Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Departamento de Matemática

Números, Relações e Criptografia

Antônio de Andrade e Silva

A minha esposa
Rosângela.

Prefácio

A idéia de escrever este livro surgiu da inexistência de um texto na literatura matemática nacional que atendesse às demandas do programa da disciplina Matemática Elementar, integrante dos cursos de graduação em Matemática da Universidade Federal da Paraíba - Campus I. É oportuno salientar que os textos disponíveis ou estão muito acima ou muito aquém do patamar em que se situa o conteúdo da referida disciplina. Por estas e por outras razões, decidimo-nos pela adoção de uma obordagem objetiva sem, contudo, descurar do rigor compatível com o que há de indispensável para a formação de licenciados e bacharéis portadores de indiscutível qualificação.

É nossa expectativa que este texto assuma o caráter de espinha dorsal de uma expreiência permanentemente renovável, sendo, portanto, bem vindas as críticas e/ou sugestões apresentadas por todos - professores ou alunos quantos dele fizerem uso.

Para desenvolver a capacidade do estudante de pensar por si mesmo em termos das novas definições, incluímos no final de cada seção uma extensa lista de exercícios.

No capítulo 1 apresentaremos algumas definições e resultados sobre sentenças, conjuntos e famílias indexadas que serão necessárias para o entendimento dos próximos capítulos.

No capítulo 2 apresentaremos as noções de relação, relação de equivalência e funções.

No capítulo 3 apresentaremos as noções de conjuntos ordenados, o Axioma da Boa Ordenação, o Princípio de Indução e resultados sobre conjuntos finitos, infinitos, contáveis e não-contáveis.

No capítulo 4 apresentaremos algumas definições e resultados básicos da Teoria dos Números Elementar.

O capítulo 5 é dedicado ao estudo da Aritmética Modular.

Finalmente, no capítulo 6 aplicaremos os conhecimentos sobre números primos e congruências para apresentar uma introdução aos sistemas de criptografia clássicos e com chave pública.

Agradecemos aos colegas e alunos do Departamento de Matemática que direta ou indiretamento comtribuiram para a realização deste trabalho.

Finalmente, nosso agradecimento aos diversos autores cujos livros influenciaram este trabalho. Em particular, L. H. Jacy Monteiro, *Elementos de Álgebra*, Elementos de Matemática, IMPA, 1969 e E. L. Lima, *Curso de Análise*, Vol. I, Projeto Euclides, IMPA, 1976.

Sumário

Parte I

Conjuntos e Relações

Capítulo 1

Conjuntos

Neste capítulo apresentaremos algumas definições e resultados clássicos de lógica simbólica e da teoria dos conjuntos que serão necessários para cursos subsequentes. O leitor interessado em mais detalhes pode consultar [6, 15, 17].

1.1 Sentenças

Nesta seção discutiremos alguns conceitos elementares de lógica simbólica de um ponto de vista intuitivo que serão necessários para uma melhor compreensão das provas dos Teoremas. O leitor interessado em mais detalhes pode consultar [15, 17].

Uma *sentença* (ou *proposição*) significa uma oração declarativa a qual, num dado contexto é, sem equívoco, ou *verdadeira* ou *falsa* e não ambos.

Por exemplo, "Brasília é a capital do Brasil" é uma sentença verdadeira, "dinheiro cresce em árvore" é uma sentença falsa e "onde é que você vai?" não é uma sentença por não ser nem verdadeira nem falsa. A validade ou falsidade de uma sentença é chamada de *valor verdade*.

Usaremos as letras p, q, r, s, etc. para denotar sentenças. Sentenças podem ser combinadas de várias maneiras para formar sentenças mais gerais. Freqüentemente, o valor verdade da sentença composta é completamente determinado pelo valor verdade das sentenças componentes. Assim, se p é uma sentença, então uma das sentenças mais simples que podemos formar, a partir de p, é a *negação* de p, em símbolos $\neg p$ ou $\sim p$, (lê-se não p). O valor verdade da negação de uma sentença satisfaz: se p é verdadeira, então $\neg p$ é falsa; se p é falsa, então $\neg p$ é verdadeira. É conveniente exibir a relação entre $\neg p$ e p numa tabela, a qual é chamada *tabela verdade*, onde V e F denotam os valores verdade, verdadeiro e falso, respectivamente.

p	$\neg p$
V	F
F	V

Se p e q são sentenças, a *conjunção* de p e q, em símbolos $p \wedge q$, (lê-se p e q) é uma

sentença cujo valor verdade é verdadeiro se p e q forem ambas verdadeiras e falso caso contrário (confira tabela).

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Se p e q são sentenças, a *disjunção* de p e q, em símbolos $p \vee q$, (lê-se p ou q com sentido de e/ou) é uma sentença cujo valor verdade é falso se p e q forem ambas falsas e verdadeiro caso contrário (confira tabela).

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Uma operação importante em sentenças, principalmente em matemática, é a *implicação*: se p e q são sentenças, então $p \rightarrow q$, (lê-se p implica em q). Note que: em uso comum, se p é verdadeiro, então q é verdadeiro significa que existe uma relação de *causa* entre p e q, como em "se José Augusto passa no curso, então José Augusto pode colar grau." Em matemática, portanto, implicação é no sentido *formal*: $p \rightarrow q$ é verdadeiro exceto se p é verdadeiro e q é falso, isto é, quando na tabela verdade de p e q não temos simultaneamente p verdadeira e q falsa, confira tabela. Neste caso, dizemos que "p é condição suficiente para q" e "q é condição necessária para p."

p	q	$p \rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

Teorema 1.1 *Sejam p e q duas sentenças. Então as seguintes afirmações são verdadeiras*:

1. $p \rightarrow p \vee q$.

2. $q \rightarrow p \vee q$.

3. $p \wedge q \rightarrow p$.

4. $p \wedge q \rightarrow q$.

Prova. Provaremos apenas o item (1). Basta provar que se p e q são duas sentenças quaisquer, então a sentença $p \to p \vee q$ é sempre verdadeira. Para isto derivamos a tabela para a sentença $p \to p \vee q$ como segue.

p	q	$p \vee q$	$p \to p \vee q$
V	V	V	V
V	F	V	V
F	V	V	V
F	F	F	V

■

Teorema 1.2 *Sejam p, q e r três sentenças. Então a seguinte sentença é verdadeira*

$$[(p \to q) \wedge (q \to r)] \to (p \to r).$$

Prova.Vamos denotar por s a sentença

$$[(p \to q) \wedge (q \to r)] \to (p \to r)$$

e derivar a tabela para a sentença s.

p	q	r	$p \to q$	$q \to r$	$(p \to q) \wedge (q \to r)$	$p \to r$	s
V	V	V	V	V	V	V	V
V	V	F	V	F	F	F	V
V	F	V	F	V	F	V	V
V	F	F	F	V	F	F	V
F	V	V	V	V	V	V	V
F	V	F	V	F	F	V	V
F	F	V	V	V	V	V	V
F	F	F	V	V	V	V	V

Como a última coluna da tabela verdade é constituída de valores "verdadeiros" temos que s é uma sentença verdadeira. ■

Teorema 1.3 *Sejam p, q e r três sentenças. Se $q \to r$ é uma sentença verdadeira, então as seguintes afirmações são verdadeiras*:

1. $(p \vee q) \to (p \vee r)$;

2. $(p \wedge q) \to (p \wedge r)$.

