1.3 Introdução a técnicas de demonstrações

Do ponto de vista lógico existem, essencialmente, dois tipos de sentenças verdadeiras: os axiomas, que são admitidos como verdadeiros, e os teoremas, que são demonstrados serem verdadeiros. Em textos matemáticos as sentenças que nós demonstramos são, geralmente, chamadas de *teoremas*, *proposições*, *lemas* e *corolários*. A diferença entre esses rótulos é circunstancial e depende de uma convenção não muito rígida que diz, em geral, que teoremas são resultados importantes, as proposições são menos importantes que os teoremas, os lemas são resultados auxiliares usadas nas provas de outros resultados e que merecem destaque, os corolários são sentenças que se seguem facilmente de outros resultados.

Ainda há sentenças que chamamos *princípio* que é um teorema ou axioma e que ocupa um papel fundamental numa teoria por ser a chave para demonstrar um grande número de propriedades importantes. Um exemplo típico é o Princípio da Indução Finita que em algumas exposições sobre os naturais ele aparece como um dos axiomas (como no tratamento axiomático de Peano), e em outras, como teorema (como na teoria dos conjuntos ZFC).

Um outro termo recorrente em textos matemáticos é *conjetura* (ou *conjectura*) que é uma sentença que está sendo proposta como uma sentença verdadeira porém não é conhecida uma demonstração. Se posteriormente demonstrada verdadeira, torna-se um teorema; se for mostrado um contraexemplo deixa de ser uma conjetura. Até o momento que este texto estava sendo escrito a seguinte sentença não tinha uma demonstração.

CONJECTURA 32 (CONJETURA DE GOLDBACH) *Todo inteiro par maior que 2 pode ser escrito como a soma de dois números primos.*

Muitas das sentenças de teoremas (talvez a maior parte) são generalizações de sentenças condicionais e vamos dar ênfase nesse caso já que é inviável considerarmos todos as possíveis estruturas lógicas dos enunciados de sentenças.

1.3.1 Considerações iniciais através de um exemplo

Para demonstrar uma sentença precisamos conhecer as definições dos termos usados na sentença. Vamos ver um exemplo. Começamos com uma definição de número par.

Definição 33. Um inteiro n é **par** se, e somente se, n é da forma $2k$ para algum inteiro k. Um inteiro n é **ímpar** se, e somente se, n é da forma $2k+1$ para algum inteiro k.

Observemos que a definição acima é dada por um "se, e somente se" de modo que é usada em demonstrações como uma equivalência lógica, para qualquer que seja o inteiro n

$$n \text{ é par} \Leftrightarrow \exists k \in \mathbb{Z},\ n = 2k. \tag{1.9}$$

Se a definição é dada por uma condicional

"n é par se n é da forma $2k$ para algum inteiro k"

ao invés de uma bicondicional ela, a rigor, não exclui a possibilidade de $n = 1$ ser par (veja a discussão no início da seção 1.1.1). Entretanto, em textos matemáticos é comum encontrar definições que usam uma condicional e nesses casos devemos entender que a intenção é a da equivalência. Por exemplo, em *um inteiro n é par se ele é múltiplo de* 2 não garante que um número par é múltiplo de 2.

Além das definições, usamos axiomas e teoremas já conhecidos. Essa metodologia de derivar teoremas a partir de axiomas, o método axiomático, foi usado de modo pragmático pela primeira vez por Euclides por volta de 300 aC. Como alguém pensa e cria uma demonstração é uma ponto que está fora do nosso alcance, não vamos discutir, mas a demonstração em si tem que se desenrolar em passos logicamente válidos do início ao fim e é da praxe que as demonstrações sigam alguns paradigmas. Cada demonstração tem os seus próprios detalhes mas os paradigmas nos dão um referencial organizado para uma boa escrita das deduções.

Em muitos casos as sentenças de teoremas são sentenças condicionais não escritas explicitamente, as palavras-chave "se, então" e "para todo", ou equivalentes, não apareçam explicitamente, assim como os quantificadores são omitidos. O trabalho inicial sempre é o da interpretação e análise do texto. Por exemplo, em "o quadrado de todo número real não nulo é positivo" temos, implicitamente, a estrutura lógica "para todo número real x, se $x \neq 0$ então $x^2 > 0$".

TEOREMA 34 *A soma de inteiros pares é par.*

Para demonstrar essa afirmação, provamos que para quaisquer x e y inteiros, se x é par e y é par, então $x+y$ é par. Essa sentença tem a "forma lógica" $A \wedge B \rightarrow C$ e o que precisamos demonstrar que se A é verdadeiro (x é par) e B é verdadeiro (y é par), então C é verdadeiro ($x+y$ é par). Para isso, assumimos A e B como hipóteses, ou premissas verdadeiras, e construímos uma demonstração que conclui que C é verdadeiro.

Demonstração do teorema 34. Sejam x e y números inteiros e assuma que x é par e y é par. Então, por definição, existem inteiros k_1 e k_2 tais que $x = 2k_1$ e $y = 2k_2$, logo $x + y = 2(k_1 + k_2)$, portanto, pela definição, $x+y$ é par. □

Note que na demostração usamos a equivalência (1.9) nos dois sentido, se x é par então ele é múltiplo de 2, e se $x+y$ é múltiplo de 2 então ele é par.

Uma consideração importante ao escrever uma demonstração é reconhecer o que precisa ser provado e o que pode ser usado sem justificativa. Esse último depende do contexto e é, em geral, calibrado de acordo com a audiência a que se destina a demonstração. O nosso contexto é o de aprendizado elementar logo é necessário escrever com bastante detalhes. Também, um trabalho de rascunhagem investigativa é muito importante para descobrir a estratégia geral para abordar o problema a ser resolvido, antes de examinar os detalhes. Todo matemático teve que tentar muitas abordagens para provar um teorema antes de encontrar uma que funcionasse, aqui está a maior parte do trabalho.

Finalmente, as demonstrações devem se escritas em português, usando frases completas e com pontuação adequada, como foi feito no caso da *Demonstração do teorema 34* e não como feita na tabela abaixo. Fórmulas e símbolos matemáticos são partes de frases e não são tratados diferente de outras palavras.

A Leitura

Ler uma demonstração exige esforço para a validação do argumento. Em casos muito simples, como no teorema acima, não dá muito trabalho explicitar todo esquema lógico desse argumento. Fazemos isso abaixo na tabela 1.6, usando alguns símbolos para encurtar a escrita fazemos referência a algumas regras de inferência, apresentadas na página 11 e seguintes, e a propriedades aritméticas apresentadas na seção 1.2.4.

1)	x é par e y é par.	(hipótese)
2)	x é par.	(regra da simplificação)
3)	y é par.	(regra da simplificação)
4)	Se x é par, então $\exists k_1 \in \mathbb{Z}, x = 2k_1$	(definição)
5)	$\exists k_1 \in \mathbb{Z}, x = 2k_1$	(modus ponens)
6)	$x = 2k_1$	(regra da instanciação existencial)
7)	Se y é par, então $\exists k_2 \in \mathbb{Z}, y = 2k_2$	(definição)
8)	$\exists k_2 \in \mathbb{Z}, y = 2k_2$	(modus ponens)
9)	$y = 2k_2$	(regra da instanciação existencial)
10)	$x = 2k_1$ e $y = 2k_2$	(regra da conjunção)
11)	Se $x = 2k_1$ e $y = 2k_2$, então $x + y = 2(k_1 + k_2)$	(compatibilidade)
12)	$x + y = 2(k_1 + k_2)$	(modus ponens)
13)	Se $x + y = 2(k_1 + k_2)$, então $\exists c \in \mathbb{Z}, x + y = 2c$	(regra da generalização universal)
14)	$\exists c \in \mathbb{Z}$ tal que $x + y = 2c$	(modus ponens)
15)	Se $\exists c \in \mathbb{Z}, x + y = 2c$, então $x + y$ é par	(definição)
16)	$x + y$ é par	(modus ponens).

Tabela 1.6: Um escrutínio da demonstração do teorema 34.

Notemos que a partir das premissas na tabela 1.6, uma linha qualquer é uma sentença verdadeira sempre a linhas anteriores a ela são verdadeiras, portanto se a hipótese é verdadeira a última linha é uma sentença verdadeira.

1.3.2 Demonstração direta de implicação

Na argumentação mais direta para demonstrar que $P \to Q$ é verdadeiro, assumimos P verdadeiro e concluímos que Q é verdadeiro. Essa estratégia é chamada de prova direta da implicação.

TEOREMA 35 *Se a e b são números inteiros tais que $0 < a < b$, então $a^2 < b^2$.*

DEMONSTRAÇÃO. Sejam a e b são números inteiros. Vamos supor que $0 < a < b$ e provar que $a^2 < b^2$.
Se $a < b$ e $0 < a$ então $a^2 < ab$. Se $a < b$ e $0 < b$ então $ab < b^2$. Por transitividade, $a^2 < b^2$ como queríamos demonstrar. □

Uma leitura detalhada do argumento é dada na tabela 1.7.

TEOREMA 36 *Sejam A, B, C conjuntos não vazios. Se $A \cap C \subset B$ e $a \in C$ então $a \notin A \setminus B$.*

De acordo com a estratégia de demonstração direta, devemos supor que $A \cap C \subset B$ e $a \in C$ é verdadeiro e provar que $a \notin A \setminus B$ é verdadeiro.

1)	$0 < a$ e $a < b$	(hipótese)
2)	$a < b$	(regra da simplificação)
3)	$0 < a$	(regra da simplificação)
4)	se $0 < a$ e $a < b$, $0 < b$	(transitividade do $<$)
5)	$0 < b$	(modus ponens)
6)	se $a > 0$ e $a < b$ então $a \cdot a < a \cdot b$	(compatibilidade do $<$ com $\cdot$)
7)	$a^2 < ab$	(modus ponens)
8)	$b > 0$ e $a < b$	(regra da conjunção)
9)	se $b > 0$ e $a < b$ então, $a \cdot b < b \cdot b$	compatibilidade do $<$ com $\cdot$)
10)	$ab < b^2$	(modus ponens)
11)	$a^2 < ab$ e $ab < b^2$	(regra da conjunção)
12)	se $a^2 < ab$ e $ab < b^2$ então $a^2 < b^2$	(transitividade do $<$)
13)	$a^2 < b^2$	(modus ponens)

Tabela 1.7: Um escrutínio do teorema 35.

