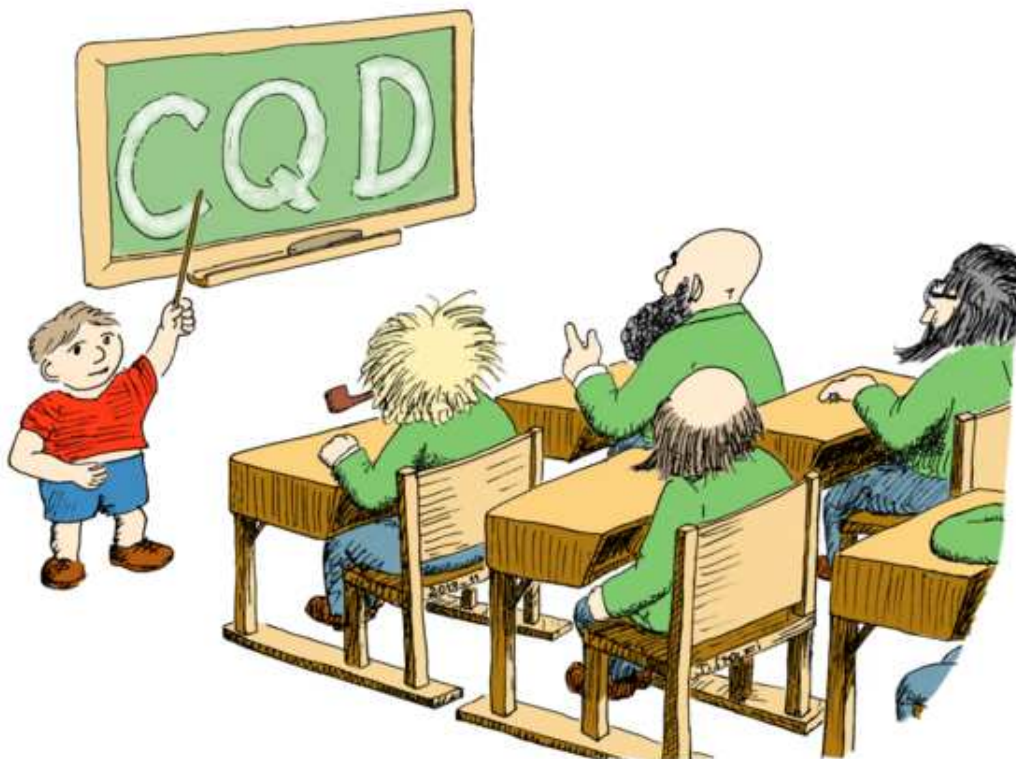


se a vale então b tem que valer

	ou	E	neg.	implicação	xor	
a	b	$a \vee b$	$a \wedge b$	$\sim a$	$a \Rightarrow b$	$a \oplus b$
V	V	V	V	F	V	F
V	F	V	F	F	F	V
F	V	V	F	V	V	V
F	F	F	F	V	V	F

Capítulo 4

Métodos de Demonstração



4.1 Introdução

para verificar que

Como vimos no capítulo 1, demonstrações são instrumentos usados por uma pessoa para convencer outras pessoas (ou a si mesma) de que uma afirmação é verdadeira. Toda demonstração precisa partir de algumas definições e/ou afirmações básicas — chamadas axiomas ou postulados — que ambas as partes aceitam como verdadeiras, e/ou afirmações que foram previamente demonstradas.

Para ser convincente, uma demonstração somente pode usar afirmações e regras de raciocínio que

a	b	$a \Rightarrow b$
V	V	V
V	F	F
F	V	V
F	F	V

 $a \Rightarrow b$

as duas partes consideram válidas. Em geral, podem ser usadas as equivalências e implicações lógicas vistas nos capítulos anteriores. Entre pessoas que pelo menos iniciaram um curso superior de ciência ou engenharia, em particular, podem também ser usadas as regras de manipulação de fórmulas da álgebra e da teoria de conjuntos.

Uma afirmação devidamente demonstrada é chamada de teorema (palavra derivada de uma expressão grega que significa “verdade dos Deuses”). Um teorema que é demonstrado apenas para ajudar na prova de um outro teorema é chamado de lema. Um corolário de um teorema é outro teorema que é consequência do primeiro, e cuja demonstração é relativamente simples.

4.1.1 Definições

Uma demonstração também pode usar definições que tenham sido feitas previamente. De modo geral, uma definição introduz no escopo da discussão um novo predicado, e uma fórmula lógica equivalente ao mesmo. Por convenção, as palavras que representam o novo predicado são enfatizadas na definição. Por exemplo:

Definição 4.1: Um inteiro n é um múltiplo de um inteiro p se, e somente se, existe um inteiro q tal que $n = pq$.

Esta definição introduz um novo predicado “é múltiplo de”, que, na notação formal, podemos denotar (por exemplo) por M . Neste caso, $M(n, p)$ é lido “ n é múltiplo de p ”. A parte que vem depois do “se, e somente se” seria escrita formalmente “ $(\exists q \in \mathbb{Z}) n = pq$ ”. Assim, depois de enunciarmos esta definição, podemos tratar a fórmula

$$(\forall n, p \in \mathbb{Z}) M(n, p) \leftrightarrow (\exists q \in \mathbb{Z}) n = pq \quad (4.1)$$

como um axioma, ou supor que $M(n, p)$ é logicamente equivalente a $(\exists q \in \mathbb{Z}) n = pq$. Em particular, podemos trocar qualquer sub-fórmula $M(\mathcal{E}, \mathcal{F})$, onde \mathcal{E} e \mathcal{F} são fórmulas com valores inteiros, por $(\exists q \in \mathbb{Z}) (\mathcal{E}) = (\mathcal{F}) q$, ou vice-versa; sem que isso quebre a equivalência lógica.

Mesmo quando escrita em linguagem natural, uma definição precisa ser completa, isto é, deve especificar todas as propriedades que identificam exatamente o predicado em questão. Deve ser também precisa, de modo que o leitor não tenha dúvidas sobre o valor lógico do predicado, quando ele se aplica.

Observe que para quaisquer inteiros n e p , tanto a definição 4.1 quanto o axioma (4.1) determinam, sem ambiguidade, se n é ou não múltiplo de p .

Por outro lado, da maneira como está escrita, a definição 4.1 só vale no domínio dos inteiros. Será o número π um múltiplo de $\sqrt{17}$? A definição 4.1 não diz nem que sim, nem que não. Enquanto o conceito de “múltiplo” não for definido para esses números, essa frase (ou a fórmula $M(\pi, \sqrt{17})$) não tem sentido: ela não é nem verdadeira nem falsa, e portanto não é uma proposição lógica.

Observe também que, na parte da definição 4.1 que descreve o sentido do predicado, as variáveis n e p são livres, enquanto que q está amarrada no quantificador “existe”.

Uma vez que um conceito foi definido, ele pode ser usado em outras definições:

Definição 4.2: Um inteiro p divide um inteiro n (é um *divisor* de n) se, e somente se, n é múltiplo de p .

Esta definição introduz um predicado “é divisor de” em termos do predicado “é múltiplo de”. Formalmente, se denotarmos esse predicado por D , ela introduz o axioma

$$(\forall p, n \in \mathbb{Z}) D(p, n) \leftrightarrow M(n, p) \quad (4.2)$$

Observe o uso do conectivo lógico “se e somente se” (\leftrightarrow) nestas definições. Este conectivo permite ao leitor decidir se uma entidade qualquer do domínio se enquadra *ou não* na definição. Portanto, toda definição deve ser uma afirmação da forma “se e somente se”.

Entretanto, em textos matemáticos e técnicos é comum encontrar definições que usam apenas a palavra “se” quando o autor na verdade quer dizer “se e somente se.” Por exemplo:

Definição 4.3: Um inteiro é *par* se ele é múltiplo de 2.

Esta definição deve ser entendida como “um inteiro é par se, e somente se, ele é múltiplo de 2”. Formalmente, ela introduz um predicado P , tal que $P(n)$ é lido “ n é um inteiro par”, e o axioma $(\forall n \in \mathbb{Z}) P(n) \leftrightarrow M(n, 2)$. Eis outro exemplo:

Definição 4.4: Se um inteiro não é par, dizemos que ele é *ímpar*.

Formalmente, esta definição introduz um predicado I , tal que $I(n)$ é lido “ n é ímpar”, e o axioma $(\forall n \in \mathbb{Z}) I(n) \leftrightarrow \neg P(n)$

Há outros formatos de definição que não usam nem “se” nem “se e somente se”. Por exemplo:

Definição 4.5: Um *número primo* é um número inteiro maior que 1, que não tem nenhum divisor exceto 1 e ele mesmo.