Prova. Provaremos apenas o item (1). Vamos derivar a tabela para a sentença $(p \vee q) \rightarrow (p \vee r)$.

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

Como, por hipótese, a sentença $q \rightarrow r$ é verdadeira, não podemos ter simultaneamente q verdadeira e r falsa. Assim, podemos descartar a sexta linha da tabela verdade. Portanto, a sentença $(p \vee q) \rightarrow (p \vee r)$ é verdadeira. ■

A sentença

$$(p \rightarrow q) \wedge (q \rightarrow p)$$

significa p se, e somente se, q; em símbolos $p \leftrightarrow q$. O valor verdade da sentença $p \leftrightarrow q$ satisfaz: $p \leftrightarrow q$ é verdadeira se p e q têm o mesmo valor verdade; caso contrário, é falsa, confira tabela. Neste caso, dizemos que "p é condição necessária e suficiente para q" e "q é condição necessária e suficiente para p."

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Duas sentenças são chamadas *logicamente equivalentes* (ou simplesmente *equivalentes*) se suas tabelas verdade são idênticas, isto é, duas sentenças p e q são equivalentes se p é verdadeira quando q é verdadeira e p é falsa quando q é falsa.

Exemplo 1.4 *Sejam p e q duas sentenças. Mostrar que as sentenças $p \rightarrow q$ e $\neg p \vee q$ são equivalentes, isto é, $(p \rightarrow q) \leftrightarrow (\neg p \vee q)$ (ou $(p \rightarrow q) = (\neg p \vee q)$).*

Solução. Basta derivar a tabela para a sentença $(p \rightarrow q) = (\neg p \vee q)$.

p	q	$\neg p$	$\neg p \vee q$	$(p \rightarrow q$
V	V	F	V	V
V	F	F	F	F
F	V	V	V	V
F	F	V	V	V

.

Dadas duas sentenças p e q, existem quatro sentenças, as quais resultam do uso de $\rightarrow$ para conectar p e q. Elas são:

$p \rightarrow q$	condicional
$q \rightarrow p$	recíproca
$\neg q \rightarrow \neg p$	contrapositiva
$\neg p \rightarrow \neg q$	inversa

Note que, a condicional e a contrapositiva são sentenças logicamente equivalentes. De fato, basta derivar a tabela para a sentença $(p \rightarrow q) = (\neg q \rightarrow \neg p)$.

p	q	$\neg q$	$\neg p$	$p \rightarrow q$	$\neg q \rightarrow \neg p$
V	V	F	F	V	V
V	F	V	F	F	F
F	V	F	V	V	V
F	F	V	V	V	V

.

Também, a recíproca e a inversa são sentenças logicamente equivalentes (prove isto!).

Frases que exprimem a idéia de quantidade são chamadas de *quantificadores*. Por exemplo, "para todo número x," "existe um número x" e "para nenhum número x." O quantificador *para todo*, em símbolos $\forall$, é chamado de *quantificador universal* e o quantificador *existe*, em símbolos $\exists$, é chamado de *quantificador existencial*. Uma expressão alternativa para o quantificador universal é *para qualquer* e para o quantificador existencial é *para algum*.

É importante considerar a negação de afirmações envolvendo quantificadores. A negação do quantificador universal é o quantificador existencial e vice-versa. Por exemplo, a negação de "para todo número x" é "existe um número x."

Freqüentemente, um Axioma em Álgebra Moderna é afirmado como segue: "Existe um único elemento x satisfazendo a propriedade P." Para negar isto, devemos usar uma das leis De Morgan, confira Exercício 3 abaixo. "Não existe um elemento x satisfazendo a propriedade P ou existe mais de um elemento x satisfazendo a propriedade P."

Muitos dos Teoremas em Álgebra Moderna são expressos como afirmação condicional. Por exemplo, se x^2 é um número par, então x é um número par. Como provar essa afirmação? Primeiro observe que, se p é a sentença "x^2 é um número par" e q é a sentença "x é um número par," então a afirmação que devemos provar é $p \rightarrow q$. Logo, para prova $p \rightarrow q$, é suficiente provar qualquer uma das sentenças logicamente equivalentes do Exercício 4 abaixo. Neste caso, dizemos que é uma *prova indireta* ou *prova por absurdo*. Assim, a prova indireta de nossa afirmação é como segue:

Suponhamos que x^2 seja um número par e x seja um número ímpar $(p \wedge \neg q)$. Então $x = 2n + 1$, para algum $n \in \mathbb{N}$. Logo,

$$x^2 = 2(2n^2 + 2n) + 1$$

e, assim, x^2 é número ímpar ($\neg p$), o que é uma contradição. Assim, se x^2 é um número par, então x deve ser um número par.

Nesse argumento, provamos que a seguinte sentença $(p \wedge \neg q) \rightarrow \neg p$ é verdadeira. Portanto, $p \rightarrow q$ é uma sentença verdadeira.

Agora, vamos provar que: se x é um número par, então x^2 é um número par. Primeiro observe que, se p é a sentença "x é um número par" e q é a sentença "x^2 é um número par," então a afirmação que devemos provar é $p \rightarrow q$. Para provar que $p \rightarrow q$, daremos uma *prova direta*, isto é, partindo de p até chegar a q. Assim, a prova direta de nossa afirmação é como segue:

Suponhamos que x seja um número par. Então $x = 2n$, para algum $n \in \mathbb{N}$. Logo,

$$x^2 = 2(2n^2)$$

e, assim, x^2 é número par. Assim, se x é um número par, então x^2 deve ser um número par.

EXERCÍCIOS

1. Sejam p, q e r três sentenças. Mostrar que as seguintes afirmações são verdadeiras:

   (a) $p \vee p \leftrightarrow p$.

   (b) $p \wedge p \leftrightarrow p$.

   (c) $(p \vee q) \leftrightarrow (q \vee p)$.

   (d) $(p \wedge q) \leftrightarrow (q \wedge p)$.

   (e) $p \vee (q \vee r) \leftrightarrow (p \vee q) \vee r$.