Pela definição de diferença de conjuntos $a \notin A \setminus B$ é logicamente equivalente a não($a \in A$ e $a \notin B$) que é logicamente equivalente a $a \notin A$ ou $a \in B$ que, por sua vez, é logicamente equivalente a $a \in A \to a \in B$. Portanto, se assumimos verdadeiro $A \cap C \subset B$ e $a \in C$ e deduzirmos que $a \in A \to a \in B$ é verdadeiro então podemos concluir, pela equivalência lógica, que $a \notin A \setminus B$ é verdadeiro. Assim, nossa tarefa é demonstrar que é verdadeira a (primeira) condicional

$$(A \cap C \subset B \text{ e } a \in C) \to (a \in A \to a \in B). \tag{1.10}$$

Para demonstrar que vale (1.10)

assumimos: $A \cap C \subset B$ e $a \in C$ verdadeiro

provamos: $a \in A \to a \in B$ verdadeiro

para provar que $a \in A \to a \in B$ é verdadeiro, uma condicional, assumimos $a \in A$ verdadeiro e deduzimos que $a \in B$ é verdadeiro, no caso $a \notin A$ não há o que fazer pois a condicional é verdadeira. Assim para demonstrar (1.10)

assumimos: $A \cap C \subset B$ e $a \in C$ e $a \in A$ verdadeiro

provamos: $a \in B$ verdadeiro.

Com esse rascunho em mãos escreveremos a demonstração.

DEMONSTRAÇÃO. Sejam A, B, C conjuntos não vazios e $a \in A$. Vamos assumir que $A \cap C \subset B$ e $a \in C$ e $a \in A$.

Se $a \in C$ e $a \in A$ então $a \in A \cap C$ por definição de interseção. Se $a \in A \cap C$ e $A \cap C \subset B$ então $a \in B$ por definição de inclusão. Portanto $a \in B$. □

Há uma esquema lógico genérico da ideia empregada acima, vale o seguinte:

$$P_1 \wedge P_2 \wedge \cdots \wedge P_n \Rightarrow (P \to Q) \text{ se, e somente se, } P_1 \wedge P_2 \wedge \cdots \wedge P_n \wedge P \Rightarrow Q.$$

Sobre enunciados Como já dissemos, muitos teoremas afirmam propriedades para todos os elementos de um domínio sem que o quantificador seja explicitamente mencionado, por exemplo,

1. Se 3 divide o inteiro n então 9 divide n^2.
2. Se n é um inteiro ímpar, então n^2 é ímpar.
3. Se $m \in \mathbb{Z}$ é par e $n \in \mathbb{Z}$ é par, então $m + n$ é par.

Essas sentenças significam,

1. Para todo $n \in \mathbb{Z}$, se 3 divide n então 9 divide n^2.
2. Para todo $n \in \mathbb{Z}$, se n é ímpar, então n^2 é ímpar.
3. Para todo $n \in \mathbb{Z}$, para todo $m \in \mathbb{Z}$, se m é par e n é par, então $m + n$ é par.

Em parte, esse comportamento é explicado pelo seguinte. Uma demonstração para uma sentença na forma lógica $\forall x(P(x) \to Q(x))$ tem os seguintes passos:

passo 1 considere c arbitrário do domínio de x

passo 2 prove $P(c) \to Q(c)$

passo 3 conclua $\forall x(P(x) \to Q(x))$ pela regra de inferência da generalização universal.

A parte principal dessa estratégia, onde se concentra todo o trabalho, é a prova da implicação $P(c) \to Q(c)$. Todo o trabalho de demonstrar "Para todo n, se 3 divide n então 9 divide n^2" está concentrado na parte "se 3 divide n então 9 divide n^2" para um número n arbitrário no universo de discurso.

No passo 2, demonstrar $P(c) \to Q(c)$, usando a estratégia direta, por exemplo, assumimos $P(c)$ verdadeiro e usamos regras de inferência, definições, axiomas e equivalências lógicas para concluir que $Q(c)$ é verdadeiro. Isso feito sabemos que $P(c) \to Q(c)$ é verdadeiro o que estabelece o passo 2 descrito acima.

No caso particular de "se 3 divide n então 9 divide n^2" vamos tomar a definição de "divide".

Definição 37. O inteiro k **divide** o inteiro n se, e somente se, existe $q \in \mathbb{Z}$ tal que $kq = n$. Nesse caso escrevemos $k \mid n$ e, também, dizemos que k e q são **fatores** de n.

Agora, vamos demonstrar que se n é um número inteiro arbitrário então

$$\text{se 3 divide o inteiro } n \text{ então 9 divide } n^2 \tag{1.11}$$

DEMONSTRAÇÃO. Seja n um inteiro e assumamos que 3 divide n.

Se $3 \mid n$ então existe $q \in \mathbb{N}$ tal que $n = 3q$, logo $n^2 = 9q^2$. Portanto, n^2 é da forma $9k$, para algum $k \in \mathbb{Z}$, ou seja, 9 divide n^2 por definição. □

Como a variável n acima pode assumir qualquer valor natural, ou seja, n é um elemento genérico de $\mathbb{Z}$, o que provamos de fato foi a seguinte sentença.

TEOREMA 38 *Para todo $n \in \mathbb{Z}$, se 3 divide n então 9 divide n^2.*

Mais um exemplo bastante simples de demonstração direta é a seguinte.

TEOREMA 39 *Para todo $n \in \mathbb{Z}$, se n é ímpar, então n^2 é ímpar.*

DEMONSTRAÇÃO. Seja n um número inteiro arbitrário. Vamos provar que se n é ímpar então n^2 é ímpar.

Assuma n ímpar. Por definição, existe $k \in \mathbb{N}$ tal que $n = 2k+1$. Se $n = 2k+1$ então $n^2 = (2k+1)^2 = 2(2k^2+2k)+1$. Portanto, existe um número ℓ tal que n^2 é da forma $2\ell+1$, ou seja, n^2 é ímpar por definição. □

Usualmente, omitimos das demonstrações os passos muito elementares (já dissemos que isso depende do contexto) e omitimos os passos ubíquos como a menção explícita da generalização universal na conclusão (passo 3 na página anterior) e os *modus ponens*: se temos a premissa A e a condicional $A \to B$, não escrevemos a dedução "de A e $A \to B$, temos B", nesse caso, assim como noutros que usam as regras de inferência, assumimos direto que vale a conclusão, nesse caso B. Por exemplo, no caso "se x é par então é múltiplo de 2" e por hipótese x é par, da sentença condicional já assumimos que x é múltiplo de 2. Ainda, comumente usamos a mesma variável (quantificada) do enunciado para representar o elemento arbitrário do domínio, isto é, a instanciação de "para todo $x \in D, P(x)$" resulta em $P(x)$. Finalmente, embora tenhamos usados símbolos lógicos para explicitar formas e argumentos, **não** éuma boa prática usarxmos símbolos de conectivos e quantificadores para escrever uma demonstração na redação final, é uma questão de estilo e de boa escrita.

Exercício 40. Escreva um escrutínio da demonstração do teorema 39.

Exercício 41. Escreva uma demonstração para o teorema: para todo $x \in \mathbb{N} \setminus \{0\}$, para todo $y \in \mathbb{N}$, se x divide y então x^2 divide y^2. (Nota: a hipótese $x \neq 0$ é desnecessária, devemos cuidar para não enunciar sentenças com hipóteses desnecessárias.)

Demonstração de sentenças sobre conjuntos

Quando precisamos provar sentenças a respeito de conjuntos caímos, essencialmente, em dois tipos de tarefas.

1. Dados x e S, provar que $x \in S$. Isto requer verificar que x satisfaz as propriedades que os elementos de S satisfazem.
2. Dados A e B, provar que $A \subseteq B$. Uma demonstração considera um elemento arbitrário x em A e mostra que ele também deve ser um elemento de B. Note que isso recai no item anterior.

3. Para provar que $A = B$, usualmente, provamos em dois casos: $A \subseteq B$ e $B \subseteq A$.

Vejamos um esboço da demonstração de uma das leis de De Morgan: $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$. Esse é um exemplo em que o item 3 acima pode ser abreviado, não precisamos mostrar as duas inclusões por causa da seguinte sequência de equivalências

$$\begin{aligned}
x \in C \setminus (A \cup B) \Leftrightarrow & \quad x \in C \text{ e } x \notin A \cup B && \text{por definição} \\
\Leftrightarrow & \quad x \in C \text{ e não}(x \in A \cup B) && \text{por definição de } \notin \\
\Leftrightarrow & \quad x \in C \text{ e não}(x \in A \text{ ou } x \in B) && \text{por definição de } \cup \\
\Leftrightarrow & \quad x \in C \text{ e não}(x \in A) \text{ e não}(x \in B) && \text{por De Morgan (lógico)} \\
\Leftrightarrow & \quad x \in C \text{ e } x \notin A \text{ e } x \notin B && \text{por definição} \\
\Leftrightarrow & \quad x \in C \text{ e } x \notin A \text{ e } x \in C \text{ e } x \notin B && \text{por definição} \\
\Leftrightarrow & \quad x \in (C \setminus A) \cap (C \setminus B) && \text{por definição de } \cap .
\end{aligned}$$

Reescrevendo de modo a torná-la mais apresentável resulta na seguinte demonstração.