Esta definição deve ser lida “ n é um número primo se, e somente se, n é um número inteiro, n é maior que 1, e não existe nenhum d que seja divisor de n e diferente de 1 e de n .” Formalmente, se R representa o predicado “é primo”, esta definição introduz o axioma

$$(\forall n) R(n) \leftrightarrow (n \in \mathbb{Z} \wedge n > 1 \wedge \neg((\exists d) D(d, n) \wedge d \neq 1 \wedge d \neq n))$$

Definições equivalentes

Por vezes, equivalências são mais claras em um sentido

Em geral há muitas maneiras diferentes de definir o mesmo conceito. Por exemplo, em vez da definição 4.4 podemos dizer

Definição 4.6: Um inteiro n é ímpar se existe um inteiro k tal que $n = 2k + 1$.

Ou então

Definição 4.7: Um inteiro n é ímpar se existe um inteiro par m tal que $n = m + 1$.

Formalmente, os predicados I , I_2 , e I_3 introduzidos pelas definições 4.4, 4.6 e 4.7 são o mesmo predicado; isto é, $(\forall n) I(n) \leftrightarrow I_2(n)$, e $(\forall n) I_2(n) \leftrightarrow I_3(n)$. Porém, estas equivalências não são inteiramente óbvias, e podem precisar de demonstrações.

$$\begin{aligned} \text{Ex.: } (x+y)^2 &= x^2 + 2xy + y^2 \\ (x+y)^3 &= x^3 + 3x^2y + \\ &\quad 3xy^2 + y^3 \end{aligned}$$

4.1.2 Conjecturas

Uma conjetura (ou conjectura) é uma afirmação para a qual ainda não existe prova. Em geral, este termo é usado quando se suspeita que a afirmação seja verdadeira. Se uma conjetura é finalmente demonstrada, ela se torna um teorema. Por outro lado, se for encontrada uma demonstração da negação da conjetura, dizemos que a mesma foi refutada. Enquanto nenhuma das duas coisas ocorre, diz-se que a conjetura continua aberta.

Um exemplo famoso é a conjetura de Fermat: “se $n > 2$, a equação $x^n + y^n = z^n$ não tem soluções inteiras positivas.” Esta conjetura foi encontrada em um livro que pertenceu ao matemático Pierre de Fermat (1601–1665), que escreveu na margem “tenho uma linda demonstração, mas ela não cabe nesta margem.” Apesar de inúmeros esforços por matemáticos de todo o mundo, a afirmação permaneceu como conjetura por mais de 300 anos. Em 1995, finalmente, o matemático inglês Andrew Wiles publicou uma demonstração com mais de 200 páginas. Hoje a conjetura é conhecida como o último teorema de Fermat.

Outro exemplo famoso é a conjetura das quatro cores: “todo mapa pode ser pintado com no máximo quatro cores, de modo que países vizinhos tenham cores diferentes.” Esta conjetura foi enunciada em 1852 por Francis Guthrie (1831–1899), mas somente foi provada em 1976 por Kenneth Appel e Wolfgang Haken, utilizando um computador. Em 1994 foi produzida uma prova simplificada por Paul Seymour, Neil Robertson, Daniel Sanders e Robin Thomas, mas continua sendo impossível demonstrar o teorema sem recorrer a um computador.

Há várias conjeturas famosas que ainda estão abertas. A conjetura de Goldbach, formulada pelo matemático alemão Christian Goldbach em 1742, afirma que todo número inteiro par maior que 2 é a soma de dois números primos. Testes com computadores mostram que esta afirmação é verdadeira para todos os inteiros pares entre 4 e 4×10^{14} (400 trilhões); mas obviamente estes testes não constituem uma prova.

O monge e matemático francês Marin Mersenne (1585–1648) investigou os números $M_n = 2^n - 1$, onde n é um número primo. Estes números, hoje, são chamados números de Mersenne. Ele observou que os números $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, e $M_7 = 127$ são primos; mas o número seguinte, $M_{11} = 2047$, não é primo ($2047 = 23 \times 89$). Depois de verificar mais alguns casos, ele conjecturou que M_n é primo para todo n em $\{2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257\}$. Porém, em 1876 Edouard Lucas (1842–1891) provou que $M_{67} = 2^{67} - 1$ não era primo, e portanto a conjetura de Mersenne era falsa. Entretanto, sua prova não exibia os fatores de M_{67} , apenas provava que eles existiam. Em 1903, Frank Nelson Cole (1861–1926) apresentou uma palestra em uma conferência de matemática, com o título vago *On the Factorisation of Large Numbers*. Sem dizer nada, Cole primeiro escreveu $2^{67} - 1$ no quadro negro, e fez os cálculos à mão, obtendo o valor 147573952589676412927. Na outra metade do quadro, ele escreveu o produto $193707721 \times 761838257287$, e fez a multiplicação à mão, obtendo o mesmo resultado. A platéia aplaudiu em pé. Depois ele contou que tinha levado três anos, trabalhando todos os domingos, para encontrar essa fatoração.

4.1.3 Métodos de demonstração

Existem teoremas que tem muitas demonstrações diferentes. Qual delas é a melhor é, até certo ponto, uma questão de gosto, e depende para quem a demonstração é dirigida. Em geral, quanto

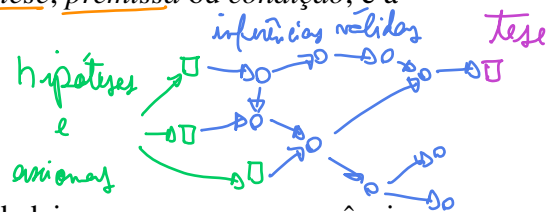
mais curta a prova, melhor; mas há outros critérios, como a facilidade de compreensão, a simplicidade dos passos, etc.. De modo geral, quando não sabemos se uma afirmação é verdadeira, nossa primeira preocupação é encontrar uma demonstração que nos convença. Para convencer outras pessoas, entretanto, devemos cuidar para que a demonstração seja, além de correta, também simples, clara e objetiva, tanto quanto possível.

Há vários métodos de demonstração (*estilos, estratégias, esquemas*, etc.) que são frequentemente usados em matemática. Em geral, a mesma demonstração pode ser reformulada e rearranjada de modo a se enquadrar em vários esquemas distintos. Dependendo do caso, algumas dessas versões podem ser mais fáceis de encontrar, escrever e entender do que outras. No restante deste capítulo vamos descrever algumas técnicas frequentemente utilizadas em provas.

4.2 Demonstração de implicações \Rightarrow

⊕ Sempre deixar claro o que se sabe/supõe e onde se deseja chegar

No decorrer de muitas demonstrações, temos que provar implicações da forma $p \rightarrow q$, isto é se p é verdadeira, então q também é. A afirmação p é chamada de hipótese, premissa ou condição, e a afirmação q é chamada de tese ou conclusão.



4.2.1 Método direto

No método direto de demonstração, supomos que a hipótese p é verdadeira, e usamos uma seqüência de proposições que são consequências lógicas das anteriores, até obter a tese q . Esta seqüência de passos prova a implicação $p \rightarrow q$. Por exemplo, digamos que, num contexto em que m e n são números inteiros, é preciso provar a afirmação

Teorema 4.1: Se m e n são pares, então $m + n$ é par.

Podemos escrever a seguinte demonstração:

Prova:

1. Suponha que m é par. (Hipótese.)
2. Suponha que n é par. (Hipótese.)
3. Existe um inteiro r tal que $m = 2r$. (Definição de “par”.)
4. Existe um inteiro s tal que $n = 2s$. (Definição de “par”.)
5. $m + n = 2r + 2s = 2(r + s)$. (De 3 e 4, por álgebra.)
6. Seja $t = r + s$. (Introdução de variável.)
7. Existe um inteiro t tal que $m + n = 2t$. (De 6.)
8. $m + n$ é par. (De 7 e definição de “par”. Tese.)

Fim.

Prova:

$$m \text{ é par} \Rightarrow \exists q (m = 2q)$$

$$n \text{ é par} \Rightarrow \exists h (n = 2h)$$

$$m+n = 2q + 2h = 2(q+h) = 2k, \\ \text{para } k = (q+h) \in \mathbb{Z}$$

Portanto $m+n$ é par



Usando símbolos lógicos e o predicado P da definição 4.3, a afirmação que queremos demonstrar é $P(m) \wedge P(n) \rightarrow P(m+n)$. A demonstração direta, com alguns passos mais detalhados, seria:

Prova:

1. Suponha $P(m)$. (Hipótese.)
2. Suponha $P(n)$. (Hipótese.)
3. $(\exists r \in \mathbb{Z}) m = 2r$. (Definição de P .)
4. $(\exists s \in \mathbb{Z}) n = 2s$. (Definição de P .)
5. $(\exists r, s \in \mathbb{Z}) m = 2r \wedge n = 2s$. (De 3 e 4.)
6. $(\exists r, s \in \mathbb{Z}) m + n = 2(r + s)$. (De 5, por álgebra.)
7. $(\forall r, s \in \mathbb{Z})(\exists t \in \mathbb{Z}) r + s = t$. (Propriedade da soma.)
8. $(\exists t \in \mathbb{Z}) m + n = 2t$. (De 6 e 7.)
9. $P(m+n)$. (De 8 e definição de P . Tese.)
10. $P(m) \wedge P(n) \rightarrow P(m+n)$. (De 3, 4 e 9.)