   (f) $p \wedge (q \wedge r) \leftrightarrow (p \wedge q) \wedge r$.

   (g) $p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$.

   (h) $p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$.

2. Sejam p e q duas sentenças. Mostrar que as seguintes afirmações são verdadeiras:

   (a) $\neg(\neg p) \leftrightarrow p$.

   (b) $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$.

   (c) $(p \rightarrow q) \leftrightarrow (\neg p \vee q)$.

   (d) $(p \rightarrow q) \leftrightarrow \neg(p \wedge \neg q)$.

   (e) $[p \wedge (p \rightarrow q)] \rightarrow q$;

   (f) $[(p \vee q) \wedge \neg p)] \rightarrow q$.

3. Sejam p e q duas sentenças. Mostrar que as seguintes afirmações são verdadeiras (Leis De Morgan):

(a) $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$.

(b) $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$.

4. Sejam p e q duas sentenças. Mostrar que as seguintes afirmações são logicamente equivalentes:

(a) $p \rightarrow q$.

(b) $\neg q \rightarrow \neg p$.

(c) $(p \wedge \neg q) \rightarrow \neg p$.

(d) $(p \wedge \neg q) \rightarrow q$.

(e) $(p \wedge \neg q) \rightarrow f$ (onde f é uma sentença, a qual é sempre falsa).

5. Sejam p, q e r três sentenças. Mostrar que as seguintes afirmações são verdadeiras:

(a) $[(p \rightarrow q) \wedge (r \rightarrow q)] \leftrightarrow [(p \vee r) \rightarrow q]$.

(b) $[(p \rightarrow q) \wedge (p \rightarrow r)] \leftrightarrow [p \rightarrow (q \wedge r)]$.

6. Sejam p, q e r três sentenças. Se $q \leftrightarrow r$ é uma sentença verdadeira, então as seguintes afirmações são verdadeiras:

(a) $(p \vee q) \leftrightarrow (p \vee r)$.

(b) $(p \wedge q) \leftrightarrow (p \wedge r)$.

(c) $(p \rightarrow q) \leftrightarrow (p \rightarrow r)$.

7. Sejam p, q, r e s quatro sentenças. Se $p \rightarrow q$ e $r \rightarrow s$, então:

(a) $p \vee r \rightarrow q \vee s$.

(b) $p \wedge r \rightarrow q \wedge s$.

8. Sejam $m, n \in \mathbb{N}$. Mostrar que se $m + n \geq 20$, então $m \geq 10$ ou $n \geq 10$.

9. Seja $x \in \mathbb{R}_+$. Mostrar que se para todo $\epsilon > 0$, tem-se $0 \leq x < \epsilon$, então $x = 0$.

10. Seja $x \in \mathbb{R}$. Mostrar que se $x > 0$, então $\frac{1}{x} > 0$.

1.2 Conjuntos

A noção de conjunto é a própria estrutura para o pensamento da matemática abstrata. Assim, sem dúvida, para atacar a lista de noções indefinidas e os vários axiomas, relacionando-os, será tomada uma abordagem formal e/ou informal do assunto.

Um *conjunto* (ou *coleção*) é formado de objetos bem definidos. Os objetos que compõem um conjunto particular são chamados de *elementos* ou *membros*.

Conjuntos e elementos serão indicados, salvo menção explicita em contrário, por letras maiúsculas e minúsculas do nosso alfabeto, respectivamente. Em particular, empregaremos as seguintes notações:

- $\mathbb{N}$ denota o conjunto de todos os números naturais $1, 2, 3, \ldots$
- $\mathbb{Z}$ é o conjunto de todos os números inteiros $0, \pm 1, \pm 2, \pm 3, \ldots$
- $\mathbb{Q}$ é o conjunto de todos os números racionais - isto é, frações $\frac{m}{n}$, onde m, n são números inteiros e $n \neq 0$.
- $\mathbb{R}$ é o conjunto de todos os números reais.
- $\mathbb{C}$ é o conjunto de todos os números complexos $a + bi$, onde a, b são números reais e $i^2 = -1$.

Quando um objeto x é um dos elementos que compõem o conjunto A, dizemos que x *pertence* a A, escreveremos $x \in A$; caso contrário, escreveremos $x \notin A$. Por exemplos,

$$2 \in \mathbb{N}, -2 \notin \mathbb{N}, -1 \in \mathbb{Z}, \frac{1}{2} \notin \mathbb{Z}, \sqrt{2} \notin \mathbb{Q}, \sqrt{2} \in \mathbb{R}, \text{ etc.}$$

Sejam A e B conjuntos. Dizemos que A e B são *iguais*, em símbolos $A = B$, se eles consistem dos mesmos elementos, isto é,

$$x \in A \Leftrightarrow x \in B.$$

Caso contrário, $A \neq B$. Assim, um conjunto é completamente determinado se conhecemos seus elementos.

Um conjunto com um número finito de elementos pode ser exibido escrevendo todos os seus elementos entre chaves e inserindo vírgulas entre eles. Assim,

$$\{1, 2, 3\}$$

denota o conjunto cujos elementos são $1, 2$ e 3. A ordem em que os elementos são escritos não altera o conjunto. Assim,

$$\{1, 2, 3\} \text{ e } \{2, 3, 1\}$$

denota o mesmo conjunto. Também, repetição de um elemento não tem efeito. Por exemplo,

$$\{1, 2, 3, 2\} = \{1, 2, 3\}.$$

Dado um conjunto A e uma propriedade $P(x)$, existe um único conjunto B cujos elementos são precisamente aqueles elementos x de A tais que $P(x)$ é verdadeira, em símbolos

$$B = \{x \in A : P(x)\},$$

onde ":" lê-se *tal que*. Por exemplo,

$$\{0, 1\} = \{x \in \mathbb{R} : x^2 = x\}.$$

Um modo de representar os elementos de um conjunto é através de pontos interiores a uma linha fechada e não entrelaçada, quando a linha fechada é um círculo chamamos de *diagrama de Venn* (Matemático Inglês John Venn, 1834 - 1923). Por exemplo,

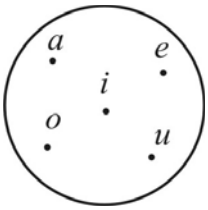

Figura 1.1: Diagrama de Venn.

Definição 1.5 *Sejam A e B conjuntos. Dizemos que A é um* subconjunto *de B se todo elemento de A é um elemento de B, isto é,*

$$x \in A \Rightarrow x \in B.$$

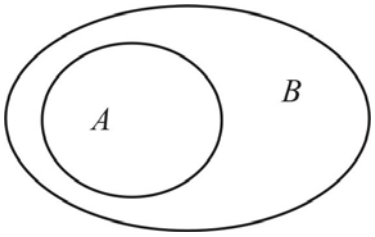

Figura 1.2: A subconjunto de B.