DEMONSTRAÇÃO. Sejam A, B e C conjuntos e vamos provar que $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$. Por definição $x \in C \setminus (A \cup B)$ se, e só se, $x \in C$ e $x \notin A \cup B$. Mas, $x \notin A \cup B$ se, e só se, $x \notin A$ e $x \notin B$ de sorte que $x \in C \setminus (A \cup B)$ se, e só se, $x \in C$ e $x \notin A$ e $x \notin B$, ou seja, , ou seja, $x \in (C \setminus A) \cap (C \setminus B)$. Portanto, $x \in C \setminus (A \cup B)$ se, e só se, $x \in (C \setminus A) \cap (C \setminus B)$, donde concluímos que $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$. □

1.3.3 Demonstração de equivalências

Para demonstrar que uma sentença da forma $P \leftrightarrow Q$ é verdadeira nem sempre conseguimos uma sequência de sentenças equivalentes como no exemplo anterior. Ao invés disso nós usamos que $(P \leftrightarrow Q)$ é logicamente equivalente a $(P \leftarrow Q) \wedge (P \rightarrow Q)$ e, de fato, escrevemos duas demonstrações para implicação, provamos $P \rightarrow Q$ e a sua recíproca $Q \rightarrow P$. Cada uma dessas duas implicações pode ser demonstrada com alguma das técnicas para demonstrar uma implicação.

TEOREMA 42 *Para todos $a, b \in \mathbb{Z}$ não nulos, $a \mid b$ e $b \mid a$ se, e somente se, $a = b$ ou $a = -b$.*

DEMONSTRAÇÃO. Sejam a e b números inteiros.

Primeiro, suponha que $a = b$ ou $a = -b$. Em cada um desses dois casos, $a \mid b$ e $b \mid a$ seguem imediatamente da definição.

Agora, suponha que $a \mid b$ e $b \mid a$. Se $a \mid b$ então existe um inteiro k tal que $ak = b$ e se $b \mid a$ então existe um inteiro q tal que $bq = a$, logo, $(bq)k = b$ donde tiramos que $qk = 1$, portanto, do item 13, página 28 concluímos que $a = b$ ou $a = -b$. □

TEOREMA 43 *Nos inteiros são equivalentes as afirmações:*

(i) Para todos a, b e $c \neq 0$, se $ac = bc$ então $a = b$.

(ii) Para todos a e b, se $ab = 0$ então $a = 0$ ou $b = 0$.

DEMONSTRAÇÃO. Vamos assumir que (i) é verdadeiro é demonstrar (ii).

Para provar (ii), sejam a e b inteiros tais que $ab = 0$. Se $a \neq 0$ então de $ab = a0$ temos, por (i) que $b = 0$. Por outro lado, se $b \neq 0$ então de $ab = 0b$ e temos que $a = 0$. Portanto, $a = 0$ ou $b = 0$.

Agora, vamos assumir que (ii) é verdadeiro é demonstrar (i).

Para provar (i), sejam a, b e c inteiros com $c \neq 0$ e tais que $ac = bc$. Se $ac = bc$, então $ac - bc = 0$. Fatorando o produto temos $(a - b)c = 0$ e, por (i), $a - b = 0$ já que $c \neq 0$. Se $a - b = 0$ então $a = b$. □

1.3.4 Demonstração indireta de implicação

Nesse tipo de prova demonstramos que é verdadeira uma sentença logicamente equivalente a $P \rightarrow Q$, como a contrapositiva, por exemplo.

Demonstração pela contrapositiva: Para provar que $P \rightarrow Q$ é verdadeira demonstramos $\neg Q \rightarrow \neg P$ é verdadeira.

Por exemplo, para um número natural n arbitrário, a seguinte implicação é verdadeira (tente uma prova direta)

$$\text{se } n^2 \text{ é par, então } n \text{ é par.} \tag{1.12}$$

A contrapositiva de (1.12) é, assumindo que ímpar é a negação de par (veja corolário 70),

$$\text{se } n \text{ é ímpar, então } n^2 \text{ é ímpar.}$$

que é verdadeira, como foi estabelecido pelo teorema 39.

Definição 44. O **maior divisor comum** dos inteiros a, b, denotado $\text{mdc}(a,b)$ é dado por

$$\text{mdc}(a,b) := \begin{cases} 0, & \text{se } a = b = 0, \\ \max\{ d \in \mathbb{N} \colon d \,|\, |a| \text{ e } d \,|\, |b| \}, & \text{caso contrário.} \end{cases} \tag{1.13}$$

Os inteiros a e b são ditos **coprimos** se, e só se, $\text{mdc}(a,b) = 1$.

Observamos que se d é um natural que divide $|a|$ então $d \leqslant |a|$, portanto o conjunto de todos os divisores de a tem um maior elemento. Se $a = 0$ então todo inteiro é divisor de a, portanto o conjunto de todos os divisores de a não tem um maior elemento. Analogamente, o conjunto de todos os divisores de $b \neq 0$ tem um maior elemento. Disso, o $\text{mdc}(a,b)$ está bem definido por (1.13).

Teorema 45 *Para todos $a, b \in \mathbb{N}$, se a e b são coprimos, então a não é par ou b não é par.*

Vamos demonstrar pela contrapositiva que se a e b são coprimos então não são ambos par. Antes o leitor é convidado a dar uma prova direta da sentença. Demonstrar a contrapositiva significa provar que vale a sentença

$$\text{se } a \text{ é par e } b \text{ é par, então } \text{mdc}(a,b) \neq 1. \tag{1.14}$$

para todos $a, b \in \mathbb{Z}$. A estratégia é clara nesse caso: (1) Tome a par e b par; (2) $2 \,|\, a$ e $2 \,|\, b \Rightarrow \text{mdc}(a,b) \geqslant 2$; (3) portanto $\text{mdc}(a,b) \neq 1$. Pela generalização universal, pois a e b são inteiros arbitrários, vale que a equação (1.14) é verdadeira. Passemos a demonstração.

Demonstração do teorema 45. Vamos provar o teorema 45 pela contrapositiva. Sejam a e b números inteiros quaisquer e assumamos que a é par e que b é par. Então, pela definição, 2 divide a e divide b, logo o $\text{mdc}(a,b)$ é pelo menos 2. Portanto, $\text{mdc}(a,b) \neq 1$. □

Demonstração por contradição: Para demonstrar que vale $P \to Q$ nós demonstramos a veracidade da condicional $(P \wedge \neg Q) \to \mathbf{F}$.

A regra da contradição, dada na página 12, é a consequência lógica

$$\neg A \to \mathbf{F} \Rightarrow A$$

e fazendo A ser a sentença $P \to Q$, cuja negação é $P \wedge \neg Q$, justifica tal equivalência lógica.

Assim, numa demonstração por contradição assumimos que a hipótese é verdadeira e a *negação* da sentença a ser provada é verdadeira e, com essas hipótese, derivamos uma *contradição*. Um exemplo de estratégia para prova por contradição é

1)	P	(por hipótese)
2)	$\neg Q$	(por hipótese)
3)	$\neg P$	(por dedução)
4)	$P \wedge \neg P$	(pela regra da conjunção)

De fato, na linha 3 deduzimos alguma sentença que junto com as premissas formam uma sentença lógica falsa. Também, pode ser o caso em que a contradição seja alguma outra sentença que negue algum teorema (alguma sentença que é sabida ser verdadeira). Veja o exemplo 50 mais adiante.

Demonstração do teorema 45. A demonstração é por contradição. Sejam a e b números inteiros arbitrários. Assumamos que a e b são coprimos. Se a é par e b é par então $\text{mdc}(a,b) \geqslant 2$, ou seja, $\text{mdc}(a,b) = 1$ e $\text{mdc}(a,b) \geqslant 2$, uma contradição. Portanto, se a e b são coprimos, então a e b não são ambos números pares. □

Um caso clássico de prova do contradição é o da irracionalidade da raiz de dois.

Definição 46. O número real x é **racional** se existem números inteiros n e m, com $m \neq 0$, tais que $x = \frac{n}{m}$. O conjunto de todos os números racionais é denotado por $\mathbb{Q}$.

Se x não é racional então x é **irracional** e $\mathbb{R} \setminus \mathbb{Q}$ é o conjunto dos números irracionais.

Teorema 47 *$\sqrt{2}$ é irracional.*

Essa sentença pode ser enunciada usando uma condiconal

Para todo real x, se $x^2 = 2$ então x é irracional.

A prova segue assumindo que $x^2 = 2$ e que $x \in \mathbb{Q}$.

Demonstração tirada do livro de Bases Matemáticas, de A. Caputi e D. Miranda. Faremos a demonstração pelo método de redução ao absurdo. Ou seja, supomos que $\sqrt{2}$ é um número racional, i.e., que existem números inteiros positivos a e b tais que $\frac{a}{b} = \sqrt{2}$ ou, equivalentemente $\left(\frac{a}{b}\right)^2 = 2$.

Podemos supor que a e b não são ambos números pares, pois se fossem, poderíamos simplificar a fração até termos que pelo menos um dos termos da fração seja ímpar.

Agora, escrevemos $\left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2} = 2$, então:

$$qa^2 = 2b^2 \tag{1.15}$$

Concluímos então que a^2 é um número par, pois é dobro de b^2. Logo a também deve ser par, pois se a fosse ímpar o seu quadrado também seria ímpar.