Fim.

Supõe-se que cada um dos passos acima é um raciocínio simples o bastante para ser aceito como válido pelo leitor.

Estritamente falando, cada passo de uma demonstração deveria ser uma aplicação de uma regra de inferência, tirada de uma lista fixa de regras que todos os matemáticos aceitam como válidas e fundamentais. Uma das regras comumente aceitas, por exemplo, é a regra de modus ponens: se já demonstramos que uma proposição p é verdade, e que $p \rightarrow q$, então podemos considerar a proposição q demonstrada. Mais geralmente, qualquer das implicações lógicas vistas na seção 3.3.5 pode ser um passo de uma demonstração. Outras regras são necessárias para lidar com quantificadores, como passagem das afirmações 3 e 4 para 5 da prova acima (veja seções 4.4–4.5).

Na prática, os passos são escritos de maneira muito abreviada, na suposição de que o leitor consegue perceber as regras de inferência usadas nas entrelinhas, e explicitá-las se for preciso. Por exemplo, a demonstração acima normalmente seria escrita da seguinte maneira:

Prova:

Suponha que m e n são inteiros pares. Por definição de número “par”, existem inteiros r e s tais que $m = 2r$ e $n = 2s$. Logo $m + n = 2r + 2s = 2(r + s)$. Como $r + s$ é inteiro, concluímos que o inteiro $m + n$ é par, pela definição.

Fim.

Resolvido na aula 1

Exercício 4.1: Demonstre que o produto de um inteiro par por um inteiro ímpar é par.

hip: x é par hip: y é ímpar tese: $x \cdot y$ é par?

x é par $\Rightarrow \exists q \in \mathbb{Z} (x = 2q) \mid y$ é ímpar $\Rightarrow \exists h \in \mathbb{Z} (y = 2h + 1) \mid x \cdot y = 2q \cdot (2h + 1) = 2(2hq + q) \mid$ Para $k = 2hq + q \in \mathbb{Z}$ tem

hip: $r \neq 0$

Exercício 4.2: Demonstre que se r é um número racional diferente de zero, então $\frac{1}{r}$ é racional. (tese)

$x \cdot y = 2k \Rightarrow x \cdot y$ é par

hip: r é racional $\Rightarrow \exists p, q \in \mathbb{Z} (r = \frac{p}{q} \wedge q \neq 0) \mid \textcircled{1} r = \frac{p}{q} \neq 0 \Rightarrow p \neq 0 \textcircled{2} \mid \frac{1}{r} = \frac{1}{(\frac{p}{q})} = \frac{q}{p} \Rightarrow \frac{1}{r}$ é racional

Resolvido na aula 1

Exercício 4.3: Demonstre que, para quaisquer conjuntos A, B, C e D , as seguintes afirmações são sempre verdadeiras

Resolvido na aula 1

Faz na conta positiva

a) Se $x \in A, (A \setminus B) \subseteq (C \cap D)$ e $x \notin D$, então $x \in B$.

hip $\textcircled{1}$ hip $\textcircled{2}$ hip $\textcircled{3}$ tese
 $\textcircled{2} \forall y (y \in A \wedge y \notin B \Rightarrow y \in C \wedge y \in D)$
 $\Rightarrow \forall y (y \notin D \Rightarrow y \notin A \vee y \in B)$

hip $\textcircled{1} B \cap C = \emptyset$ hip $\textcircled{2} \forall y (y \in A \Rightarrow y \in C)$ hip $\textcircled{3} x \in A$
 • Se B e C são disjuntos, $A \subseteq C$ e $x \in A$, então $x \notin B$. $\textcircled{3} \textcircled{2} \Rightarrow x \in C \Rightarrow x \notin B$

c) Se $x \in C$ e $(A \cap C) \subseteq B$, então $x \notin (A \setminus B)$. $\textcircled{2} \forall y (y \in A \wedge y \in C \Rightarrow y \in B)$ $\textcircled{1} x \in A \Rightarrow x \in B$

$a \Rightarrow b \Leftrightarrow \sim a \vee b$ $\textcircled{3} x \notin A \vee x \in B \mid \sim (x \in A \wedge x \notin B) \Leftrightarrow x \notin A \vee x \in B$

Resolvido na aula 1

Exercício 4.4: Sejam X_1, X_2, Y_1, Y_2 subconjuntos de um conjunto U . Suponha que $X_1 \cup X_2 = U$ e $Y_1 \cap Y_2 = \emptyset$, que $X_1 \subseteq Y_1$ e que $X_2 \subseteq Y_2$. Prove que $X_1 = Y_1$ e $X_2 = Y_2$.

na aula não está aqui

$x \in X_1 \Rightarrow x \in Y_1 \mid x \in X_2 \Rightarrow x \in Y_2$ Basta mostrar $x \in Y_i \Rightarrow x \in X_i, i=1,2$

Note que, se $x \in Y_1$, pela hip $\textcircled{1}, x \in X_1 \cup X_2$, mas pela hip $\textcircled{2} x \notin X_2$, e pela hip $\textcircled{1} x \in X_1$. Logo $x \in X_1$

4.2.2 Método da contrapositiva

Se $p \Rightarrow q$ então $\sim q \Rightarrow \sim p$

No método da contrapositiva, para provar a afirmação $p \rightarrow q$, supomos que a negação da tese $\sim q$ é verdadeira, e procuramos uma sequência de deduções lógicas que termina com a negação da hipótese $\sim p$. Esta sequência de passos prova que $(\sim q) \rightarrow (\sim p)$. Como vimos na seção 3.3.2, esta afirmação é logicamente equivalente a $p \rightarrow q$, que portanto também está provada.

Por exemplo, digamos que é necessário provar a afirmação, num contexto em que sabemos que n é um inteiro:

Prova: n^2 é par $\Rightarrow \exists p \in \mathbb{Z} (n^2 = 2 \cdot p)$. Como encontrar

Teorema 4.2: Se n^2 é par, então n é par.

$q \in \mathbb{Z} : n = 2 \cdot q$? Tentar a contra-positiva, pois a hipótese fica mais simples (próxima página)

Prova:

Vamos demonstrar a contrapositiva dessa afirmação, ou seja, se n é ímpar, n^2 é ímpar. Suponha que n é ímpar. Pela definição de "ímpar", existe um inteiro k tal que $n = 2k + 1$. Portanto $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2t + 1$, onde t é $2k^2 + 2k$. Como t é um inteiro, $2t + 1$ é ímpar. Concluímos que n^2 é ímpar.

Fim.

implicação = se a vale então b tem que valer

Usando a notação formal, queremos provar que $P(n^2) \rightarrow P(n)$, onde P é o predicado "é par". Vamos usar o predicado I ("é ímpar") da definição 4.4, supondo já provado que ela equivale à definição 4.6:

a	b	$a \Rightarrow b$	$\sim a$	$\sim b$	$\sim b \Rightarrow \sim a$
V	V	V	F	F	V
V	F	F	F	V	F
F	V	V	V	F	V
F	F	V	V	V	V

contra-positiva = se b não vale então a não pode valer

Prova:

1. Suponha $\neg P(n)$. (Negação da tese.)
2. $I(n)$. (Definição 4.4.)
3. $(\exists k \in \mathbb{Z}) n = 2k + 1$. (De 2 e definição 4.6.)
4. $(\exists k \in \mathbb{Z}) n^2 = (2k + 1)^2 = 4k^2 + 2k + 1 = 2(2k^2 + k) + 1$. (De 3 e álgebra.)
5. $(\forall k \in \mathbb{Z})(\exists t \in \mathbb{Z}) 2k^2 + k = t$. (Props. da mult. e soma.)
6. $(\exists t \in \mathbb{Z}) n^2 = 2t + 1$. (De 4 e 5.)
7. $I(n^2)$. (De 6 e definição 4.6.)
8. $\neg P(n^2)$. (De 7 e definição 4.4. Negação da hipótese.)
9. $\neg P(n) \rightarrow \neg P(n^2)$. (De 1 e 8.)
10. $P(n^2) \rightarrow P(n)$. (Equivalência lógica com 9.)

*Prova: contra-positiva de n^2 é par $\Rightarrow n$ é par
 é igual a n é ímpar $\Rightarrow n^2$ é ímpar
 n é ímpar $\Rightarrow \exists p \in \mathbb{Z} (n = 2p + 1)$
 $n^2 = (2p + 1)^2 = (2p + 1)(2p + 1) = 4p^2 + 4p + 1$
 $= 2(2p^2 + 2p) + 1$
 Para $k = (2p^2 + 2p) \in \mathbb{Z}$
 temos $n^2 = 2k + 1 \Rightarrow n^2$ é ímpar*

Fim.