Se A é um subconjunto de B, denotaremos por $A \subseteq B$ (O símbolo $\subseteq$ significa "está contido ou igual"): Na definição, acima, não está excluída a possibilidade de A e B serem iguais. Se $A \subseteq B$ e $A \neq B$, dizemos que A é um *subconjunto próprio* de B e denotaremos por $A \subset B$. Se o conjunto A não está contido no conjunto B, denotaremos por $A \nsubseteq B$. Por exemplos,

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

O termo *conjunto-universo* (ou *universal*) é, às vezes, usado para um conjunto U que contém todos os conjuntos em um dado contexto. Por exemplo, na Geometria Plana, o

universo é o conjunto de todos os pontos do plano. Assim, admitiremos, no que segue, que todos os conjuntos considerados sejam subconjuntos de um conjunto-universo U. Note que se

$$A = \{x \in U : P(x)\} \text{ e } B = \{x \in U : Q(x)\},$$

então a afirmação $P(x) \Rightarrow Q(x)$, significa que $A \subseteq B$.

É possível citar uma propriedade que não possa ser gozada por qualquer elemento. Neste caso, o conjunto

$$\{x \in U : P(x)\}$$

não possui elemento algum. Esse conjunto é conhecido como o *conjunto vazio*, denotaremos por $\emptyset$.

Exemplo 1.6

$$\emptyset = \{x \in \mathbb{Z} : x \neq x\}.$$

Note que o conjunto vazio $\emptyset$ está contido em qualquer conjunto, de fato:

$$x \notin A \Rightarrow x \notin \emptyset,$$

pois $\emptyset$ não contém nenhum elemento.

Teorema 1.7 *Sejam A, B e C subconjuntos de U. Então*:

1. $A \subseteq A, \emptyset \subseteq A$.
2. $A = B \Leftrightarrow A \subseteq B$ *e* $B \subseteq A$.
3. $A \subseteq \emptyset \Leftrightarrow A = \emptyset$.
4. $x \in A \Leftrightarrow \{x\} \subseteq A$.
5. *Se* $A \subseteq B$ *e* $B \subseteq C$, *então* $A \subseteq C$.

Prova. Exercício. ■

Definição 1.8 *Sejam A e B subconjuntos de U. A* união *de A e B, em símbolos $A \cup B$, é o conjunto*

$$A \cup B = \{x \in U : x \in A \text{ ou } x \in B\}.$$

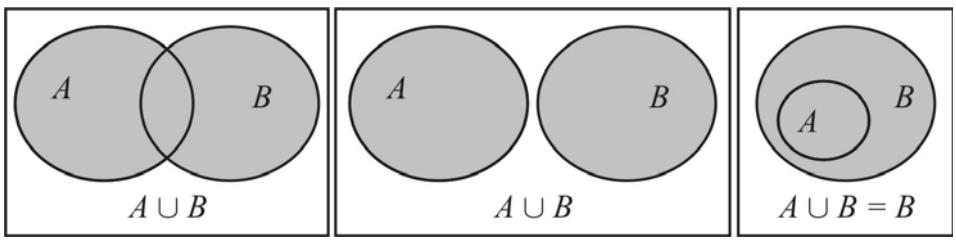

Figura 1.3: A união de A e B.

Definição 1.9 *Sejam A e B subconjuntos de U. A* interseção *de A e B, em símbolos $A \cap B$, é o conjunto*

$$A \cap B = \{x \in U : x \in A \ e \ x \in B\}.$$

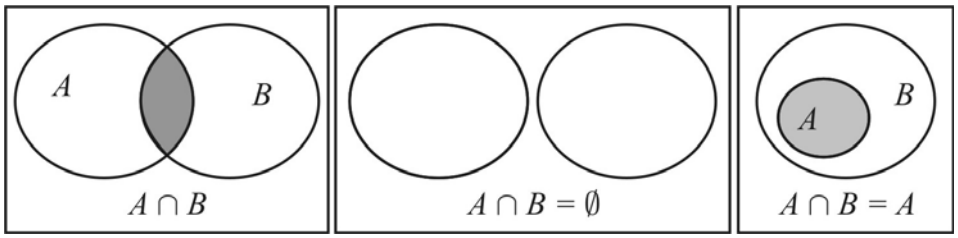

Figura 1.4: A interseção de A e B.

Definição 1.10 *Sejam A e B subconjuntos de U. A* diferença *de A e B, em símbolos $A - B$, é o conjunto*

$$A - B = \{x \in U : x \in A \ e \ x \notin B\}.$$

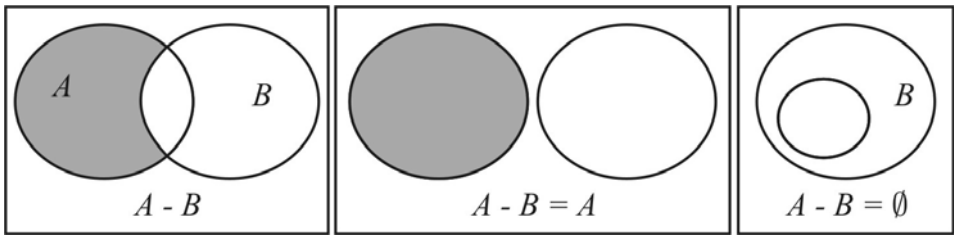

Figura 1.5: A diferença de A e B.

Teorema 1.11 *Sejam A e B subconjuntos de U. Então*:

1. $A \subseteq A \cup B$ *e* $B \subseteq A \cup B$.
2. $A \cap B \subseteq A$ *e* $A \cap B \subseteq B$.
3. $A - B \subseteq A$.
4. $A \cup B = (A \cap B) \cup (A - B) \cup (B - A)$.

Prova. Exercício. ■

Se $A \subseteq B$, então $B - A$ é chamado o *complementar* de A em B. Os conjuntos A e B são chamados *disjuntos* se $A \cap B = \emptyset$. O complementar de A em U é simplesmente

chamado de *complementar* de A, em símbolos A' ou A^c, sem referência explícita a U. Assim, $A - B = A \cap B'$.

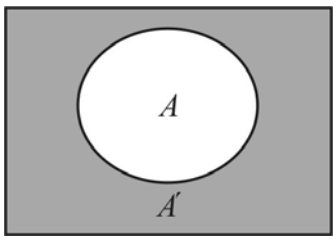

Figura 1.6: O complementar de A.