Temos então que a é um número par e, portanto, é o dobro de algum número inteiro, digamos k: $a = 2k$. em (1.15) temos:

$$(2k)^2 = 2b^2 \Rightarrow 4k^2 = 2b^2 \Rightarrow 2k^2 = b^2.$$

De modo análogo, temos que b deve ser um número par. O que é absurdo pois a e b não são ambos números pares. Portanto, $\sqrt{2}$ tem que ser um número irracional. Como queríamos demonstrar. □

O método da redução ao absurdo mencionado na demonstração é como também é chamado o método da contradição. Um escrutínio dessa demonstração é apresentado na tabela 1.8. Nela usamos que todo racional pode ser escrito como uma fração

1)	$\sqrt{2} \in \mathbb{Q}$	(premissa)
2)	$\sqrt{2} \in \mathbb{Q} \rightarrow \exists a, b \in \mathbb{N}$ coprimos e $\sqrt{2} = \frac{a}{b}$.	(corolário 49 dado abaixo)
3)	$\exists a, b \in \mathbb{N}$ coprimos e $\sqrt{2} = \frac{a}{b}$.	(modus ponens)
4)	$\sqrt{2} = \frac{a}{b}$ e a e b são coprimos.	(instanciação existencial)
5)	a e b são coprimos.	(regra da simplificação)
6)	$\sqrt{2} = \frac{a}{b}$.	(regra da simplificação)
7)	Se $\sqrt{2} = \frac{a}{b}$ então $2 = \left(\frac{a}{b}\right)^2$.	(compatibilidade)
$7\frac{1}{2}$)	Se $2 = \left(\frac{a}{b}\right)^2$ então $2 = \frac{a^2}{b^2}$.	(propriedade da potência)
8)	Se $2 = \frac{a^2}{b^2}$ então $a^2 = 2b^2$.	(compatibilidade)
9)	Se $\sqrt{2} = \frac{a}{b}$ então $a^2 = 2b^2$.	(silogismo)
10)	$a^2 = 2b^2$.	(modus ponens)
11)	Se $a^2 = 2b^2$ então a^2 é par.	(definição de par)
12)	Se a^2 é par então a é par	(contrapositiva teo. 39)
13)	Se $a^2 = 2b^2$ então a é par	(silogismo)
14)	a é par	(modus ponens)
15)	Se a é par então existe $k \in \mathbb{N}$, $a = 2k$.	(definição de par)
16)	Existe $k \in \mathbb{N}$, $a = 2k$.	(modus ponens)
17)	$a = 2k$.	(instanciação universal)
18)	$a = 2k$ e $a^2 = 2b^2$.	(conjunção)
19)	Se $a = 2k$ e $a^2 = 2b^2$ então $4k^2 = 2b^2$.	(compatibilidade)
$19\frac{1}{2}$)	Se $4k^2 = 2b^2$ então $2k^2 = b^2$.	(compatibilidade)
20)	Se $b^2 = 2k^2$ então b^2 é par.	(definição de par)
21)	Se b^2 é par então b é par.	(contrapositiva teo. 39)
22)	Se $a = 2k$ e $a^2 = 2b^2$ então b é par.	(silogismos)
23)	b é par.	(modus ponens)
24)	a é par e b é par.	(conjunção)
25)	a e b coprimos e a é par e b é par.	(contradição)

Tabela 1.8: Um escrutínio da demonstração da irracionalidade de $\sqrt{2}$.

de números coprimos, a qual chamamos de **forma reduzida**. Para demonstrar que toda fração tem uma forma reduzida vamos primeiro mostrar um resultado mais poderoso.

O que precisamos para usar na linha 2 da tabela 1.8 acima seguirá como corolário do seguinte resultado.

TEOREMA 48 *Para todo $d \in \mathbb{N}^*$ e todo $e \in \mathbb{N}^*$*

$$\text{mdc}\left(\frac{d}{\text{mdc}(d,e)}, \frac{e}{\text{mdc}(d,e)}\right) = 1.$$

Nesse caso, vamos provar que se o mdc acima for maior que 1 então temos um contradição. O resultado segue da regra da contradição pois inferimos que o mdc é $\leqslant 1$ e como não são ambos os números iguais a 0 temos por definição de mdc que o mdc é $\geqslant 1$. Portanto concluímos que vale a igualdade, isto é, o mdc vale 1.

DEMONSTRAÇÃO. Sejam d e e números naturais arbitrários e não nulos. Façamos, para fins de simplificação,

$$m := \text{mdc}(d,e) \text{ e } k := \text{mdc}\left(\frac{d}{m}, \frac{e}{m}\right).$$

Vamos assumir $k > 1$. Pela definição de mdc, k divide $\frac{d}{m}$ e k divide $\frac{e}{m}$.

Se k divide $\frac{d}{m}$ então km divide d. (verifique) Logo km divide d. Analogamente, km divide e.

Se $k > 1$ então $km > m$. Se $km \mid d$ e $km \mid e$ então $km \leqslant m$, pois m é o maior divisor de d e e.

Portanto $km > m$ e $km \leqslant m$, uma contradição. □

COROLÁRIO 49 *Todo número racional pode ser escrito como $\frac{a}{b}$ com a e b coprimos.*

DEMONSTRAÇÃO. Seja q um racional arbitrário. Por definição, existem inteiros n e $m \neq 0$ tais que $q = \frac{n}{m}$. Faça $d = \text{mdc}(n,m)$, $a = \frac{n}{d}$ e $b = \frac{m}{d}$ que temos, pelo teorema anterior, $\text{mdc}(a,b) = 1$. Portanto $q = \frac{n}{m} = \frac{a}{b}$. □

Exemplo 50 (Outra prova de que $\sqrt{2} \notin \mathbb{Q}$). Suponha $\sqrt{2} = \frac{p}{q}$ de modo que $2 = \frac{p^2}{q^2}$. Escreva, $q^2 = 2^k r$ com r ímpar; isso pode ser feito por causa do teorema fundamental da aritmética (teorema 73, página 41). Por $2^k r$ ser um quadrado k tem que ser par. Por outro lado $p^2 = 2q^2 = 2^{k+1} r$ e por $2^{k+1} r$ ser um quadrado k é impar. Portanto k é par e k é ímpar, o que é uma contradição (pelo corolário 70, pagína 41).

A seguir damos um exemplo de prova de uma equivalência usando métodos diferentes para cada condicional.

TEOREMA 51 *Para todo $n \in \mathbb{Z}$, n é ímpar se, e somente se, n^2 é ímpar.*

DEMONSTRAÇÃO. Seja $n \in \mathbb{Z}$ arbitrário. Vamos provar que n^2 ímpar se, e só se, n ímpar.

Vamos assumir que n é ímpar. Então n^2 é ímpar pelo teorema 39.

Agora, vamos assumir que n^2 ímpar e provar que n ímpar. A prova é por contradição, suponha que n é par. Então $n = 2k$ para algum $k \in \mathbb{Z}$ e se $n = 2k$, então $n^2 = 4k^2$, ou seja, n^2 é par e n^2 ímpar, uma contradição. Portanto, se n^2 é ímpar então n é ímpar.

Portanto n^2 ímpar se, e só se, n ímpar, para todo natural n. □

COROLÁRIO 52 *Para todo $n \in \mathbb{Z}$, n é par se, e somente se, n^2 é par.*

DEMONSTRAÇÃO. Exercício. □

1.3.5 Demonstração por vacuidade e prova trivial

Estabeleceremos que a sentença $P \to Q$ é verdadeira se assegurarmos que P é falso, independentemente do valor lógico de Q, ou assegurarmos que Q é verdadeiro, independentemente do valor de P. No primeiro caso chamamos de *prova por vacuidade* e no segundo *prova trivial*.

Um exemplo de prova por vacuidade foi dado no teorema 34, na página 30, de que vazio é subconjunto de qualquer conjunto A, isso vale por vacuidade com a condicional que define a inclusão $x \in \varnothing \to x \in A$.

Os dois próximos exemplo são irrelevantes do ponto de vista matemático e servem apenas para ilustração.

TEOREMA 53 *Se x é um número real tal que $x^2 + 1 < 0$ então $x^5 \geqslant 4$.*

Isso é um teorema pois para qualquer real x temos que $x^2 \geqslant 0$, logo $x^2 + 1 > 0$.

TEOREMA 54 *Se $n > 3$ é um número par e primo, então n é da forma $4n+1$.*

Isso é um teorema pois não há número primo par maior que 3. Uma curiosidade é que existem infinitos números primos da forma $4n+1$, mas todos são ímpares pois são da forma $2(2n)+1$.

Notemos que a contrapositiva do primeiro teorema afirma que "se $x^5 < 4$ então $x^2 + 1 \geqslant 0$". Como a conclusão é sempre verdadeira a implicação também será, isto é, "se $x^5 < 4$ então $x^2 + 1 \geqslant 0$" é verdadeiro porque $x^2 + 1 \geqslant 0$ é verdadeiro. Essa é uma prova trivial.

Consideremos o predicado "se $n > 1$ então $n^2 > n$" para números naturais. Por vacuidade vale "se $0 > 1$ então $0^2 > 0$" e também vale "se $1 > 1$ então $1^2 > 1$", qualquer outro valor de n é maior que 1 e, se $n > 1$ é verdadeiro, então $n^2 > n$ é verdadeiro, pois deduzimos multiplicando ambos os lados na desigualdade da hipótese por n.

Exercício 55. A sentença:

$$\text{para todo } n \in \mathbb{N}^*, \text{ se } n + \tfrac{1}{n} < 2 \text{ então } n^2 + \left(\tfrac{1}{n}\right)^2 < 2$$

é verdadeira? Demonstre ou dê um contraexemplo para justificar a resposta.

1.3.6 Demonstração por casos

O argumento por casos para $P \to Q$ é usado quando P é equivalente na forma $P_1 \vee P_2 \vee \cdots \vee P_n$ baseado na equivalência lógica

$$((P_1 \vee P_2 \vee \cdots \vee P_n) \to Q) \text{ se e somente se } ((P_1 \to Q) \wedge (P_2 \to Q) \wedge \cdots \wedge (P_n \to Q))$$

as implicações $P_i \to Q$ são os casos. Um cuidado importante nessa estratégia é assegurar que $P_1 \vee P_2 \vee \cdots \vee P_n$ equivale a P ou que nenhum caso é deixado de lado. Por exemplo, se P afirma algo sobre inteiros podemos escrevê-la como a disjunção dos casos "inteiros positivos", "inteiros negativos" e o "inteiro nulo" (o 0, que não é negativo, nem positivo), como na sentença

$$\text{para todo inteiro } n,\ n^2 \geqslant n$$

DEMONSTRAÇÃO. Seja n um inteiro artbitrário. Então $n \leqslant -1$ ou $n = 0$ ou $n \geqslant 1$.

1. Caso $n = 0$: se $n = 0$ então $n^2 = 0^2 = 0 = n$, portanto $n^2 \geqslant n$.
2. Caso $n \geqslant 1$: se $n \geqslant 1$ então $n^2 \geqslant n$, multiplicando os dois lados da desigualdade por n, portanto $n^2 \geqslant n$.
3. Caso $n \leqslant -1$: se $n \leqslant -1$ então $n^2 \geqslant n$. Suponha $n \leqslant -1$, então $n < 0$. Se $n < 0$ e $0 \leqslant n^2$ então $n \leqslant n^2$.