*$\forall n \in \mathbb{Z} (n^3 + 5 \text{ é ímpar} \Rightarrow n \text{ é par}) \iff \forall n \in \mathbb{Z} (n \text{ é ímpar} \Rightarrow n^3 + 5 \text{ é par})$
 Hip. n é ímpar $\Rightarrow \exists q \in \mathbb{Z} (n = 2q + 1) \mid n^3 + 5 = (2q + 1)^3 + 5 = (2q + 1)(2q + 1)^2 + 5 = (2q + 1)(4q^2 + 4q + 1) + 5$*

Exercício 4.5: Demonstre que, para todo inteiro n , se $n^3 + 5$ é ímpar, então n é par. *$= 2q(4q^2 + 4q + 1) + 2(2q^2 + 2q) + 1 + 5 = 2k \mid k = q(2q + 1)^2 + 2q^2 + 2q + 3 \in \mathbb{Z}$*

Exercício 4.6: Seja n um número inteiro da forma $4k + 3, k \geq 0$. Demonstre que não existem inteiros x, y tais que $x^2 + y^2 = n$. *Provar que $\forall n (\exists k \in \mathbb{Z} (n = 4k + 3, k \geq 0)) \Rightarrow \nexists x, y \in \mathbb{Z} (x^2 + y^2 = n)$*

*Contra-positiva: $\forall n \in \mathbb{Z} (\exists x, y \in \mathbb{Z} (x^2 + y^2 = n)) \Rightarrow \nexists k \in \mathbb{Z} (n = 4k + 3, k \geq 0)$
 Prova: $n = x^2 + y^2 \Rightarrow$ caso 1) x e y par $\Rightarrow n$ é par $\Rightarrow \forall k \in \mathbb{Z} (n \neq 4k + 3)$ | caso 2) x e y ímpar $\Rightarrow n$ é par
 caso 3) Sem perda de generalidade x é par e y é ímpar*

4.2.3 Método de redução ao absurdo

$n = x^2 + y^2 = (2g)^2 + (2h + 1)^2 = 4g^2 + 4h^2 + 4h + 1 = 4(g^2 + h^2 + h) + 1 \neq 4k + 3 \mid \text{todo } k \in \mathbb{Z}$
 O método de redução ao absurdo (também chamado de prova indireta ou por contradição), baseia-se na equivalência lógica entre a fórmula $(p \rightarrow q)$ e a fórmula $(p \wedge \neg q) \rightarrow \mathbf{F}$, vista na seção 3.3.2. Neste método, para provar a afirmação $p \rightarrow q$, supomos que tanto a hipótese p quanto a negação da tese $\neg q$ são verdadeiras, e procuramos uma sequência de deduções lógicas que termina com uma contradição (uma afirmação com valor lógico \mathbf{F}). Isto prova a afirmação $(p \wedge \neg q) \rightarrow \mathbf{F}$, e portanto também a afirmação equivalente a $p \rightarrow q$.

Por exemplo, suponha que num contexto em que m e n são números inteiros, queremos provar a afirmação

Teorema 4.3: Se m e n são pares, então $m + n$ é par

Uma prova por contradição seria:

*hip. ① m é par $\Rightarrow \exists g \in \mathbb{Z} (m = 2g)$ | Para absurdo, supon ③ $m + n$ é ímpar $\Rightarrow \exists p \in \mathbb{Z} (m + n = 2p + 1)$
 hip. ② n é par $\Rightarrow \exists h \in \mathbb{Z} (n = 2h)$ | $m + n = 2g + 2h = 2(g + h) = 2p + 1 \Rightarrow 2(g + h - p) = 1 \Rightarrow g + h - p = 1/2 \Rightarrow \mathbf{F}$, pois $(g + h - p) \in \mathbb{Z}$*

*direta
 $p \rightarrow q$
 hip. tese
 contra-positiva
 $\neg q \rightarrow \neg p$
 hip. tese
 contradição
 $p \wedge \neg q \rightarrow \mathbf{F}$
 hip. hip. tese*

Aula de exercícios

Resolvido na aula 2

Prova:

Suponha que m e n são pares e $m + n$ é ímpar; vamos mostrar que estas suposições levam a uma contradição.

Pela definição de “par”, existem r e s inteiros tais que $m = 2r$ e $n = 2s$. Pela definição de “ímpar”, existe um inteiro t tal que $m + n = 2t + 1$. Logo $2r + 2s = 2t + 1$, ou seja, $r + s - t = 1/2$. Isto é falso pois $r + s - t$ é um inteiro.

Concluimos que, se m e n são pares, $m + n$ não pode ser ímpar.

Fim.

Em notação formal, queremos provar que $P(m) \wedge P(n) \rightarrow P(m + n)$. Usando os predicados P e I definidos anteriormente, e supondo que as definições 4.4 e 4.6 são equivalentes, uma demonstração por contradição seria:

Prova:

1. Suponha $P(m) \wedge P(n)$. (Hipótese.)
2. Suponha $\neg P(m + n)$. (Negação da tese.)
3. $P(m)$. (De 1 por implicação lógica.)
4. $P(n)$. (De 1 por implicação lógica.)
5. $(\exists r \in \mathbb{Z}) m = 2r$. (De 3 e definição 4.3.)
6. $(\exists s \in \mathbb{Z}) n = 2s$. (De 4 e definição 4.3.)
7. $(\exists r, s \in \mathbb{Z}) m = 2r \wedge n = 2s$. (De 5 e 6.)
8. $(\exists r, s \in \mathbb{Z}) m + n = 2(r + s)$. (De 7 e álgebra.)
9. $I(m + n)$. (De 2 e definição 4.4.)
10. $(\exists t \in \mathbb{Z}) m + n = 2t + 1$. (De 9 e definição 4.6.)
11. $(\exists r, s, t \in \mathbb{Z}) (m + n = 2(r + s) \wedge (m + n = 2t + 1))$. (De 8 e 10.)
12. $(\exists r, s, t \in \mathbb{Z}) 2(r + s) = 2t + 1$. (De 11 e álgebra.)
13. $(\exists r, s, t \in \mathbb{Z}) r + s - t = 1/2$. (De 12 e álgebra.)
14. $(\forall r, s, t \in \mathbb{Z})(\exists k \in \mathbb{Z}) r + s - t = k$. (Prop. da soma.)
15. $(\exists k \in \mathbb{Z}) k = 1/2$. (De 13 e 14.)
16. $1/2 \in \mathbb{Z}$. (De 15.)
17. **F**. (De 16 e definição de \mathbb{Z} .)
18. $P(m) \wedge P(n) \wedge \neg P(m + n) \rightarrow \mathbf{F}$. (De 1, 2 e 17.)
19. $P(m) \wedge P(n) \rightarrow P(m + n)$. (De 18 e equiv. lógica.)

Fim.

Exercício 4.7: Seja n um número inteiro da forma $4k + 3$, $k \geq 0$. Escreva uma demonstração detalhada de não existirem inteiros x, y tais que $x^2 + y^2 = n$.

Exercício 4.8: Demonstre que a soma de um número racional com um número irracional é um número irracional. Seja $x = \frac{p}{q}$ um racional, $q \neq 0$. Seja y um irracional. Por absurdo, seja $z = \frac{h}{h}$ um racional t.q. $h \neq 0$ e $x + y = z \Rightarrow \frac{p}{q} + y = \frac{h}{h} \Rightarrow y = \frac{h}{h} - \frac{p}{q} \Rightarrow y = \frac{hq - ph}{h \cdot q}$ é racional, um absurdo.

Exercício 4.9: Demonstre que o número $\sqrt{2}$ é irracional.

Exercício 4.10: Sejam x, y, z números reais. Demonstre que pelo menos um deles é maior ou igual à média aritmética dos três. $\textcircled{*}$ aula de exercícios

Exercício 4.11: Demonstre que, se p é um inteiro ímpar, então a equação $x^2 + x - p = 0$ não tem solução inteira.

Exercício 4.12: Demonstre que, se r é um número irracional, então $\frac{1}{r}$ é irracional.

4.2.4 Implicação com tese conjuntiva

Para provar uma conjunção de duas afirmações $p \wedge q$, basta provar cada uma das afirmações separadamente.

Em particular, para provar uma implicação da forma $p \rightarrow (q \wedge r)$, podemos observar que ela equivale logicamente à afirmação " $(p \rightarrow q) \wedge (p \rightarrow r)$ ". Portanto, basta provar cada uma destas duas implicações separadamente. Se usarmos o método direto para provar cada implicação, supomos que p é verdadeira; provamos então q ; e provamos em seguida r .