Exemplo 1.12 *Sejam* $U = \{0, 1, 2, 3, 4, 5, 6\}$, $A = \{1, 2, 4\}$, $B = \{2, 3, 5\}$. *Então*:

$$\begin{aligned} A \cup B &= \{1, 2, 3, 4, 5\} \\ A \cap B &= \{2\} \\ A - B &= \{1, 4\} \\ B - A &= \{3, 5\} \\ A' &= \{0, 3, 5, 6\} \\ B' &= \{0, 1, 4, 6\}. \end{aligned}$$

Note que $(A - B) \cap (B - A) = \emptyset$ e, em geral, $A - B \neq B - A$. $A = B$ se, e somente se, $A - B = B - A = \emptyset$. É fácil verificar que:

$$\begin{aligned} x \notin A \cup B &\Leftrightarrow x \notin A \text{ e } x \notin B. \\ x \notin A \cap B &\Leftrightarrow x \notin A \text{ ou } x \notin B. \\ x \notin A - B &\Leftrightarrow x \notin A \text{ ou } x \in B. \\ x \notin A &\Leftrightarrow x \in A'. \end{aligned}$$

Teorema 1.13 *Sejam* A, B *e* C *subconjuntos de* U. *Então*:

1. $A \cup A = A, \ A \cap A = A.$
2. $A \cup B = B \cup A, \ A \cap B = B \cap A.$
3. $A \cup (B \cup C) = (A \cup B) \cup C, \ A \cap (B \cap C) = (A \cap B) \cap C.$
4. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C), \ A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$
5. $A \cup \emptyset = A, \ A \cap \emptyset = \emptyset.$
6. $A \cup U = U, \ A \cap U = A.$

Prova. Provaremos apenas a primeira parte do item *4*.

$$\begin{aligned} x \in A \cup (B \cap C) &\Leftrightarrow x \in A \text{ ou } x \in B \cap C \\ &\Leftrightarrow x \in A \text{ ou } (x \in B \text{ e } x \in C) \\ &\Leftrightarrow (x \in A \text{ ou } x \in B) \text{ e } (x \in A \text{ ou } x \in C) \\ &\Leftrightarrow x \in A \cup B \text{ e } x \in A \cup C \\ &\Leftrightarrow x \in (A \cup B) \cap (A \cup C). \end{aligned}$$

■

Note que a *lei do cancelamento* não vale para a união e interseção de conjuntos, isto é, $A \cup B = A \cup C$ ou $A \cap B = A \cap C$ não implica, em geral, que $B = C$. Para ver isto, basta tomar $A = U$ na primeira equação e $A = \emptyset$ na segunda.

Teorema 1.14 *Sejam A e B subconjuntos de U. Então*:

1. $(A')' = A$.
2. $\emptyset' = U, \ U' = \emptyset$.
3. $A \cup A' = U, \ A \cap A' = \emptyset$.
4. $A \subseteq B \Leftrightarrow B' \subseteq A'$.
5. $(A \cup B)' = A' \cap B', \ (A \cap B)' = A' \cup B'$.

Prova. Provaremos apenas a primeira parte do item *5*.

$$\begin{aligned} x \in (A \cup B)' &\Leftrightarrow x \notin A \cup B \\ &\Leftrightarrow x \notin A \text{ e } x \notin B \\ &\Leftrightarrow x \in A' \text{ e } x \in B' \\ &\Leftrightarrow x \in A' \cap B'. \end{aligned}$$

■

O item *5*. do Teorema acima é chamado as *Leis De Morgan* (Matemático Inglês Augustus De Morgan, 1806 - 1871).

Definição 1.15 *Seja A um conjunto qualquer. Então o conjunto cujos elementos são subconjuntos de A é chamado o* conjunto de potências *de A, em símbolos $\mathcal{P}(A)$, isto é,*

$$\mathcal{P}(A) = \{X : X \subseteq A\}.$$

Note que o conjunto vazio $\emptyset$ e o conjunto A (ele próprio) são subconjuntos de A e, portanto, são elementos de $\mathcal{P}(A)$.

Exemplo 1.16 *Seja $A = \{0, 1\}$. Então os subconjuntos de A são $\emptyset, \{0\}, \{1\}$ e A. Logo,*

$$\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, A\}.$$

Se A é o conjunto vazio $\emptyset$, então $\mathcal{P}(A)$ tem um elemento: $\emptyset$. Note que x e $\{x\}$ não são o mesmo, pois x representa um elemento, enquanto, $\{x\}$ representa um conjunto. Se $x \in A$, então $\{x\} \in \mathcal{P}(A)$.

Sejam I um conjunto qualquer não-vazio e com cada $i \in I$ associaremos um conjunto $A_i \subseteq U$, a família de conjuntos

$$\mathcal{A} = \{A_i : i \in I\} = \{A_i\}_{i \in I}$$

é chamada a *família indexada* pelos elementos de I e o conjunto I é chamado o *conjunto de índice*, isto é, a família indexada $\{A_i\}_{i \in I}$ é a regra que associa a cada elemento $i \in I$ seu objeto A_i. Por exemplo, se $I = \{1, 2\}$, então a família indexada são pares ordenados $\{A_1, A_2\}$.

Seja $\{A_i\}_{i \in I}$ uma família indexada de subconjuntos de U. A união dos conjuntos A_i consiste de todos os elementos de U que pertencem a pelo menos um conjunto A_i, em símbolos

$$\bigcup_{i \in I} A_i = \{x \in U : x \in A_i, \text{ para pelo menos um } i \in I\}.$$

A interseção dos conjuntos A_i consiste de todos os elementos de U que pertencem a todos os conjuntos A_i, em símbolos

$$\bigcap_{i \in I} A_i = \{x \in U : x \in A_i, \text{ para todo } i \in I\}.$$

Observação 1.17 *Quando $I = \mathbb{N}$, usaremos a notação*:

$$\bigcup_{i \in I} A_i = \bigcup_{i=1}^{\infty} A_i \ \ e \ \ \bigcap_{i \in I} A_i = \bigcap_{i=1}^{\infty} A_i.$$

Exemplo 1.18 *Seja $\{A_i\}_{i \in \mathbb{N}}$ uma família indexada de subconjuntos de $\mathbb{R}$, onde*

$$A_i = \{x \in \mathbb{R} : -\frac{1}{i} \leq x \leq \frac{1}{i}\}.$$

Então

$$\bigcup_{i=1}^{\infty} A_i = A_1 \ \ e \ \ \bigcap_{i=1}^{\infty} A_i = \{0\}.$$

Teorema 1.19 *Seja $\{A_i\}_{i \in I}$ uma família indexada de subconjuntos de U.*

1. *Se $A_i \subseteq B$ para qualquer $i \in I$, então $\bigcup_{i \in I} A_i \subseteq B$.*
2. *Se $B \subseteq A_i$ para qualquer $i \in I$, então $B \subseteq \bigcap_{i \in I} A_i$.*

Prova. Provaremos apenas o item *1*. Suponhamos que $A_i \subseteq B$, para qualquer $i \in I$. Se $x \in \bigcup_{i \in I} A_i$, então existe $i \in I$ tal que $x \in A_i$. Logo, por hipótese, $x \in B$. ■

EXERCÍCIOS

1. Numa faculdade em que estudam 250 alunos houve, no final do semestre, reposição nas disciplinas de Matemática e Português, sendo que 10 alunos fizeram reposição das duas matérias, 42 fizeram reposição de Português e 187 alunos não ficaram em reposição. Determinar:

   (a) Quantos alunos ficaram, no total, em reposição?