Portanto, para todo n natural, $n^2 \geqslant n$. □

TEOREMA 56 *Para todo $n \in \mathbb{Z}$, $n^2 + 3n + 5$ é ímpar.*

DEMONSTRAÇÃO. Seja n um inteiro arbitrário. Vamos provar que $n^2 + 3n + 5$ é ímpar em dois casos: (1) $2 \mid n$ e (2) $2 \nmid n$.
Caso 1: Assuma que $2 \mid n$. Se $2 \mid n$ então $n = 2k$ para algum inteiro k e

$$n^2 + 3n + 5 = (2k)^2 + 3(2k) + 5 = 2(2k^2 + 3k + 2) + 1$$

portanto $n^2 + 3n + 5$ é ímpar.
Caso 2: Assuma $2 \nmid n$. Se $2 \nmid n$ então $n = 2k + 1$ para algum inteiro k e

$$n^2 + 3n + 5 = (2k + 1)^2 + 3(2k + 1) + 5 = 2(2k^2 + 5k + 4) + 1.$$

logo $n^2 + 3n + 5$ é ímpar. Portanto, para todo n inteiro, $n^2 + 3n + 5$ é ímpar. □

Algumas situações não deixam alternativa a não ser uma prova exaustiva, como no próximo exemplo.

TEOREMA 57 *Seja n um número inteiro. Se $1 \leqslant n \leqslant 40$ então $n^2 - n + 41$ é primo.*

DEMONSTRAÇÃO. Defina $f(n) = n^2 - n + 41$.
$f(1) = 41$ é primo, $f(2) = 43$ é primo, $f(3) = 47$ é primo, $f(4) = 53$ é primo, $f(5) = 61$ é primo, $f(6) = 71$ é primo, $f(7) = 83$ é primo, $f(8) = 97$ é primo, $f(9) = 113$ é primo, $f(10) = 131$ é primo, $f(11) = 151$ é primo, $f(12) = 173$ é primo, $f(13) = 197$ é primo, $f(14) = 223$ é primo, $f(15) = 251$ é primo, $f(16) = 281$ é primo, $f(17) = 313$ é primo, $f(18) = 347$ é primo, $f(19) = 383$ é primo, $f(20) = 421$ é primo, $f(21) = 461$ é primo, $f(22) = 503$ é primo, $f(23) = 547$ é primo, $f(24) = 593$ é primo, $f(25) = 641$ é primo, $f(26) = 691$ é primo, $f(27) = 743$ é primo, $f(28) = 797$ é primo, $f(29) = 853$ é primo, $f(30) = 911$ é primo, $f(31) = 971$ é primo, $f(32) = 1033$ é primo, $f(33) = 1097$ é primo, $f(34) = 1163$ é primo, $f(35) = 1231$ é primo, $f(36) = 1301$ é primo, $f(37) = 1373$ é primo, $f(38) = 1447$ é primo, $f(39) = 1523$ é primo, $f(40) = 1601$ é primo. □

Exercício 58. A demonstração por casos em geral é útil para provar propriedades do valor absoluto, porque esse é definido por casos. Sejam a e $b \neq 0$ números reais. Demonstre que $\left|\frac{a}{b}\right| = \frac{|a|}{|b|}$.

1.3.7 Demonstrações existenciais

Para provar uma sentença da forma lógica $\exists x \in D,\ P(x)$ podemos exibir um elemento do domínio D para o qual o predicado P vale ou inferir indiretamente que tal elemento existe, por exemplo, derivando uma contradição caso assumamos a não existência de um tal elemento. Esses dois casos são, usualmente, classificadas como demonstrações construtivas e demonstrações não construtivas.

Demonstração construtiva: Exibe um elemento c do universo tal que $P(c)$ seja verdade.

Demonstração não-construtiva: Infere, indiretamente, a existência de um objeto que torna $P(x)$ verdadeira.

Exercício 59. Prove que existe um quadrado perfeito da forma $1 + 13n$, para $n \geqslant 1$ natural.

TEOREMA 60 *Existe um inteiro positivo n que pode ser escrito como a soma de dois cubos de duas maneiras diferentes.*

Demonstração (construtiva). Faça $n = 1729$ e temos $1729 = 10^3 + 9^3 = 12^3 + 1^3$. □

TEOREMA 61 *Existem x, y irracionais tais que x^y é racional.*

Demonstração (não-construtiva). Sabemos que $\sqrt{2}$ é irracional. Prosseguimos em dois casos, o número $\sqrt{2}^{\sqrt{2}}$ é racional ou irracional.

Caso 1: Se $\sqrt{2}^{\sqrt{2}}$ é racional então faça $x = y = \sqrt{2}$ e temos x^y racional.

Caso 2: Se $\sqrt{2}^{\sqrt{2}}$ é irracional então faça $x = \sqrt{2}^{\sqrt{2}}$ e $y = \sqrt{2}$ e temos

$$x^y = \sqrt{2}^{\sqrt{2}^{\sqrt{2}}} = \sqrt{2}^2 = 2$$

que é racional.

Portanto existem x, y irracionais com x^y racional. □

É possível provar que $\sqrt{2}^{\sqrt{2}}$ é irracional, é consequência do teorema de Gelfond–Schneider, um resultado da teoria dos números bastante difícil para exibirmos aqui.

TEOREMA 62 *Para todo racional y, existe um inteiro x tal que $y < x$.*

Demonstração (construtiva). Seja $\frac{p}{q}$ um racional arbitrário. Vamos exibir um inteiro n tal que $\frac{p}{q} < n$.

Faça $n = |p| + 1$. Temos da definição de valor absoluto que $\frac{p}{q} \leqslant |\frac{p}{q}|$. Ademais $|\frac{p}{q}| \leqslant |p|$ e $|p| < |p| + 1$. Portanto $\frac{p}{q} < |p| + 1$. □

TEOREMA 63 *O polinômio $p(x) = x^3 + x - 1$ tem exatamente uma raiz real.*

Nesse enunciado temos duas afirmações a serem demonstradas. A primeira é que o polinômio tem raiz. A segunda é que a raiz do passo anterior é única.

Demonstração (não-construtiva). Seja $p(x) = x^3 + x - 1$. Então p é uma função real e contínua em todo intervalo da reta real.

Pelo Teorema do Valor Intermediário, para todo $b \in [p(0), p(1)]$, existe $a \in [0, 1]$ tal que $p(a) = b$. Como $p(0) = -1$ e $p(1) = 1$ temos $0 \in [p(0), p(1)]$ assim fazendo $b = 0$ concluímos, pelo enunciado acima, que existe $a \in [0, 1]$ tal que $p(a) = 0$. Portanto a é raiz de p.

Agora, vamos demonstrar que essa raiz é única. A prova é por gg contradição. Suponha que p tenha pelo menos duas raízes. Sejam r_1 e r_2 raízes distintas de $p(x)$, sem perda de generalidade, $r_1 < r_2$.

Como $p(x)$ é contínua em $[r_1, r_2]$ e derivável em (r_1, r_2), pelo Teorema do Valor Médio existe um ponto $c \in [r_1, r_2]$ tal que

$$p'(c) = \frac{p(r_2) - p(r_1)}{r_2 - r_1}$$

mas $p(r_2) - p(r_1) = 0$, portanto $p'(c) = 0$ que é uma contradição pois o $p'(x) = 3x^2 + 1 > 0$ qualquer que seja x. Portanto, não pode haver duas raízes de p. □

Exercício 64. Prove que existe um real que é a raiz quadrada principal de 2. Note que, dado que existe $x \in \mathbb{R}$ positivo tal que $x^2 = 2$, então tal número é irracional de modo que não conseguimos escrever tal número, ou seja, é preciso dar uma prova indireta de sua existência.

1.3.8 Mais exemplos - demonstração de algumas propriedades de inteiros

Vamos começar essa seção com um prova da propriedade arquimediana dos inteiros dada na página 29: *dados $a, b \in \mathbb{Z}$ com $b \neq 0$, existe um n tal que $nb > a$.*

Demonstração do item 38, página 29. Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$, arbitrários.

Se $|b| \neq 0$, então $|b| \geqslant 1$. Logo $(|a|+1)\cdot|b| \geqslant |a|+1$ e, também, $|a|+1 > |a| \geqslant a$, ou seja, $(|a|+1)\cdot|b| > a$ por transitividade. Agora, se $b > 0$ então tomamos $n = |a|+1$ e se $b < 0$ então tomamos $n = -(|a|+1)$. Em ambos os casos $nb > a$. □

Usando o PBO

O próximo resultado tem como corolário que não existe um número inteiro entre dois inteiros "consecutivos" quaisquer.

TEOREMA 65 *Prove que não existe natural p tal que $0 < p < 1$.*

DEMONSTRAÇÃO. A prova é por contradição. Vamos assumir que $p \in \mathbb{N}$ é tal que $0 < p < 1$. Com isso temos que $A := \{x \in \mathbb{N} : 0 < x < 1\}$ é um subconjunto não vazio dos naturais e pelo PBO existe $m = \min(A)$. De $m > 0$, temos $m^2 > 0$. De $m < 1$, temos $m^2 < m$ e como $m < 1$ deduzimos que $m^2 < 1$, logo $m^2 \in A$ e $m^2 < \min(A)$, uma contradição. □

Agora, vamos provar que toda sequência não-crescente de números naturais é constante a partir de um algum momento.

Definição 66. Uma **sequência numérica** $a_0, a_1, a_2, \ldots$, denotada por (a_n) é uma função $f : \mathbb{N} \to A$, onde A é um conjunto de números, tal que $f(n) = a_n$.

A sequência é **não-crescente** se, e só se, $x < y$ implica $f(x) \geqslant f(y)$ e é **não-decrescente** se, e só se, $x < y$ implica $f(x) \leqslant f(y)$.

A sequência é **crescente** se, e só se, $x < y$ implica $f(x) < f(y)$ e é **decrescente** se, e só se, $x < y$ implica $f(y) < f(x)$.

