20

Conjecturas antigas

Conjectura dos primso gêmeos: existem infinitos pares de primos cuja diferença é 2.

$(3,5),(11,13),(17,19),(29,31),(41,43),(59,61),(71,73),\ldots$

$(1319,1321),(1607,1609),\ldots,(4001,4003),(4157,4159),\ldots$

Também é um problema em aberto.

20 / 20