   (b) Quantos fizeram reposição apenas em Matemática?

   (c) Quantos ficaram em apenas uma matéria?

2. Sejam A, B e C subconjuntos de U com $A \subseteq B$. Mostrar que:

   (a) $A \cup C \subseteq B \cup C$.

   (b) $A \cap C \subseteq B \cap C$.

   (c) $A \cup (B - A) = B$.

   (d) $B - (B - A) = A$.

3. Sejam A e B subconjuntos de U. Mostrar que:

$$A \cap B = \emptyset \Leftrightarrow A - B = A \text{ e } B - A = B.$$

4. Sejam A e B subconjuntos de U. Mostrar que:

   (a) $A \subseteq B \Leftrightarrow A \cup B = B$.

   (b) $A \subseteq B \Leftrightarrow A \cap B = A$.

5. Sejam A e B subconjuntos de U. Mostrar que:

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

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

6. Sejam A, B e C subconjuntos de U. Se $A \cup B = A \cup C$ e $A \cap B = A \cap C$, então $B = C$.

7. Sejam A e B subconjuntos de U. Mostrar que $A \subseteq B \Leftrightarrow A \cap B' = \emptyset$.

8. Sejam A e B subconjuntos de U. Mostrar que $A \cap (A' \cup B) = A \cap B$.

9. Sejam A, B e C subconjuntos de U. Se $A \cap B = \emptyset$ e $A \cup B = U$, então $A = B'$.

10. Sejam A, B e C subconjuntos de U. Mostrar que

$$A = B \Leftrightarrow (A \cap B') \cup (A' \cap B) = \emptyset.$$

11. Sejam A, B e C subconjuntos de U. Se $A \subseteq B$ e $C = B - A$, então $A = B - C$.

12. Sejam A e B subconjuntos de U e seja X um subconjunto de U com as seguintes propriedades:

    (a) $A \subseteq X$ e $B \subseteq X$;

    (b) Se $A \subseteq Y$ e $B \subseteq Y$, então $X \subseteq Y$, para todo $Y \subseteq U$.

    Mostrar que $X = A \cup B$.

13. Enuncie e demonstre um resultado análogo ao anterior, caracterizando $A \cap B$.

14. Sejam A e B subconjuntos de U. Mostrar que:

    (a) $(A \cap B) \cap (A - B) = \emptyset$.

    (b) $A \cap B = A - (A - B)$.

    (c) $A = (A \cap B) \cup (A - B)$.

15. Sejam A e B subconjuntos de U. Usando $A - B = A \cap B'$ mostrar que:

    (a) $A - A = \emptyset$.

    (b) $A - B = A - (A \cap B) = (A \cup B) - B$.

    (c) $(A - B) \cap (B - A) = \emptyset$.

    (d) $A \cup B = (A \cap B) \cup (A - B) \cup (B - A)$.

16. Sejam A, B e C subconjuntos de U. Mostrar que:

    (a) $(A - B) - C = A - (B \cup C)$.

    (b) $A - (B - C) = (A - B) \cup (A \cap C)$.

    (c) $A \cup (B - C) = (A \cup B) - (C - A)$.

    (d) $A \cap (B - C) = (A \cap B) - (C \cap A)$.

17. Sejam A e B subconjuntos de U. Usando $A * B = A' \cap B'$ como definição mostrar que:

    (a) $A * A = A'$.

    (b) $(A * A) * (B * B) = A \cap B$.

    (c) $(A * B) * (A * B) = A \cup B$.

18. Sejam A, B e C subconjuntos de U. A *diferença simétrica* ou *soma Booleana* de A e B é o conjunto $A \triangle B = (A - B) \cup (B - A)$. Mostrar que:

(a) $A \triangle \emptyset = A$.

(b) $A \triangle B = \emptyset \Leftrightarrow A = B$.

(c) $A \triangle B = (A \cup B) - (B \cap A)$.

(d) $A \triangle B = B \triangle A$.

(e) $A \triangle B = A \triangle C \Rightarrow B = C$.

(f) $A \triangle (B \triangle C) = (A \triangle B) \triangle C$.

(g) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.

(h) $A \cup C = B \cup C \Leftrightarrow A \triangle B \subseteq C$.

(i) $(A \cup C) \triangle (B \cup C) = (A \triangle B) - C$.

19. Seja B um subconjunto de U com pelo menos dois elemento, se $A \subseteq B$ e $B - \{x\} \subseteq A$, para todo $x \in B$, então $A = B$.

20. Durante a verificação de controle de qualidade de uma amostra com 1.000 TV's foram encotradas 100 TV's tendo um defeito no tubo de imagem, 75 TV's tendo um defeito no sistema de som, 80 TV's tendo um defeito no controle remoto, 20 TV's tendo um defeito no tubo de imagem e controle remoto, 30 TV's tendo um defeito no tubo de imagem e sistema de som, 15 TV's tendo um defeito no sistema de som e controle remoto, e 5 TV's tendo todos os defeitos relacionados acima. Use um diagrama de Venn para mostrar que:

(a) 195 têm pelo menos um defeito.

(b) 805 não têm defeitos.

(c) 55 têm somente um defeito no tubo de imagem.

(d) 35 têm somente um defeito no sistema de som.

(e) 50 têm somente um defeito no controle remoto.

21. Sejam $\{A_i\}_{i \in I}$ uma família indexada de subconjuntos de U e X um subconjunto de U com as seguintes propriedades:

(a) Para todo $i \in I$, tem-se $X \subseteq A_i$;

(b) Se $Y \subseteq A_i$ para todo $i \in I$, então $Y \subseteq X$.

Mostrar que $X = \bigcap_{i \in I} A_i$.

22. Enuncie e demonstre um resultado análogo ao anterior, caracterizando $\bigcup_{i \in I} A_i$.

23. Seja $\{A_i\}_{i \in I}$ uma família indexada de subconjuntos de U. Mostrar que:

(a) $(\bigcup_{i \in I} A_i)' = \bigcap_{i \in I} A_i'$.

(b) $(\bigcap_{i\in I} A_i)' = \bigcup_{i\in I} A_i'$.