PROPOSIÇÃO 67 *Para toda sequência (a_n) não-crescente de números naturais, existe um natural n_0 a partir do qual a é constante.*

DEMONSTRAÇÃO. Seja (a_n) uma sequência não-crescente de números naturais. Seja f a função que define (a_n).

A imagem da função, $\mathrm{Im}(f)$, é um subconjunto não vazio de naturais. Seja n_0 um natural tal que $f(n_0)$ é o menor elemento de $\mathrm{Im}(f)$, esse menor elemento existe pelo PBO. Como f é não-crescente, se $n > n_0$ então $f(n) \leqslant f(n_0)$, mas $f(n) \not< f(n_0)$ pois $f(n_0)$ é o menor elemento de $\mathrm{Im}(f)$, portanto $n > n_0 \Rightarrow f(n) = f(n_0)$. □

COROLÁRIO 68 (PRINCÍPIO DA DESCIDA INFINITA DE FERMAT) *Não existe uma sequência decrescente de números naturais.* □

Podemos usar o princípio de Fermat para dar a seguinte prova de que $\sqrt{2}$ não é racional.

Esboço de uma demonstração de $\sqrt{2} \notin \mathbb{Q}$ usando o corolário 68. Suponha que existam inteiros p e q tais $\sqrt{2} = \frac{p}{q}$. Então $2q^2 = p^2$, donde concluímos que p é par. Mas se assim for, então $2q^2 = (2p_1)^2$, ou seja, $q^2 = 2k^2$, donde concluímos que p é par, $q = 2q_1$. Repetindo esse argumento encontramos $p > p_1 > p_2 > \cdots$, contrariando o corolário 68. □

Agora provaremos o teorema da divisão euclidiana. Na aritmética, a divisão euclidiana ou divisão inteira é uma operação que, com dois inteiros não nulos chamados dividendo e divisor, associa dois outros inteiros chamados quociente e resto, que é menor que o divisor. Sua principal propriedade é que o quociente e o resto existem e são únicos Essa divisão está na base dos teoremas da aritmética elementar, como a aritmética modular que dá origem à criação de congruências em inteiros e o algoritmo euclidiano para encontrar o maior divisor comum de dois inteiros.

Pode-se também definir uma divisão euclidiana em outros conjuntos, como o anel de polinômios ou outros anéis. O termo "divisão euclidiana" foi surgiu no século XX como uma abreviação para "divisão em anéis euclidianos". Embora a divisão tenha o nome associado a Euclides, acredita-se que ele não conhecia o teorema e que o único método de computação que ele conhecia era a divisão por subtração repetida. Curiosamente, antes da descoberta do sistema numeral hindu-arabico (400 aC), cuja utilização na Europa Ocidental se deve muito a Fibonacci no século XIII, a divisão era extremamente difícil, e apenas os melhores matemáticos eram capazes de fazê-lo.

TEOREMA 69 (TEOREMA DA DIVISÃO EUCLIDIANA) *Para todo inteiro a e todo inteiro $b > 0$ existe um único inteiro q e existe um único inteiro r tal que*

$$a = qb + r \;\; e \;\; 0 \leqslant r < b.$$

DEMONSTRAÇÃO. Sejam a e b inteiros com $b > 0$.

Definimos

$$R := \{a - nb : n \in \mathbb{Z}\}$$

e temos que $R \cap \mathbb{N} \neq \varnothing$ pois para $n = -|a|b$ temos $a + |a|b^2 \geqslant a + |a| \geqslant 0$ pertence a $R \cap \mathbb{N}$. Seja r o menor inteiro positivo de $R \cap \mathbb{N}$, que existe pelo princípio da boa-ordem, então $r \geqslant 0$ é da forma

$$r = a - qb$$

para algum q.

Se $r \geqslant b$ então $r - b \geqslant 0$ e

$$r - b = a - (q+1)b \in R \cap \mathbb{N}$$

e $r - b < r$, uma contradição pois r é mínimo de $R \cap \mathbb{N}$.

Falta provar que r e q são únicos. Suponha que $a = q_1 b + r_1$ e $a = q_2 b + r_2$. Se $r_1 \neq r_2$, então $(q_2 - q_1)b = r_1 - r_2$, logo $b \mid r_1 - r_2$. Porém, $-b < r_1 - r_2 < b$, e temos uma contradição. Logo $r_1 = r_2$ e $q_1 = q_2$. □

COROLÁRIO 70 *Para todo natural n, se n não é par então n é ímpar.*

DEMONSTRAÇÃO. Seja n um natural. Pelo teorema da divisão existe $q_1 \mathbb{Z}$ e $r \in \{0,1\}$ tal que $n = 2q + r$. Se n não é par então $r \neq 0$, logo $r = 1$, ou seja, n é ímpar. □

Exercício 71. Enuncie e prove o teorema da divisão para todo inteiro $b \neq 0$.

Agora, provaremos outro resultado importante, o **teorema fundamental da aritmética** afirma que todo número inteiro maior que 1 é primo ou pode ser decomposto num produto fatores primos e esta decomposição é única a menos da permutações dos fatores. Por exemplo, podemos fatorar 6936 como $23 \cdot 3 \cdot 172$ e não há nenhuma outra fatoração de 6936 como primo ou produto de primos, com exceção de um rearranjo dos fatores acima como, por exemplo, $3 \cdot 23 \cdot 172$.

Como no teorema da divisão, esse resultado pode ser generalizado para outros conjuntos, os anéis de fatoração única, tais como os anéis de polinômios com coeficientes nos números reais ou complexos. Carl Friedrich Gauss, em seu livro *Disquisitiones arithmeticae* desenvolve a aritmética em outras estruturas nos quais a existência de uma fatoração única vale, como é o caso dos polinômios com coeficientes em um corpo e o caso do anel de inteiros algébricos, os inteiros de Gauss. A noção de número primo é então estendida nessas estruturas (polinômios irredutíveis e os números primos de Gauss).

Definição 72. Um número natural maior que 1 é **primo** se, e só se, tem exatamente dois divisores positivos, o 1 e o próprio número. Um número natural maior que 1 que não é primo é dito **composto**, o qual tem um divisor positivos diferente do 1 e do próprio número.

TEOREMA 73 (TEOREMA FUNDAMENTAL DA ARITMÉTICA) *Para todo $n \in \mathbb{N}$, se $n > 1$ então n é primo ou pode ser escrito como produto de números primos, ademais tal escrita é única a menos da ordem com que se escreve os fatores primos.*

DEMONSTRAÇÃO. Seja $n > 1$ um natural. A prova é por contradição. Assuma que exista $n > 1$ natural que não é primo e não pode ser escrito como produto de primos e defina o conjunto não vazio A formado por todos naturais com tal propriedade.

Pelo PBO o conjunto A tem um mínimo m. Como m não é primo, tem um divisor $a \neq 1, m$, isto é, existe $q \in \mathbb{N}$ tal que $m = a \cdot q$. Claramente, $1 < a, q < m$. Como m é mínimo a e q são primos ou produtos de primos e em todos os casos m é produto de primos, assim temos uma contradição. □

Exercício 74. Prove que há um único modo de escrever $n > 1$ como produto de primos, exceto pela ordem dos fatores.

COROLÁRIO 75 *Se $n \neq -1, 0, 1$ é inteiro então existem primos $p_1, \ldots, p_k$ tais que $n = \pm p_1 p_2 \cdots p_k$.*

Vejamos uma prova existencial construtiva para outra propriedade de inteiros dada na página 29: *todo $A \subset \mathbb{Z}$ não vazio e limitado inferiormente tem um menor elemento.*

Demonstração do item 37, página 29. Seja $A \subset \mathbb{Z}$ um subconjunto limitado inferiormente e seja m é uma cota inferior de A. Defina o conjunto

$$B = \{a - m \colon a \in A\}.$$

Então $B \subset \mathbb{N}$ e $B \neq \varnothing$, logo, para algum $b \in A$ temos $b - m = \min(B)$. Se $a \in A$ então $a - m \in B$, logo $b - m \leqslant a - m$, portanto $b \leqslant a$, ou seja, $b = \min(A)$. □

Uma aplicação dessa versão do PBO é o seguinte resultado.

PROPOSIÇÃO 76 *Qualquer postagem que custe pelo menos oito reais pode ser feita com selos de 3 e 5 reais.*

Vamos chamar $n \in \mathbb{N}$ de *postal* se n pode ser um valor obtido a partir de selos de 3 e 5 reais. Por exemplo 8 é postal pois $8 = 3 + 5$, também 9 é postal pois $9 = 3 \cdot 3 + 0 \cdot 5$ e 10 é postal pois $10 = 0 \cdot 3 + 2 \cdot 5$.

DEMONSTRAÇÃO. O teorema afirma que para todo elemento de $\{n \in \mathbb{N}\colon\ n \geqslant 8\}$ é postal. A prova é por contradição.

Suponha que a afirmação do teorema é falsa. Seja $A \subseteq \mathbb{N}$ o subconjunto dos naturais maiores ou iguais a 8 não-postais. Por hipótese $A \neq \varnothing$, portanto tem um menor elemento m. Pelas considerações acima sabemos que $m \geqslant 11$.

Se $m \geqslant 11$ então $m-3 \geqslant 8$ e é postal, logo existem naturais x e y tais que $m-3 = x\cdot 3 + y\cdot 5$. De $m-3 = x\cdot 3 + y\cdot 5$ temos $m = (x+1)\cdot 3 + y\cdot 5$, e como m não é postal obtemos uma contradição. □

Se permitimos troco, todo valor pode ser obtido com selos de 3 e 5. Por exemplo, se entregamos 3 selos de 3 e recebemos de volta 1 selo de 5, ficamos com $3\cdot 3 + 5\cdot(-1) = 4$ pagos pela postagem.

Exercício 77. Prove que qualquer inteiro z pode se obtido como múltiplo (inteiro) de 3 mais múltiplo (inteiro) de 5.

Exercício 78 (**teorema de Bézout**). Escreva um enunciado preciso e use o PBO para provar a seguinte sentença. Sejam $a, b \in \mathbb{N}$ números coprimos. Existem inteiros x e y tais que $ax + by = 1$ (*dica:* tome o mínimo do conjunto dos números positivos da forma $ax + by$; prove por contradição que esse mínimo é 1).