Por exemplo, considere o teorema abaixo:

Teorema 4.4: Se 6 divide um inteiro n , então 2 divide n e 3 divide n .

hip. 6 divide $n \Rightarrow \exists q \in \mathbb{Z} (n = 6 \cdot q) \Rightarrow n = 2 \cdot 3 \cdot q$
 $\rightarrow m = 2(3 \cdot q) = 2p \Rightarrow 2$ divide m
 $\rightarrow m = 3(2 \cdot q) = 2h \Rightarrow 3$ divide m

$\textcircled{*}$ aula de exercícios

resolvido na aula 2 \bullet

Por absurdo \bullet

super $x < m$, $y < m$ e $z < m$, $p/m = \frac{x+y+z}{3} \Rightarrow x+y+z < 3m = 3 \cdot \frac{x+y+z}{3} = x+y+z \Rightarrow$ absurdo

$\textcircled{*}$ aula de exercícios

que

esta fração é irredutível, i.e., p e q são os menores inteiros positivos que a satisfazem

Por absurdo, supor $\sqrt{2}$ é racional $\Rightarrow \exists p, q \neq 0 \in \mathbb{Z} (\sqrt{2} = p/q) \Rightarrow (\sqrt{2})^2 = (\frac{p}{q})^2 \Rightarrow p^2 = 2 \cdot q^2 \Rightarrow p^2$ é par $\Rightarrow p$ é par $\Rightarrow \exists h \in \mathbb{Z} (p = 2h) \Rightarrow \sqrt{2} = \frac{p}{q} = \frac{2h}{q} \Rightarrow 2 = \frac{4h^2}{q^2} \Rightarrow q^2 = 2h^2 \Rightarrow q^2$ é par $\Rightarrow q$ é par $\Rightarrow \exists n \in \mathbb{Z} (q = 2n) \Rightarrow \sqrt{2} = \frac{p}{q} = \frac{2h}{2n} = \frac{h}{n} \Rightarrow$ contradição

$\Rightarrow \sqrt{2} = \frac{p}{q} = \frac{2h}{2n} = \frac{h}{n} \Rightarrow$ contradição

Depois

3.g

= 2.g

Prova:

Se 6 divide n então existe um inteiro k tal que $n = 6k$. Então, $n = 2(3k)$, logo 2 divide n . Temos também que $n = 3(2k)$, logo 3 divide n . Portanto 2 divide n e 3 divide n .

Fim.

Depois de provar a parte $p \rightarrow q$, podemos supor que q também é verdadeira, o que pode facilitar a prova de r . Ou seja, para provar $p \rightarrow (q \wedge r)$, podemos provar " $p \rightarrow q$ " e em seguida " $(p \wedge q) \rightarrow r$ ".

Essa análise pode ser estendida para tese com três ou mais termos, isto é, $p \rightarrow (q_1 \wedge q_2 \wedge q_3 \cdots \wedge q_n)$ é equivalente a $(p \rightarrow q_1) \wedge (p \rightarrow q_2) \wedge \cdots \wedge (p \rightarrow q_n)$.

p impotato

4.2.5 Implicação com hipótese disjuntiva

$$p \vee q \rightarrow r \equiv \sim(p \vee q) \vee r \equiv \sim p \wedge \sim q \vee r \equiv \sim p \wedge r \vee \sim q \wedge r \equiv (\sim p \wedge r) \vee (\sim q \wedge r)$$

Suponha que é necessário provar uma implicação da forma $(p \vee q) \rightarrow r$, onde a hipótese é uma disjunção de duas afirmações. Pode-se verificar que esta implicação equivale a $(p \rightarrow r) \wedge (q \rightarrow r)$. (Note a troca de ' \vee ' por ' \wedge '.) Portanto, basta provar cada uma destas duas implicações separadamente.

Assim como na seção 4.2.4 podemos estender essa técnica para hipóteses com três ou mais termos. Observamos que $(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q$ equivale a $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)$ e se cada uma das implicações for provada pelo método direto, a demonstração consistirá de uma lista de casos:

- Caso 1: Supomos que p_1 vale. Provamos q .
- Caso 2: Supomos que p_2 vale. provamos q .
- ...
- Caso n : Supomos que p_n vale. Provamos q .

Note que os casos não precisam ser mutuamente exclusivos. Por exemplo:

Teorema 4.5: Para quaisquer inteiros m e n , se m for par ou n for par, então mn é par.

Prova: *Caso 1) m é par $\Rightarrow \exists p \in \mathbb{Z} (m = 2 \cdot p) \Rightarrow m \cdot n = 2 \cdot p \cdot n \Rightarrow m \cdot n = 2 \cdot (p \cdot n) \Rightarrow m \cdot n$ é par*
Caso 2) n é par $\Rightarrow \exists q \in \mathbb{Z} (n = 2 \cdot q) \Rightarrow m \cdot n = m \cdot 2 \cdot q = 2 \cdot (q \cdot m) \Rightarrow m \cdot n$ é par

Sejam m e n inteiros quaisquer. Temos dois casos (não exclusivos):

- Caso 1: m é par. Pela definição, existe um inteiro q tal que $m = 2q$. Nesse caso, $mn = (2q)n = 2(qn)$, e portanto mn é par.
- Caso 2: n é par. pela definição, existe um inteiro r tal que $n = 2r$. Nesse caso $mn = m(2r) = 2(mr)$, e portanto mn é par.

Portanto, se m é par ou n é par, mn é par.

Fim.

Muitas vezes os casos não são óbvios no enunciado, e tem que ser intuitivos. Por exemplo, considere este teorema:

① **Teorema 4.6:** Se o número inteiro n não é divisível por 3, então seu quadrado tem resto 1 quando divisível por 3.

Prova:

Seja n um inteiro não divisível por 3. Podemos escrever $n = 3p + r$, onde p e r são inteiros e r é 1 ou 2. Então $n^2 = (3p + r)^2 = 9p^2 + 6pr + r^2$. Note que $9p^2 + 6pr$ é um múltiplo de 3, portanto $n^2 \equiv r^2 \pmod{3}$. Temos dois casos:

- Caso 1: $r = 1$, então $r^2 = 1$, cujo resto na divisão por 3 é 1.
- Caso 2: $r = 2$, então $r^2 = 4$, cujo resto na divisão por 3 é 1.

Portanto, o resto de n^2 é 1.

Fim.

Exercício 4.13: Demonstre que não existem soluções inteiras x e y para a equação $x^2 + 3y^2 = 8$.

Exercício 4.14: Demonstre que, se x e y são números reais, então $\max(x, y) + \min(x, y) = x + y$

Exercício 4.15: Demonstre que o quadrado de um número inteiro, não divisível por 5, tem resto 1 ou 4 quando dividido por 5.

ii) $x \not\equiv 0 \pmod{5} \Rightarrow$
 $x^2 = (5k+r)^2$

$= (5k)^2 + 2 \cdot 5k \cdot r + r^2$
 $\Rightarrow x^2 \pmod{5} = r^2$

iii) ? iv) ?

Exercício 4.16: Demonstre que o algarismo das unidades do quadrado de qualquer inteiro n é 0, 1, 4, 5, 6 ou 9.

Exercício 4.17: Demonstre que o algarismo das unidades da quarta potência de qualquer inteiro n é 0, 1, 5 ou 6.

Exercício 4.18: Demonstre que, para todo inteiro n , se n não é divisível nem por 2 nem por 3, então $n^2 - 1$ é divisível por 24.

⊕ aula de exercícios

$x \in \mathbb{Z} \wedge x \not\equiv 0 \pmod{5} \Rightarrow x^2 \pmod{5} = 1 \vee x^2 \pmod{5} = 4 \mid x = 5k + x \pmod{5} \mid$ i) $x \pmod{5} = 1 \Rightarrow x^2 = (5k+1)^2 = (5k)^2 + 2 \cdot 5k \cdot 1 + 1 \Rightarrow x^2 \pmod{5} = 1$

4.3 Demonstrações de afirmações “se e somente se”

Outro tipo comum de teorema tem a forma $p \leftrightarrow q$, ou seja, “ p vale se e somente se q vale.”

Para demonstrar este tipo de teorema, podemos usar a equivalência lógica entre as afirmações $p \leftrightarrow q$ e $(p \rightarrow q) \wedge (q \rightarrow p)$. Ou seja, dividimos a demonstração em duas partes: (1) prova que $p \rightarrow q$; (2) prova que $q \rightarrow p$. Por exemplo: ida

• **Teorema 4.7:** Os inteiros x e y são ambos ímpares se, e somente se, o produto xy é ímpar.