24. Sejam $\{A_i\}_{i\in I}$ uma família indexada de subconjuntos de U, onde $I = \{1, 2, \ldots, n\}$ e A um subconjunto de U. Mostrar que:

(a) $\bigcup_{i=1}^{n} \mathcal{P}(A_i) \subseteq \mathcal{P}(\bigcup_{i=1}^{n} A_i)$.
(b) $\bigcap_{i=1}^{n} \mathcal{P}(A_i) = \mathcal{P}(\bigcap_{i=1}^{n} A_i)$.
(c) $A \cup (\bigcap_{i=1}^{n} A_i) = \bigcap_{i=1}^{n}(A \cup A_i)$.
(d) $A \cap (\bigcup_{i=1}^{n} A_i) = \bigcup_{i=1}^{n}(A \cap A_i)$.

25. Seja $\{A_i\}_{i\in\mathbb{N}}$ uma família indexada de subconjuntos de U. Defina a família indexada $\{B_i\}_{i\in\mathbb{N}}$, onde

$$B_1 = A_1, B_i = A_i - \bigcup_{n=1}^{i-1} A_n.$$

Mostrar que os elementos da família $\{B_i\}_{i\in\mathbb{N}}$ são disjuntos aos pares e $\bigcup_{i=1}^{\infty} B_i = \bigcup_{i=1}^{\infty} A_i$.

26. Seja $\{A_i\}_{i\in\mathbb{N}}$ uma família indexada de subconjuntos de U. Mostrar que:

(a) Se

$$A = \{x \in U : x \in A_i \text{ para uma infinidade de valores de } i\},$$

então

$$A = \bigcap_{i=1}^{\infty} \left(\bigcup_{n=i}^{\infty} A_n \right).$$

(b) Se

$$A = \{x \in U : x \in A_i \text{ exceto um número finito de valores de } i\},$$

então

$$A = \bigcup_{i=1}^{\infty} \left(\bigcap_{n=i}^{\infty} A_n \right).$$

(Sugestão: Se $x \in \bigcap_{i=1}^{\infty}(\bigcup_{n=i}^{\infty} A_n)$, então $x \in \bigcup_{n=i}^{\infty} A_n, \forall i \in \mathbb{N}$. Logo, existe um primeiro $i_1 \in \mathbb{N}$ tal que $x \in A_{i_1}$. Como $x \in \bigcup_{n=i_1+1}^{\infty} A_n$ temos que existe $i_2 \in \mathbb{N}$ com $i_2 > i_1$ tal que $x \in A_{i_2}$, e assim por diante.)

27. Seja $\{A_i\}_{i\in\mathbb{N}}$ uma família indexada de subconjuntos de $\mathbb{R}$, onde

$$A_i = \begin{cases} (-1, \frac{1}{i}], & \text{se } i \text{ é par} \\ (-\frac{1}{i}, 1], & \text{se } i \text{ é ímpar.} \end{cases}$$

Determinar o conjunto A do exercício 26.

28. Seja $\{A_i\}_{i\in\mathbb{N}}$ uma família indexada de subconjuntos de $\mathbb{R}^2$, onde

$$A_i = \{(x, y) \in \mathbb{R}^2 : (x - \frac{(-1)^i}{i})^2 + y^2 < 1\}.$$

Determinar o conjunto A do exercício 26.

Capítulo 2

Relações e Funções

Neste capítulo apresentaremos dois tipos de relações, as quais são básicas para todos os ramos da Matemática: relações de equivalência e funções. O leitor interessado em mais detalhes pode consultar [13, 17].

2.1 Relações

Definição 2.1 *Sejam x e y elementos de um conjunto A. Então o conjunto $\{\{x\},\{x,y\}\}$ é chamado* par ordenado*, em símbolos (x,y); x é chamada a* primeira componente (*ou* coordenada) *e y a* segunda componente (*ou* coordenada)*.*

Provaremos que $(x,y)=(z,w) \Leftrightarrow x=z$ e $y=w$.

De fato, se $x=z$ e $y=w$, então trivialmente $(x,y)=(z,w)$. Reciprocamente, seja $(x,y)=(z,w)$. Então

$$\{\{x\},\{x,y\}\}=\{\{z\},\{z,w\}\}.$$

Pela definição de iguadade de conjuntos, obtemos

$$\{x\}=\{z\} \text{ ou } \{x\}=\{z,w\}.$$

Se $\{x\}=\{z\}$, então devemos ter $\{x,y\}=\{z,w\}$. Assim, $x=z$ e $y=w$. Se, por outro lado, $\{x\}=\{z,w\}$, então devemos ter $\{x,y\}=\{z\}$. Logo, $x=z=w$ e $x=y=z$. Portanto, $x=z=y=w$.

Definição 2.2 *Sejam A e B dois conjuntos. O conjunto de todos os pares ordenados (x,y), onde $x\in A$ e $y\in B$, é chamado o* produto cartesiano *de A e B, nesta ordem, em símbolos $A\times B$, isto é,*

$$A\times B=\{(x,y): x\in A, y\in B\}.$$

Quando $A=B$, temos o produto cartesiano $A^2=A\times A$. O subconjunto

$$D=\{(a,b)\in A^2 : a=b\}$$

é chamado a *diagonal* de A^2.

Exemplo 2.3 *Se* $A = \{0, 1\}$ *e* $B = \{0, 2, 4\}$*, então*

$$A \times B = \{(0,0), (0,2), (0,4), (1,0), (1,2), (1,4)\}$$

e

$$B \times A = \{(0,0), (0,1), (2,0), (2,1), (4,0), (4,1)\}.$$

Assim, claramente $A \times B \neq B \times A$*. De fato,* $A \times B = B \times A \Leftrightarrow A = B$*,* $A = \emptyset$ *ou* $B = \emptyset$*.*

O termo "cartesiano" é tomado emprestado da geometria de coordenadas, onde um ponto no plano é representado por um par ordenado de números reais (x, y), chamado suas coordenadas cartesiana. O produto cartesiano $\mathbb{R} \times \mathbb{R}$ é então o conjunto das coordenadas cartesiana de todos os pontos do plano.