1.3.9 Considerações sobre a escrita de uma demonstração

Em um sentido técnico e abstrato, uma demonstração matemática é a verificação de uma proposição por uma cadeia de deduções lógicas a partir de um conjunto básico de axiomas, porém o objetivo de uma demostração é fornecer aos leitores provas convincentes para a veracidade de uma afirmação. Para cumprir o objetivo de fornecer aos leitores provas convincentes para a veracidade de uma afirmação uma boa demonstração deve ser clara. Uma prova bem escrita é mais provável de ser uma prova correta, já que os erros são difíceis de esconder. Aqui estão algumas dicas sobre como escrever boas provas:

Indique sua estratégia, uma boa prova começa por explicar a linha geral de raciocínio, por exemplo. "Nós usamos indução em n" ou "Nós provamos por contradição". Isso cria uma imagem mental na qual o leitor pode ajustar os detalhes subsequentes.

Explique seu raciocínio. Muitos estudantes inicialmente escrevem provas da forma como eles computam integrais. O resultado é uma longa sequência de expressões sem explicação. Uma boa prova geralmente parece um ensaio com algumas equações lançadas. Use frases completas. Evite o simbolismo excessivo.

Simplifique, provas longas e complicadas levam o leitor mais tempo e esforço para entender e pode ocultar mais facilmente os erros. Então, uma demonstração com menos passos lógicos é melhor.

Introduza a notação cuidadosamente, às vezes, um argumento pode ser bastante simplificado introduzindo uma variável, elaborando uma notação especial ou definindo um novo termo. Mas faça isso com moderação, já que você exige que o leitor se lembre de todas essas coisas novas. E lembre-se de realmente definir os significados de novas variáveis, termos ou notações; não basta começar a usá-los.

Estruture provas longas. Um programa longo geralmente é dividido em um hierarquia de pequenos procedimentos. As provas longas são iguais. Fatos necessários na sua prova que são fáceis mas não prontamente provados são lemas. Além disso, se você repete essencialmente o mesmo argumento repetidamente, tente capturar esse argumento em um lema.

Conclua. Em algum momento de uma demonstração, você terá estabelecido todos os fatos essenciais que você precisa. Resista à tentação de encerrar e deixar o leitor tirar conclusões corretas. Em vez disso, amarre tudo e explicite a sentença original.

Não seja "telegráfico" como no seguinte exemplo.

Teorema. *Há infinitos números primos.*

DEMONSTRAÇÃO. Se houvessem finitos números primos

$$0 < \prod_{p \text{ primo}} \sin\left(\frac{\pi}{p}\right) = \prod_{p} \sin\left(\pi \frac{1 + 2\prod_{p'} p'}{p}\right) = 0$$

uma contradição. □

Antes de redigir a sua demonstração, revise sua estratégia e seu rascunho. Pense cuidadosamente em cada passo da prova, se você não sabe explicar claramente um passo, precisa voltar e pensar um pouco mais. Em tese, cada etapa de uma prova deve ser justificada por uma definição ou teorema. Na prática, a profundidade com que se deve fazer isso é uma questão de experiência. Uma justificação pode ser apresentada sem provas apenas se você estiver absolutamente confiante de que está correta o leitor concordará automaticamente que está correto.

Exercícios

1. Escreva as definições de número primo e de número composto. Enuncie, em seguida simbolize na linguagem da lógica (informal) o Teorema Fundamental da Aritmética.

2. Enuncie precisamente[11] cada proposição abaixo, incluindo quantificadores, domínio das variáveis e dê uma prova direta para:

   (a) se a divide b e a divide c então a divide $xb+yc$, quaisquer que sejam x e y inteiros.

   (b) se a divide b e b divide c então a divide c.

   (c) se $a>0$ é composto então a tem um fator primo p com $1<p\leqslant\sqrt{a}$.

   (d) se $\text{mdc}(a,b)=1$ então $\text{mdc}(a^2,b^2)=1$

3. Enuncie precisamente cada proposição abaixo, incluindo quantificadores, domínio das variáveis e dê uma prova pela contra-positiva:

   (a) se n não tem divisor primo d com $1<d\leqslant\sqrt{n}$ então n é primo.

   (b) se $x\in B\setminus A$ então $x\notin A\cap B$.

   (c) se $3n+2$ é ímpar então n é ímpar.

   (d) se c^5+7 é par, então c é ímpar.

4. Enuncie precisamente cada proposição abaixo, incluindo quantificadores, domínio das variáveis e dê uma prova por contradição:

   (a) se a não divide bc, então a não divide b.

   (b) se $3n+2$ é ímpar então n é ímpar.

   (c) $\sqrt[3]{3}$ não é racional.

   (d) se $d>1$ e $d\,|\,n$ então d não divide $n+1$.

   (e) Prove que existem infinitos números primos. (Dica: exercício anterior)

5. Justifique os passos do seguinte leitura da demonstração de (1.11).

   1) Suponha que 3 divide n
   2) Se 3 divide n, então existe $q\in\mathbb{N}$ tal que $n=3q$
   3) $n=3q$
   4) Se $n=3q$, então $n^2=9q^2$
   5) Se $n^2=9q^2$ então existe $k\in\mathbb{Z}$ tal que $n^2=9k$
   6) Se existe $k\in\mathbb{Z}$ tal que $n^2=9k$ então 9 divide n^2
   7) Se $n=3q$ então 9 divide n^2
   8) 9 divide n^2

6. Prove que $n^2+1>2^n$ sempre que $n\in\{1,2,3,4\}$.

7. Para números reais x e y usamos $\max\{x,y\}$ para denotar o maior deles e usamos $\min\{x,y\}$ para denotar o menor deles. Prove que $\max\{x,y\}+\min\{x,y\}=x+y$.

8. **Desigualdade triangular.** Prove que para todo $x\in\mathbb{R}$, para todo $y\in\mathbb{R}$, vale $|x+y|\leqslant|x|+|y|$.

9. Prove que para todo real x, se $x>0$ então existe y real tal que $y(y+1)=x$.

10. Sejam A,B,C conjuntos. Prove que se $A\subseteq B$ e $A\cap C=\varnothing$ então $A\subseteq B\setminus C$.

[11] isso não significa usar símbolos, significa dizer *tudo* o que precisa ser dito e *só* o que precisa ser dito

11. **Quantificador de unicidade:** $\exists!$. A proposição $(\exists!x)P(x)$ indica que existe um único x no domínio do discurso tal que $P(x)$ é verdadeiro. Por exemplo, $(\forall n \in \mathbb{N})(\exists! m \in \mathbb{N})nm = n$ é verdadeiro pois somente o número 1 tem a propriedade de que qualquer outro natural x vezes ele resulta em x.

$$(\exists!x)P(x) \text{ se, e somente se, } (\exists x)\big(P(x) \wedge (\forall y)(P(y) \to x = y)\big). \tag{1.16}$$

Prove que para todo irracional r, existe um único inteiro n tal que $|r-n| < \frac{1}{2}$ (*dica*: use (1.16) mostre que existe n e depois mostre que para qualquer m com a mesma propriedade $m = n$. Nesse último passo pode ser preciso usar a desigualdade triangular).

12. Prove que não há uma quantidade finita de números primos.

13. Prove que não há um "menor racional positivo".

14. Prove que para qualquer natural $n > 1$, existe uma sequência formada por n números naturais consecutivos tal que nenhum deles é primo (*dica:*$(n+1)! + j$ é divisível por j.).

15. Prove que no domínio dos números reais a seguinte sentença é verdadeira:

$$\forall \varepsilon > 0,\ \exists \delta > 0, \forall x \in \mathbb{R},\ \left(|x-3| < \delta \to \left|\frac{2x^2-5x-3}{x-3}\right| < \varepsilon\right).$$

16. $A \subseteq \mathbb{N}$ é dito **limitado superiormente** se existir um natural n tal que

$$\forall x \in A,\ x \leq n \tag{1.17}$$

Um natural n com a propriedade (1.17) e que pertence a A é dito **maior elemento** de A. Demonstre que se $A \neq \varnothing$ é limitado superiormente, então admite maior elemento. Denotamos o maior elemento de A por $\max(A)$.

17. A seguinte estratégia prova que $\sqrt{3} \notin \mathbb{Q}$?

Assuma $\sqrt{3}$ racional. Então $\sqrt{3}$ pode ser representado como $\frac{a}{b}$ onde a e b são coprimos e positivos. Então, $3b^2 = a^2$. Agora, $3 \mid 3b^2$, portanto $3 \mid a^2$, mas então $3 \mid a$. Assim, temos $3b^2 = (3k)^2$, logo $3b^2 = 9k^2$ ou seja $b^2 = 3k^2$ e temos uma contradição.

18. Nesse exercício assuma que todas as variáveis têm mesmo domínio e vamos omiti-lo. Leia atentamente o teorema 79 e a sua demonstração dados abaixo.

TEOREMA 79 *Se existe x tal que $P(x)$ e existe x tal que $Q(x)$ então existe x tal que $P(x)$ e $Q(x)$.*

Em símbolos: $(\exists x, P(x)) \wedge (\exists x, Q(x)) \to \exists x\,(P(x) \wedge Q(x))$.

DEMONSTRAÇÃO. Considere o seguinte argumento

1)	$(\exists x,\ P(x))$ e $(\exists x,\ Q(x))$	(premissa)
2)	$\exists x,\ P(x)$	(simplificação de 1)
3)	$P(c)$	(instanciação existencial de 2)
4)	$\exists x,\ Q(x)$	(simplificação de 1)
6)	$Q(c)$	(instanciação existencial de 4)
7)	$P(c)$ e $Q(c)$	(conjunção de 3 e 5)
8)	$\exists x, (P(x)$ e $Q(x))$	(generalização existencial de 7)

□

(a) Dê um contraexemplo para a afirmação feita no teorema, isto é, encontre um domínio D e predicados P e Q sobre elementos de D para o qual a sentença não vale.