Prova:

Sejam x e y inteiros quaisquer.

$$\left. \begin{aligned} x \text{ é ímpar} &\equiv \exists p \in \mathbb{Z} (x = 2p+1) \\ y \text{ é ímpar} &\equiv \exists q \in \mathbb{Z} (y = 2q+1) \end{aligned} \right\} \Rightarrow x \cdot y = (2p+1)(2q+1) = 4pq + 2p + 2q + 1 \\ = 2(2pq + p + q) + 1 = 2k + 1 \Rightarrow x \cdot y \text{ é ímpar}$$

- Parte (1): provaremos que, se x e y são ímpares, então xy é ímpar. Se x e y são ímpares, por definição existem inteiros r e s tais que $x = 2r + 1$ e $y = 2s + 1$. Portanto $xy = (2r + 1)(2s + 1) = 2(rs + r + s) + 1$. Como $rs + r + s$ é um inteiro, concluímos que xy é ímpar.
- Parte (2): provaremos que, se xy é ímpar, então x e y são ambos ímpares. Ou seja (pela contrapositiva), que se x é par ou y é par, então xy é par. Temos dois casos (não exclusivos):
 - Caso (a): x é par. Neste caso existe um inteiro r tal que $x = 2r$. Portanto $xy = (2r)y = 2(ry)$. Como ry é inteiro, concluímos que xy é par.
 - Caso (b): y é par. Então existe um inteiro s tal que $y = 2s$. Portanto $xy = x(2s) = 2(xs)$. Como xs é inteiro, concluímos que xy é par.

Fim.

Observe que neste exemplo usamos o método da contrapositiva na segunda parte. Com essa escolha, que é bastante comum, a prova de $p \leftrightarrow q$ passa a ser (1) prova de que $p \rightarrow q$; (2) prova de que $(\neg p) \rightarrow (\neg q)$.

Exercício 4.19: Prove que um número inteiro positivo n é ímpar se, e somente se, $5n + 6$ é ímpar.

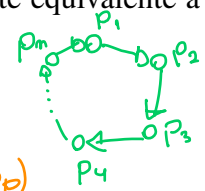
Este método pode ser generalizado para afirmações com três ou mais termos, como $(p_1 \leftrightarrow p_2) \wedge (p_2 \leftrightarrow p_3) \wedge \dots \wedge (p_{n-1} \leftrightarrow p_n)$. Observe que esta afirmação significa que, no contexto corrente, todas as afirmações p_1, p_2, \dots, p_n são equivalentes. Esta afirmação é logicamente equivalente a $(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \dots \wedge (p_{n-1} \rightarrow p_n) \wedge (p_n \rightarrow p_1)$. Por exemplo:

2ª aula acabou aqui

Teorema 4.8: Para todo inteiro n , as seguintes afirmações são equivalentes:

1. n é um número par
2. $n - 1$ é um número ímpar

Prova 1 \rightarrow 2: n é par $\Rightarrow \exists p \in \mathbb{Z} (n = 2p)$
 $n - 1 = 2p - 1 = 2p + 2 - 2 - 1 = 2(p - 1) + 1 \Rightarrow n - 1$ é ímpar



Prova 2 \rightarrow 3: $n - 1$ é ímpar $\Rightarrow \exists q \in \mathbb{Z} (n - 1 = 2q + 1)$
 $n^2 = (n - 1 + 1)^2 = (2q + 1 + 1)^2 = (2q + 2)^2 = 4q^2 + 8q + 4 = 2(2q^2 + 4q + 2) \Rightarrow n^2$ é par

3. n^2 é um número par.

Prova:

Parte (1): vamos provar que se n é par então $n - 1$ é ímpar. Como n é par, por definição existe um inteiro r tal que $n = 2r$. Logo, $n - 1 = 2r - 1 = 2(r - 1) + 1$. Como $r - 1$ é inteiro, concluímos que $n - 1$ é ímpar.

Parte (2) vamos provar que, se $n - 1$ é ímpar, então n^2 é par. Como $n - 1$ é ímpar, existe um inteiro s tal que $n - 1 = 2s + 1$. Logo $n = (2s + 1) + 1 = 2(s + 1)$, e $n^2 = (2(s + 1))^2 = 2(2(s + 1)^2)$. Como $2(s + 1)^2$ é inteiro, concluímos que n^2 é par. Portanto $n^2 = 4(k + 1)^2 = 2(2(k + 1)^2)$ é par.

Parte (3) vamos provar que, se n^2 é par, então n é par. Esta afirmação é verdadeira pelo teorema 4.2.

Fim.

Prova 3 \rightarrow 1:

Exercício 4.20: Demonstre que as seguintes afirmações são equivalentes:

1. $(\exists x) P(x) \wedge (\forall y) (P(y) \rightarrow y = x)$.
2. $(\exists x)(\forall y) P(y) \leftrightarrow y = x$.
3. $(\exists x) P(x) \wedge (\forall y)(\forall z) ((P(y) \wedge P(z)) \rightarrow y = z)$

Exercício 4.21: Demonstre que, se x e y são números reais, as seguintes afirmações são equivalentes:

1. x é menor que y . 1 \Rightarrow 2) $x < y \mid m = (x+y)/2 \Rightarrow 2m = x+y > 2x \Rightarrow m > x$
2. A média aritmética de x e y é maior que x . 2 \Rightarrow 3) $(x+y)/2 > x \mid m = (x+y)/2 \Rightarrow x+y = 2m > x+m \Rightarrow y > m$
3. A média aritmética de x e y é menor que y . 3 \Rightarrow 1) $(x+y)/2 < y \mid x+y < 2y \Rightarrow x < y$

Algumas vezes é possível demonstrar afirmações do tipo $p \leftrightarrow q$ sem dividir as duas implicações. Por exemplo, em alguns casos é possível obter q a partir de p (ou vice-versa) através de uma cadeia de equivalências lógicas. Essa cadeia então é uma prova de que $p \leftrightarrow q$.

Teorema 4.9: Sejam A e B conjuntos. Prove que $(A \subseteq \bar{B}) \leftrightarrow (A \cap B = \emptyset)$.

Prova:

$A \subseteq \bar{B}$ é equivalente a $(\forall x \in A) x \in \bar{B}$; que é equivalente a $(\forall x \in A) x \notin B$. Esta afirmação é equivalente a $(\forall x)(x \in A) \rightarrow (x \notin B)$, que é equivalente a $(\forall x), \neg((x \in A) \wedge (x \in B))$. Pela definição de intersecção, esta afirmação equivale a $A \cap B = \emptyset$.

$$\begin{aligned} A \subseteq \bar{B} &\equiv \forall x (x \in A \Rightarrow x \notin B) \equiv \forall x (x \notin A \vee x \notin B) \equiv \forall x \neg (x \in A \wedge x \in B) \\ &\equiv \forall x \neg (x \in A \wedge x \in B) \equiv A \cap B = \emptyset \end{aligned}$$

Fim.



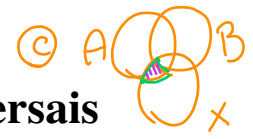
Ver no
aula de
exercícios

Exercício 4.22: Em cada item abaixo, encontre e prove uma condição necessária e suficiente sobre dois conjuntos A e B para que a fórmula seja verdadeira, qualquer que seja o conjunto X .

a) $A \cup (X \cap B) = (A \cup X) \cap B$. | $\circ A \setminus B = \phi$ | Provar que $\circ \Rightarrow a$ e $a \Rightarrow \circ$

b) $A \setminus (X \setminus B) = (A \setminus X) \setminus B$ | $\Delta A \cap B = \phi$ | Provar que $\Delta \Rightarrow b$ e $b \Rightarrow \Delta$

c) $A \cap (X \setminus B) = (A \cap X) \setminus B$



4.4 Regras para quantificadores universais

4.4.1 Instanciação universal

No decorrer de uma prova, uma vez que tivermos estabelecido a veracidade de uma afirmação do tipo $(\forall x \in D) P(x)$, podemos afirmar $P(c)$ para qualquer elemento c do domínio D . Por exemplo, se tivermos provado que “para todo inteiro x , $2^x > x^2$ ”, podemos imediatamente concluir que $2^{418} > 418^2$. Esta regra é chamada de *instanciação universal*.

4.4.2 Generalização universal

Por outro lado, se o objetivo é provar uma afirmação do tipo $(\forall x \in D) P(x)$, podemos começar supondo que x é um elemento de D escolhido arbitrariamente, e omitir o quantificador no restante da prova. Se, com essa suposição, conseguirmos provar a afirmação $P(x)$, podemos concluir que o teorema original (com o quantificador) é verdadeiro. Este último passo é chamado de *generalização universal* ou *suspensão do quantificador universal*.

O mesmo método pode ser usado para vários quantificadores universais encaixados. Por exemplo:

- o **Teorema 4.10:** Para quaisquer números reais x e y , $(x + y)^2 - (x - y)^2 = 4xy$.

Prova:

Sejam x e y dois números reais quaisquer.

Pelo teorema do binômio, temos $(x + y)^2 = x^2 + 2xy + y^2$, e $(x - y)^2 = x^2 - 2xy + y^2$.

Portanto, $(x + y)^2 - (x - y)^2 = (x^2 + 2xy + y^2) - (x^2 - 2xy + y^2) = 4xy$.

