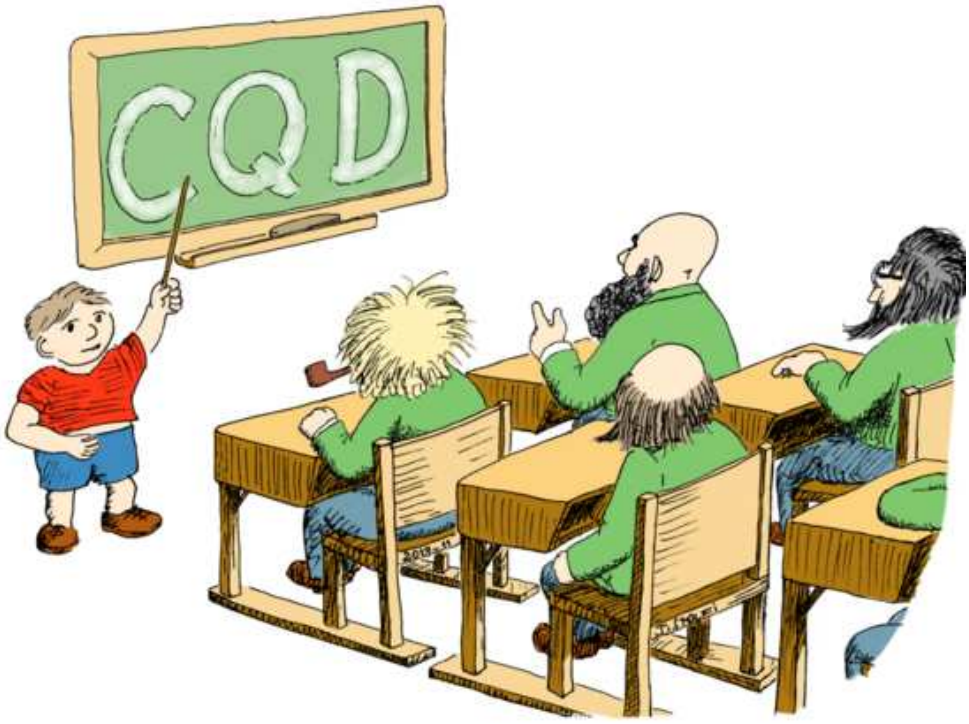
Capítulo 4

Métodos de Demonstração



4.1 Introdução

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 as duas partes consideram válidas. Em geral, podem ser usadas as equivalências e implicações lógicas vistas nos capítulos anteriores. 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. Uma definição precisa ser *completa*, isto é, deve especificar todas as propriedades que identificam exatamente o conceito definido. Deve ser também *precisa*, de modo que o leitor não tenha dúvidas sobre seu significado. Por convenção, o termo definido é enfatizado por ocasião de sua 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 $n = pq$.

Observe que esta definição não deixa dúvidas: para quaisquer inteiros n e p, ela permite ao leitor decidir se n é ou não múltiplo de p. Por outro lado, ela só vale no domínio dos inteiros. O número π é um múltiplo de $\sqrt{17}$? Esta definição não diz nem que sim, nem que não. Enquanto o conceito de "múltiplo" não for definido para números reais, essa frase não tem sentido: ela não é nem verdadeira nem falsa, e portanto não é uma proposição lógica.

Observe também que, na afirmação que define o conceito, as variáveis n e p são livres, enquanto que q está amarrada no quantificador "existe". Formalmente, podemos entender esta declaração como a definição de um predicado P ("é multiplo de") com dois parâmetros (n e p).

Esta definição pode ser usada em demonstrações como se fosse um axioma, ou seja ela nos autoriza a supor que a afirmação

$$(\forall n, p \in \mathbb{Z})\,(n \text{ é um múltiplo de } p) \leftrightarrow ((\exists q \in \mathbb{Z})\, n = pq)$$

é verdadeira.

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.

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 é 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 n é *par* se ele é múltiplo de 2.

Esta definição deve ser entendida como "um inteiro n é par se, e somente se, n é múltiplo de 2". Eis outro exemplo:

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

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.

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 palesta 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 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

No decorrer de muitas demonstrações, temos que provar implicaçoes da forma $p \to q$, 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 sequência de proposições que são consequências lógicas das anteriores, até obter a tese q. Esta sequência de passos prova a implicação $p \to q$. Por exemplo, digamos que é preciso provar a afirmação

Teorema 4.1: Se m e n são inteiros 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. (Definição de "par", dada 6. Tese.)

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 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 $p \to q$, então podemos considerar a proposição

q demonstrada. Mais geralmente, qualquer das implicações lógicas vistas na seção 3.3.4 pode ser um passo de uma demonstração. Outras regras são necessárias para lidar com quantificadores, como nos passos 5–7 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. Isto prova que, se m e n são pares, $m + n$ é par.

Fim.

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

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

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

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

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 $Y_1 \cap Y_2 =$, que $X_1 \subset Y_1$ e que $X_2 \subset Y_2$. Prove que $X_1 = Y_1$ e $X_2 = Y_2$.