(b) Indique o(s) erro(s) na demonstração.

19. Leia com atenção o seguinte teorema e uma suposta demonstração.

TEOREMA 80 *Para todos a, b, c, d números naturais, se c divide a e c divide b e d divide a e d divide b e c não divide d, então dc divide a e dc divide b.*

Em símbolos[a]: $\forall a,b,c,d \in \mathbb{N}, \left(c \mid a \text{ e } c \mid b \text{ e } d \mid a \text{ e } d \mid b \text{ e } c \nmid d \rightarrow dc \mid a \text{ e } dc \mid b\right)$.

DEMONSTRAÇÃO. Sejam a, b, c, d números naturais tais que c divide a, c divide b, d divide a, d divide b e c não divide d.
Se d divide a e b, então existem x e y naturais tais que $a = xd$ e $b = yd$.
Se c divide a então c divide xd.
Se c divide xd e não divide d, então c divide x.
Analogamente, se c divide b então c divide yd.
Se c divide yd e não divide d, então c divide y.
Se c divide x e y, então existem z e w tais que $x = cz$ e $y = cw$.
Das conclusões acima temos $a = xd = (cz)d = (dc)z$ e $b = yd = (cw)d = (dc)w$, portanto, dc divide a e dc divide b. □

[a] isso ajudou a fixar as informações?

(a) Dê um contraexemplo para a afirmação feita no teorema.

(b) Indique o(s) erro(s) na demonstração.

20. Dizem que nos seus primeiros anos de Hogwarts, Harry Potter resolveu usar seus poderes para escrever uma prova análoga de que $\sqrt{4}$ não é racional, coisa que quase todo mundo sabe que não é. A prova de Harry Potter foi:

TEOREMA 81 *$\sqrt{4}$ não é racional.*

DEMONSTRAÇÃO. Se $\sqrt{4}$ é racional então existem $a, b \in \mathbb{N}^*$, primos entre si, tais que

$$\frac{a}{b} = \sqrt{4}.$$

Elevando os dois termos da equação ao quadrado, temos

$$a^2 = 4b^2$$

Logo a^2 é divisível por 4 e, portanto, a também o é. Por definição,podemos escrever $a = 4k$, para algum $k \in \mathbb{N}$, e ficamos com

$$(4k)^2 = 4b^2$$

e, portanto

$$16k^2 = 4b^2,$$

ou seja

$$b^2 = 4k^2.$$

Logo b^2 é divisível por 4 e, portanto, b também o é, o que contraria a escolha de a e b primos entre si.
Portanto, $\sqrt{4}$ não é racional. □

Onde está a mágica?

21. Seja n um natural. Prove que se n não é um quadrado então $\sqrt{n}$ é irracional (*dica*: exerc. 2, item 4, ou o corolário 68).

22. Prove que existe um racional x e um irracional y tais que x^y é irracional.

23. O que está errado na seguinte demonstração.

TEOREMA 82 *Para todo natural n, $n^2 + n + 1$ é par.*

DEMONSTRAÇÃO. A prova é por contradição, assuma que existem naturais tais que $n^2 + n + 1$ é ímpar e seja A o subconjunto formado por tais números. Pelo PBO, podemos tomar $m = \min A$.
Como $m - 1 \notin S$ temos que $(m-1)^2 + (m-1) + 1$ é par. Porém $(m-1)^2 + (m-1) + 1 = m^2 - m + 1 = (m^2 + m + 1) - 2m$, ou equivalentemente, $m^2 + m + 1 = ((m-1)^2 + (m-1) + 1) - 2m$, que é par e temos uma contradição. □

24. Prove que todo subconjunto não vazio de $\mathbb{N}\times\mathbb{N}$ tem um menor elemento com respeito a relação $\preccurlyeq$ definida no exercício 10, página 26,

O método probabilístico

O método probabilístico é um método não construtivo usado para provar a existência de um objeto matemático com uma propriedade prescrita. Nas várias estratégias probabilísticas a ideia geral pode ser resumida como: mostrar que escolhendo aleatoriamente objetos de uma classe especificada, a probabilidade de que o resultado seja do tipo prescrito é estritamente maior do que zero, o que indica a existência de tal objeto. Uma explicação intuitiva para essa abordagem é pensar que a probabilidade de que a propriedade prescrita ocorra como a razão do número de objetos com a propriedade pelo número total de objetos. Se esta proporção for positiva, é garantido que deve haver pelo menos uma construção que exiba a propriedade.

Embora esse método de prova use probabilidade, a conclusão final não é probabilística. Este método também é aplicado em outras áreas como a teoria dos números, álgebra, análise real, ciência da computação e teoria da informação.

Seja $\mathscr{H}$ um conjunto cujos elementos são os conjuntos $A_1,\dots,A_m$ todos eles com k elementos e fixamos $V \coloneqq \bigcup \mathscr{H}$.

Teorema 83 *Se $m < 2^{k-1}$ então é possível pintar os elementos de V com duas cores sem que tenha um A_i com todos os seus elementos da mesma cor.*

Demonstração. Para cada elemento de V lançamos uma moeda, se resultar cara pintamos tal elemento de *azul* e se resultar coroa pintamos tal elemento de *vermelho*. Fixado i, a probabilidade com que A_i tem todos os seus elementos azuis é $(1/2)^k$. A probabilidade com que A_i tem todos os seus elementos da mesma cor é $2\cdot(1/2)^k = 2^{1-k}$.

A probabilidade de existir $i\in\{1,\dots,m\}$ tal que os seus elementos são da mesma cor é $m\cdot 2^{1-k}$.

Pela hipótese em m temos que $m\cdot 2^{1-k} < 2^{k-1}\cdot 2^{1-k} = 1$, portanto, a probabilidade de existir $i\in\{1,\dots,m\}$ tal que os seus elementos são da mesma cor é < 1. Logo a probabilidade com que ocorram as duas cores em cada A_i, para todo $i\in\{1,\dots,m\}$, é maior que 0, ou seja, deve existir um modo de colorir V com duas cores sem que tenha um A_i com todos os seus elementos da mesma cor. □

Dizemos que $H\subset V$ é um *conjunto de acerto* se H encontra todo elemento de $\mathscr{H}$, isto é, $H\cap A_i\neq\varnothing$ para todo i. O próprio V é um conjunto de acerto. Também é qualquer H com $|V|-k+1$ elementos pois para todo i temos que o número de elementos em A_i somado ao número de elementos de H é $|V|+1>|V|$ portanto eles devem ter elemento em comum. Ainda, podemos escolher um elemento de cada A_i para formar um conjunto de acerto com $\leqslant m$ elementos. Claramente, o desafio é encontrar um H tão pequeno quanto possível.

Teorema 84 *Existe um conjunto de acerto para $\mathscr{H}$ com no máximo $\left\lceil \frac{|V|\log m}{k}\right\rceil$ elementos.*

Demonstração. Sorteamos uniformemente $h \coloneqq \left\lceil \frac{|V|\log m}{k}\right\rceil$ elementos de V com repetição; para cada um deles, a probabilidade de não estar em A_j é $1-(k/|V|)$. A probabilidade de nenhum dos sorteados estarem em A_j é $(1-(k/|V|))^h$.

Usando que $(1-1/x)^x < \mathrm{e}^{-1}$ temos

$$\left(1-\frac{k}{|V|}\right)^h < \mathrm{e}^{\frac{hk}{|V|}} \leqslant \mathrm{e}^{-\log(m)} = \frac{1}{m}.$$

A probabilidade de haver algum $j\in\{1,2,\dots,m\}$ tal que nenhum dos sorteados estarem em A_j é menor que

$$\sum_{j=1}^{m}\frac{1}{m} = 1,$$

portanto, com probabilidade positiva essa seleção define um conjunto com $\leqslant h$ elementos (por causa da repetição) que encontra todos os elementos de $\mathscr{H}$. □

Esses dois teoremas são clássicos em combinatória. De fato, a combinatória é um terreno fértil para o método probabilístico, em parte porque probabilidade está intrinsecamente ligada a contagem, que é uma ferramenta central em combinatória.

Vamos usar o método probabilístico para provar, por contradição, que existem infinitos números primos.

Teorema 85 *Há infinitos números primos.*

Demonstração. Vamos assumir que M é o maior número primo. Seja R um número aleatório sorteado de acordo com a seguinte regra: $R = 2^{T_2}\cdot 3^{T_3}\cdot 5^{T_5}\cdots M^{T_M}$ onde T_p é um a menos da quantidade de lançamentos de um dado com p faces (as faces são $1,\dots,p$) até obtermos um resultado diferente de 1

$$\mathrm{Prob}\big(T_p = n\big) = \frac{1}{p^n} - \frac{1}{p^{n+1}} = \frac{1}{p^n}\left(1-\frac{1}{p}\right).$$

Por exemplo, para T_2 se os lançamentos resultam $1,1,1,1,1,2$ então $T_2 = 5$, se o primeiro lançamento é 2 então $T_2 = 0$. Os sorteios são independentes de modo que, por exemplo,

$$\begin{aligned}\text{Prob}(R = 10) &= \text{Prob}(T_2 = 1)\text{Prob}(T_3 = 0)\text{Prob}(T_5 = 1)\text{Prob}(T_7 = 0)\cdots\text{Prob}(T_M = 0)\\ &= \frac{1}{2}\frac{1}{5}\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\cdots\left(1-\frac{1}{M}\right)\end{aligned}$$

e, de modo geral,

$$\text{Prob}(R = k) = \frac{1}{k}\prod_p\left(1-\frac{1}{p}\right)$$

onde o produto é sobre todo primo p. Mas disso temos que

$$\sum_{k\geqslant 1}\text{Prob}(R = k) = \sum_{k\geqslant 1}\frac{1}{k}\prod_p\left(1-\frac{1}{p}\right)\prod_p\left(1-\frac{1}{p}\right)\sum_{k\geqslant 1}\frac{1}{k}$$

o lado esquerdo é 1, por ser uma distribuição de probabilidade, e o lado direito é ∞ pois $\sum_{k\geqslant 1} 1/k$ diverge, uma contradição que encerra a prova. □