Fim.

$$\left. \begin{array}{l} \circ (x+y)^2 = x^2 + 2xy + y^2 \\ \circ (x-y)^2 = x^2 - 2xy + y^2 \end{array} \right\} \Rightarrow \begin{array}{l} (x+y)^2 - (x-y)^2 = \\ = x^2 + 2xy + y^2 \\ - (x^2 - 2xy + y^2) = 4xy \end{array}$$

Ao usar este método, deve-se tomar cuidado para usar variáveis que não tenham significado já definido anteriormente.

Exercício 4.23: Prove a seguinte proposição:

$$(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(\forall k \in \mathbb{Z}) x + y = 7k \leftrightarrow 4x - 3y = 7(4k - y)$$

$$x + y = 7k \Leftrightarrow 4x + 4y = 7 \cdot 4k \Leftrightarrow 4x + 4y - 7y = 7 \cdot 4k - 7y \Leftrightarrow 4x - 3y = 7(4k - y)$$

4.4.3 Demonstração por vacuidade

Lembramos que, se E é o conjunto vazio, a afirmação $(\forall x \in E) Q(x)$ é verdadeira, qualquer que seja o predicado Q . Como vimos na seção 3.6.4 esta afirmação é verdadeira por vacuidade.

○ **Exemplo 4.1:** Todos os pares primos maiores que dois são quadrados perfeitos.

Esta afirmação é verdadeira por vacuidade pois não existem primos pares maiores que dois.

Uma maneira de provar uma afirmação da forma $(\forall x \in D) P(x)$, para um domínio arbitrário D , é mostrar que ela é equivalente a outra afirmação $(\forall x \in E) Q(x)$, para um certo domínio E e algum predicado Q ; e então mostrar que E é vazio.

Por exemplo, a afirmação $(\forall x \in D) A(x) \rightarrow B(x)$ equivale a $(\forall x \in E) B(x)$ onde $E = \{x \in D : A(x)\}$. Portanto, se mostrarmos que $A(x)$ é falsa para todo x em D , a afirmação $(\forall x \in D) A(x) \rightarrow B(x)$ estará provada por vacuidade — qualquer que seja o predicado B .

Exemplo 4.2: Para todo número inteiro x , se $x^2 = 5$ então x é par.

Esta afirmação pode ser escrita $(\forall x \in D) Q(x) \rightarrow P(x)$ onde $D = \mathbb{Z}$, $Q(x)$ significa “ $x^2 = 5$ ”, e $P(x)$ é “ x é par”. Ela é equivalente a “Para todo número inteiro x cujo quadrado é 5, x é par”, ou seja $(\forall x \in E) P(x)$ onde E é o conjunto dos inteiros cujo quadrado é 5. Como E é vazio, a afirmação é verdadeira por vacuidade.

4.5 Regras para quantificadores existenciais

4.5.1 Instanciação existencial

Uma vez que estabelecemos a veracidade de uma proposição do tipo $(\exists x \in D) P(x)$, podemos supor, dali em diante, que a variável x é um dos elementos cuja existência é afirmada, e portanto que $P(x)$ é verdadeira. Desse ponto em diante, a variável x passa a ser livre (veja seção 3.6.10). Esta regra é chamada de *instanciação existencial*.

Para evitar confusão, a variável x deve ser distinta de todas as outras variáveis livres criadas em passos anteriores da demonstração. Se necessário, pode-se trocar a variável do quantificador.

4.5.2 Demonstrações construtivas

Por outro lado, em muitas demonstrações é necessário provar a existência de objetos com uma propriedade particular, ou seja, são da forma $(\exists x \in D) P(x)$. Uma maneira de chegar a essa

conclusão é através de uma demonstração construtiva, em que se exhibe um elemento específico a do domínio D (explicitamente, ou através de uma construção algorítmica) e prova-se que $P(a)$ é verdadeira, para esse elemento. Por exemplo:

- **Teorema 4.11:** Existem três números inteiros positivos tais que $x^2 + y^2 = z^2$.

Sejam $x=3, y=4, z=5$ ou $x=5, y=12, z=13$

Prova:

Sejam $x = 3$, $y = 4$, e $z = 5$. Como $x^2 + y^2 = 3^2 + 4^2 = 25 = 5^2 = z^2$, a afirmação é verdadeira.

Fim.

(Três números x, y, z que satisfazem o teorema 4.11 são chamados de *tripla de inteiros pitagóricos* ou *tripla pitagórica*. Essas triplas correspondem a triângulos retângulos cujos lados têm comprimentos inteiros.)

Naturalmente, este método pode ser usado como parte de uma demonstração mais longa. Por exemplo:

- ? **Teorema 4.12:** Para todo número natural n , se $2^n - 1$ é primo, então n é primo.

Prova: Pela contra-positiva, n não-primo $\Rightarrow 2^n - 1$ não é primo. Seja $n = r \cdot s$, $r, s \in \mathbb{Z}$.

Seja n um número natural. Vamos provar a contra-positiva, ou seja, que se n não é um número primo, então $2^n - 1$ não é primo. Se $n = 0$ ou $n = 1$, nenhum dos dois é primo, e a afirmação é trivialmente verdadeira. Suponhamos então que n é maior que 1 e não é primo. Por definição, existem inteiros r e s maiores que 1 e menores que n tais que $n = rs$. Note que $2^n - 1 = 1 + 2 + 4 + \dots + 2^{n-1}$. Tome $x = 2^s - 1$.

Vamos agora mostrar que existe um inteiro x que é divisor próprio de $2^n - 1$. Seja $x = 2^s - 1$ e $y = 1 + 2^s + 2^{2s} + \dots + 2^{(r-1)s}$. Então e $y = 1 + 2^s + 2^{2s} + \dots + 2^{(r-1)s}$.

$$\begin{aligned} xy &= (2^s - 1)(1 + 2^s + 2^{2s} + \dots + 2^{(r-1)s}) \\ &= 2^s(1 + 2^s + 2^{2s} + \dots + 2^{(r-1)s}) - (1 + 2^s + 2^{2s} + \dots + 2^{(r-1)s}) \\ &= (2^s + 2^{2s} + \dots + 2^{rs}) - (1 + 2^s + 2^{2s} + \dots + 2^{(r-1)s}) \\ &= 2^{rs} - 1 \\ &= 2^n - 1. \end{aligned}$$

$x \cdot y = (2^s - 1)(1 + 2^s + 2^{2s} + \dots + 2^{(r-1)s}) = (2^s + 2^{2s} + \dots + 2^{rs}) - (1 + 2^s + 2^{2s} + \dots + 2^{(r-1)s}) = 2^{rs} - 1 = 2^n - 1$

Uma vez que s é maior que 1 e menor que n , temos que $x = 2^s - 1$ é maior que $2^1 - 1 = 1$ e menor que $2^n - 1$. Ou seja, x é um divisor próprio de $2^n - 1$.

Concluimos portanto $2^n - 1$ não é primo.

Fim.

Observe na demonstração acima, que a existência do divisor próprio de $2^n - 1$ foi provada exibindo um x e provando que ele tem essa propriedade. Esta regra de inferência é também chamada de generalização existencial.

Outro exemplo de demonstração construtiva é a seguinte afirmação, conhecida como teorema do deserto de primos:

- **Teorema 4.13:** Para todo número inteiro positivo n , existe uma sequência de n números inteiros consecutivos que não são primos.

Prova: $(n+1)! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \dots \cdot (n-1) \cdot n \cdot (n+1)$ é divisível por $k \in S = \{2, 3, 4, \dots, n+1\}$ e $|S| = n$.
Seja $x = (n+1)!$ e considere os números $x+k$, $p/ k \in S$. Note que $x+2$ é divisível por 2, $x+3$ por 3, $x+4$ por 4, ..., $x+n+1$ por $n+1$.
Seja n um inteiro positivo, e seja $x = (n+1)! + 2$. Observe que

$$2 \text{ divide } x = (n+1)! + 2, \quad (4.3) \text{ Ou seja, todos}$$

$$3 \text{ divide } x+1 = (n+1)! + 3, \quad (4.4) \text{ inteiros entre } x+2$$

$$\dots \quad (4.5) \text{ e } x+n+1 \text{ não}$$

$$n+1 \text{ divide } x+(n-1) = (n+1)! + n+1. \quad (4.6) \text{ são primos. } \square$$

Logo todos os inteiros $x+i$ com $0 \leq i < n$ são não primos; e eles formam uma sequência de n inteiros consecutivos.

Fim.