4.2.2 Método da contrapositiva

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

Por exemplo, digamos que é necessário provar a afirmação:

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

Prova:

Suponha que n é ímpar. Pela definição de "ímpar", existe um inteiro k tal que $n = 2k + 1$. Portanto $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Como $2k^2 + 2k$ é um inteiro, pela definição de "ímpar" concluímos que n^2 é impar.

Pela regra da contrapositiva, isto prova que, se n^2 é um inteiro par, então n é um inteiro par.

Fim.

Exercício 4.5: Demonstre que, para todo inteiro n, se $n^3 + 5$ é impar, então n é par.

Exercício 4.6: Seja n um número inteiro da forma $4k + 3$, $k \geq 0$. Demonstre que não existem inteiros x, y tais que $x^2 + y^2 = n$.

4.2.3 Método de redução ao absurdo

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 **F**). Isto prova a afirmação $(p \wedge \neg q) \rightarrow \mathbf{F}$, e portanto também a afirmação equivalente a $p \rightarrow q$.

Por este método, a afirmação

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

pode ser provada desta maneira:

Prova:

Suponhamos que m e n são inteiros pares e $m + n$ é um inteiro 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 j tal que $m + n = 2j + 1$. Logo $2r + 2s = 2j + 1$, ou seja, $r + s - j = 1/2$. Isto é falso pois $r + s - j$ é um inteiro.

Esta contradição prova que, se m e n são inteiros pares, $m + n$ é um inteiro par.

Fim.

Exercício 4.7: Seja n um número inteiro da forma $4k + 3$, $k \geq 0$. Escreva uma demonstração detalhada de não existem 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.

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.

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.

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 $(p \rightarrow q_1) \wedge (p \rightarrow q_2) \wedge \cdots \wedge (p \rightarrow q_n)$.

4.2.5 Implicação com hipótese disjuntiva

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 quaiquer inteiros m e n, se m for par ou n for par, então mn é par.

Prova:

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, $mn = (2q)n = 2(nq)$, 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 intuidos. Por exemplo, considere este teorema:

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 r^2. 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.

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.

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:

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.

- 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 $(p_1 \leftrightarrow p_2) \wedge (p_2 \leftrightarrow p_3) \wedge \cdots \wedge (p_{n-1} \leftrightarrow p_n)$. Observe que esta afirmação significa que, no contexto corrente, todas as afirmações p_1, p_2, ..., p_n são equivalentes. Esta afirmação é logicamente equivalente a $(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \cdots \wedge (p_{n-1} \rightarrow p_n) \wedge (p_n \rightarrow p_1)$. Por exemplo:

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
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.

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. $(\exists x)\, P(x) \wedge (\forall y)(\forall z)\, ((P(y) \wedge P(z)) \rightarrow y = x)$

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

1. x é menor que y.
2. A média aritmética de x e y é maior que x.
3. A média aritmética de x e y é menor que 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 $A \cap B = \emptyset$.

Fim.

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) $A \cup (X \cap B) = (A \cup X) \cap B)$.

b) $A \setminus (X \setminus B) = (A \setminus X) \setminus B)$

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:

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.

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:

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

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 $(\forall x \in D)\, A(x) \to B(x)$ 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 $(\forall x \in D)\, A(x) \to B(x)$ 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 exibe um elemento específico a do domínio D (explicitamente, ou através de uma construção algoritmica) e prova-se que $P(a)$ é verdadeira, para esse elemento. Por exemplo:

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

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:

Seja n um número natural. Vamos provar a contrapositiva, 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 $n = rs$.

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

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

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 $2^n - 1$.

Concluímos 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:

Seja n um inteiro positivo, e seja $x = (n + 1)! + 2$. Observe que

$$\begin{aligned} 2 \text{ divide } x &= (n+1)! + 2, && (4.1) \\ 3 \text{ divide } x+1 &= (n+1)! + 3, && (4.2) \\ &\ldots && (4.3) \\ n+1 \text{ divide } x+(n-1) &= (n+1)! + n + 1. && (4.4) \end{aligned}$$

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.

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

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:

Sabemos que 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.

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.

Prova:

Vamos usar o método da demonstração por absurdo. Suponhamos que existem finitos números primos, a saber $2, 3, 5, \ldots, p$. Seja n o inteiro $(2 \times 3 \times 5 \times \cdots \times p) + 1$. Como n é maior que 1, ele tem algum fator primo r. Observe que n não é divisível por $2, 3, 5, \ldots, p$, 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-se (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 $zx = 1$.

Prova:

Seja z um número complexo qualquer, diferente de zero. Por definição, existem a e b em $\mathbb{R}$ tais que $z = a + b\mathbf{i}$, onde $\mathbf{i}$ é um elemento de $\mathbb{C}$ tal que $\mathbf{i}^2 = -1$.

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 $x = (a - b\mathbf{i})/(a^2 + b^2)$. Temos que

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

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 conjeturas são falsas:

a) Todo inteiro positivo é soma dos quadrados de três inteiros.

b) Se n é um número inteiro e $4n$ é par, então n é par.

c) O produto de dois números irracionais é um número irracional.

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 $((\exists x \in D)\, P(x)) \wedge (\exists x \in D)\, Q(x))$.