Exercício 4.24: Existem 100 inteiros consecutivos que não são quadrados perfeitos.

$$1, 4, 9, 16, 25, 36, 49, 64, 81, 100, \dots \quad | \quad 10^4 = 100 \square \quad \square 101 = 10^4 + 201$$

Exercício 4.25: Demonstre que existem dois inteiros positivos consecutivos, tal que um é um cubo perfeito e o outro é um quadrado perfeito.

$$2^3 = 8 \quad \text{e} \quad 3^2 = 9$$

4.5.3 Demonstrações não construtivas

Em alguns casos, é possível demonstrar a existência de um elemento que satisfaz uma dada condição mesmo sem exibir explicitamente tal elemento. Uma demonstração deste tipo é chamada de demonstração não construtiva. Por exemplo:

- **Teorema 4.14:** Existem dois números reais irracionais x e y tais que x^y é racional.

Prova: Tome $x=y=\sqrt{2}$. Temos $x^y = \sqrt{2}^{\sqrt{2}}$, mas não sabemos se $\sqrt{2}^{\sqrt{2}}$ é racional. Se for, temos o resultado.
Sabemos que o número $\sqrt{2}$ é irracional. Se $(\sqrt{2})^{\sqrt{2}}$ for racional, a afirmação está satisfeita tomando-se $x = \sqrt{2}$ e $y = \sqrt{2}$. Por outro lado, se $(\sqrt{2})^{\sqrt{2}}$ for irracional, podemos tomar $x = (\sqrt{2})^{\sqrt{2}}$ e $y = \sqrt{2}$. Então $x^y = ((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2} \cdot \sqrt{2}} = (\sqrt{2})^2 = 2$ que é racional. *Seja $x = \sqrt{2}^{\sqrt{2}}$ e $y = \sqrt{2}$. Então $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2 \in \mathbb{Q}$*

Fim.

Observe que esta demonstração prova que existem valores de x e y que satisfazem a condição, mas deixa em suspenso o valor de x ($\sqrt{2}$ ou $(\sqrt{2})^{\sqrt{2}}$). Para tornar esta demonstração construtiva, teríamos que determinar se $(\sqrt{2})^{\sqrt{2}}$ é racional ou não; mas este é um problema muito difícil.

Outro exemplo clássico de demonstração não construtiva de existência é o seguinte teorema, atribuído a Euclides (360 AC – 295 AC).

- **Teorema 4.15:** Existem infinitos números primos.

Suponha, por absurdo, que existe um # finito de primos e todos estão em
Prova: $P = \{p_1, p_2, p_3, \dots, p_m\}$. Seja $x = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_m + 1 = \prod_{i=1}^m p_i + 1 = \prod_{p \in P} p + 1$. Note que x não é divisível por qualquer $p_i \in P$, pois x sempre sobra resto 1.
 Vamos usar o método da demonstração por absurdo. Suponhamos que existem finitos números primos, a saber $2, 3, 5, \dots, p$. Seja n o inteiro $(2 \times 3 \times 5 \times \dots \times p) + 1$. Como n é maior que 1, ele tem algum fator primo r . Observe que n não é divisível por $2, 3, 5, \dots, p$, pois tem resto 1 quando dividido por qualquer desses números. Portanto, r , que é divisor de n , não pode ser nenhum dos primos listados acima. Isso contradiz a suposição de que essa lista contém todos os primos.

Fim.

4.5.4 Demonstração de existência e unicidade

Lembramos que uma afirmação do tipo $(\exists! x \in D) P(x)$ equivale logicamente a

$$((\exists x \in D) P(x)) \wedge ((\forall x \in D)(\forall y \in D) ((P(x) \wedge P(y)) \rightarrow x = y))$$

Portanto, uma demonstração de existência e unicidade pode ser dividida em duas partes:

- Existência: prova-se ~~que~~ (construtivamente ou não) que existe pelo menos um x em D que satisfaz $P(x)$.
- Unicidade: supõe-se que y também é um elemento de D que satisfaz $P(y)$, e prova-se que ele é igual ao x cuja existência foi mostrada na primeira parte.

? **Teorema 4.16:** Para todo número complexo z diferente de zero, existe um único número complexo x tal que $zx = 1$.

Seja $z = a + bi$. Note que $(a + bi)(a - bi) = a^2 - abi + abi - bi^2 = a^2 + b^2$
Prova: Assim, seja $x = (a - bi)/(a^2 + b^2)$, $p/a^2 + b^2 \neq 0$, o que vale se $a \neq 0$ ou $b \neq 0$
 Seja z um número complexo qualquer, diferente de zero. Por definição, existem a e b em \mathbb{R} tais que $z = a + bi$, onde i é um elemento de \mathbb{C} tal que $i^2 = -1$.

Existência: $z \cdot x = (a + bi) \cdot \frac{(a - bi)}{a^2 + b^2} = \frac{a^2 + b^2}{a^2 + b^2} = 1$

Unicidade: $zy = 1 \Rightarrow x \cdot zy = x \Rightarrow (x \cdot z)y = x \Rightarrow y = x$

Vamos primeiro mostrar que existe pelo menos um x em \mathbb{C} tal que $zx = 1$. Como z é diferente de zero, pelo menos um dos números a e b é diferente de zero. Isso implica que $a^2 + b^2$ é positivo. Seja então $x = (a - bi)/(a^2 + b^2)$. Temos que

$$\begin{aligned}zx &= (a + bi)((a - bi)/(a^2 + b^2)) \\ &= (a^2 - abi + abi - b^2i^2)/(a^2 + b^2) \\ &= (a^2 + b^2)/(a^2 + b^2) \\ &= 1.\end{aligned}$$

Suponha agora que y é um número complexo qualquer tal que $zy = 1$; vamos mostrar que ele é igual a x . Multiplicando os dois lados da equação $zy = 1$ por x temos $(zy)x = x$. Como a multiplicação de números complexos é associativa e comutativa, esta afirmação equivale a $(zx)y = x$. Como $zx = 1$, concluímos que $y = x$.

Fim.

Exercício 4.26: Demonstre que, se m e n são inteiros distintos e $m - n$ é par, então existe um único inteiro r tal que $|m - r| = |n - r|$

Exercício 4.27: Demonstre que, se r é um número irracional, então existe um único inteiro n tal que a distância entre r e n é menor do que $1/2$.

Exercício 4.28: Prove que para qualquer matriz A 2×2 de números reais com determinante $|a|$ não nulo existe uma única matriz B 2×2 de números reais tal que

$$AB = BA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

4.5.5 Demonstração de falsidade por contra-exemplo

Demonstrações de existência são usadas, em particular, para refutar conjeturas da forma $(\forall x \in D) P(x)$; pois a negação desta afirmação é $(\exists x \in D) \neg P(x)$. Neste caso dizemos que o elemento x de D que comprovadamente não satisfaz $P(x)$, e que portanto mostra a falsidade da conjetura, é um contra-exemplo para a mesma.

Considere a seguinte afirmação: “Para todo primo n , o inteiro $2^n - 1$ é primo.” Esta afirmação não é verdadeira, basta ver que o número $n = 11$ é um contra-exemplo, pois $P(11) = 2^{11} - 1 = 2047 = 23 \times 89$.

Exercício 4.29: Demonstre (por meio de contra-exemplos) que as seguintes conjecturas são falsas:

- a) Todo inteiro positivo é soma dos quadrados de três inteiros. $0^2=0, 1^2=1, 2^2=4, 3^2=9 \mid 7$ é contra-exemplo
- b) Se n é um número inteiro e $4n$ é par, então n é par. $n=3$ é ímpar, mas $4n=4 \cdot 3=12$ é par
- c) O produto de dois números irracionais é um número irracional. $\sqrt{2}$ é irracional, mas $\sqrt{2} \cdot \sqrt{2} = 2 \in \mathbb{Q}$

Exercício 4.30: Em cada caso abaixo, demonstre (por meio de contra-exemplo) que as duas proposições *não* são equivalentes:

- a) $(\forall x \in D) P(x) \vee Q(x)$ e $((\forall x \in D) P(x)) \vee (\forall x \in D) Q(x)$.
- b) $(\exists x \in D) P(x) \wedge Q(x)$ e $((\exists x \in D) P(x)) \wedge (\exists x \in D) Q(x)$.

⊗
Aula de
exercícios

Mostre que $(a \cdot b) \% m = ((a \% m) (b \% m)) \% m$ \rightarrow resultado útil na implementação de funções de espalhamento

$$a = p_a \cdot m + a \% m$$

$$b = p_b \cdot m + b \% m$$

$$(a \cdot b) \% m = ((p_a \cdot m + a \% m) \cdot (p_b \cdot m + b \% m)) \% m$$

$$= (p_a \cdot p_b \cdot m^2 + p_a \cdot (b \% m) \cdot m + p_b \cdot (a \% m) \cdot m + (a \% m) \cdot (b \% m)) \% m$$

$$= \underline{m} \cdot (\underline{p_a \cdot p_b \cdot m + p_a \cdot (b \% m) + p_b \cdot (a \% m)}) + (a \% m) \cdot (b \% m) \underline{\% m}$$

$$= ((a \% m) (b \% m)) \% m$$