Note que, se o conjunto A contém m elementos e B contém n elementos, então $A \times B$ contém mn elementos, pois no par ordenado (x, y) existem m possibilidades para a primeira componente e n possibilidades para a segunda componente. É fácil verificar que:

$$(x, y) \notin A \times B \Leftrightarrow x \notin A \text{ ou } y \notin B.$$

Teorema 2.4 *Sejam* A, B, C *e* D *conjuntos. Então*:

1. $A \times (B \cap C) = (A \times B) \cap (A \times C)$;
2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$;
3. $A \times (B - C) = (A \times B) - (A \times C)$;
4. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$;
5. *Se* $C \times D \neq \emptyset$*, então* $C \times D \subseteq A \times B \Leftrightarrow C \subseteq A$ *e* $D \subseteq B$*.*

Prova. Provaremos apenas o item (1).

$$\begin{aligned}
(x, y) \in A \times (B \cap C) &\Leftrightarrow x \in A \text{ e } y \in (B \cap C) \\
&\Leftrightarrow x \in A \text{ e } y \in B \text{ e } y \in C \\
&\Leftrightarrow (x, y) \in A \times B \text{ e } (x, y) \in A \times C \\
&\Leftrightarrow (x, y) \in (A \times B) \cap (A \times C).
\end{aligned}$$

■

Definição 2.5 *Sejam* A, B *conjuntos e* $\mathcal{R}$ *um subconjunto de* $A \times B$*. Então* $\mathcal{R}$ *é chamado uma* relação *de* A *em* B*. Se* $(x, y) \in \mathcal{R}$*, então dizemos que* x está relacionado com y*, em símbolos* $x\mathcal{R}y$*. Quando* $A = B$ *dizemos que* $\mathcal{R}$ *é uma* relação binária *em* A*.*

Note que, uma relação é determinada por três conjuntos A, B e um subconjunto $\mathcal{R}$ de $A \times B$, embora chamamo-a simplesmente de relação. Se $\mathcal{R}$ é uma relação de A em B e $\mathcal{S}$ uma relação de C em D, então $\mathcal{R}$ e $\mathcal{S}$ são *iguais*, em símbolos $\mathcal{R} = \mathcal{S}$, se, e somente se, $A = C$, $B = D$ e $x\mathcal{R}y \Leftrightarrow x\mathcal{S}y$, para todo $x \in A$ e $y \in B$.

Exemplo 2.6

$$\begin{aligned}\mathcal{R}_1 &= \{(x,y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 = 1\};\ \mathcal{R}_2 = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : y = 2x\}\ e \\ \mathcal{R}_3 &= \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : x^2 + y^2 = 4\} = \{(\pm 2, 0), (0, \pm 2)\}.\end{aligned}$$

Definição 2.7 *Seja $\mathcal{R}$ uma relação de A em B, então $\mathcal{R}^{-1}$ definida por*

$$\mathcal{R}^{-1} = \{(y,x) \in B \times A : x\mathcal{R}y\}$$

é uma relação de B em A, chamada relação inversa *de $\mathcal{R}$.*

Exemplo 2.8 *Seja $A = \{0,1,2,3\}$. Se*

$$\mathcal{R} = \{(1,1),(1,2),(2,2),(2,3)\},\ \ \textit{então}\ \mathcal{R}^{-1} = \{(1,1),(2,1),(2,2),(3,2)\}.$$

Definição 2.9 *Sejam $\mathcal{R}$ uma relação de A em B e $\mathcal{S}$ uma relação de B em C. Então a* relação composta *de A em C, em símbolos $\mathcal{S} \circ \mathcal{R}$, é dada por*

$$\mathcal{S} \circ \mathcal{R} = \{(x,z) \in A \times C : \exists\ y \in B\ \textit{tal que}\ x\mathcal{R}y\ \ e\ \ y\mathcal{S}z\}.$$

Exemplo 2.10 *Seja $A = \{0,1,2,3\}$. Se*

$$\mathcal{R} = \{(1,1),(1,2),(2,2),(2,3)\}\ \ e\ \ \mathcal{S} = \{(1,0),(2,1),(3,2)\}$$

são duas relações em A, então

$$\mathcal{S} \circ \mathcal{R} = \{(1,0),(1,1),(2,1),(2,2)\}\ \ e\ \ \mathcal{R} \circ \mathcal{S} = \{(2,1),(2,2),(3,2),(3,3)\}.$$

Teorema 2.11 *Sejam $\mathcal{R}$ uma relação de A em B, $\mathcal{S}$ uma relação de B em C e $\mathcal{T}$ uma relação de C em D. Então as seguintes condições são satisfeitas*:

1. $(\mathcal{R}^{-1})^{-1} = \mathcal{R}$.
2. $(\mathcal{S} \circ \mathcal{R})^{-1} = \mathcal{R}^{-1} \circ \mathcal{S}^{-1}$.
3. $(\mathcal{T} \circ \mathcal{S}) \circ \mathcal{R} = \mathcal{T} \circ (\mathcal{S} \circ \mathcal{R})$.

Prova. Provaremos apenas o item (1).

$$(x,y) \in (\mathcal{R}^{-1})^{-1} \Leftrightarrow (y,x) \in \mathcal{R}^{-1} \Leftrightarrow (x,y) \in \mathcal{R}.$$

■

Seja $\mathcal{R}$ uma relação de A em B. Então o *domínio* de $\mathcal{R}$, em símbolos $\mathrm{Dom}\mathcal{R}$, é o conjunto

$$\mathrm{Dom}\mathcal{R} = \{x \in A : \exists\ y \in B\ \text{tal que}\ x\mathcal{R}y\}$$

e a *imagem* de $\mathcal{R}$, em símbolos $\mathrm{Im}\,\mathcal{R}$, é o conjunto

$$\mathrm{Im}\,\mathcal{R} = \{y \in B : \exists\ x \in A\ \text{tal que}\ x\mathcal{R}y\}.$$

Note que $\mathrm{Dom}\mathcal{R} \subseteq A$, $\mathrm{Im}\,\mathcal{R} \subseteq B$ e $\mathcal{R} \subseteq \mathrm{Dom}\mathcal{R} \times \mathrm{Im}\,\mathcal{R}$. O conjunto B é chamado o *contradomínio* da relação $\mathcal{R}$.

Teorema 2.12 *Sejam $\mathcal{R}$ uma relação de A em B e $\mathcal{S}$ uma relação de B em C. Então:*

1. $Dom\mathcal{R} = \operatorname{Im}\mathcal{R}^{-1}$.
2. $\operatorname{Im}\mathcal{R} = Dom\mathcal{R}^{-1}$.
3. $Dom(\mathcal{S}\circ\mathcal{R}) \subseteq Dom\mathcal{R}$.
4. $\operatorname{Im}(\mathcal{S}\circ\mathcal{R}) \subseteq \operatorname{Im}\mathcal{S}$.

Prova. Provaremos apenas os itens (1) e (3).

$$\begin{aligned} x \in \operatorname{Dom}\mathcal{R} &\Leftrightarrow \exists\ y \in B \text{ tal que } (x,y) \in \mathcal{R} \\ &\Leftrightarrow \exists\ y \in B \text{ tal que } (y,x) \in \mathcal{R}^{-1} \\ &\Leftrightarrow x \in \operatorname{Im}\mathcal{R}^{-1}. \end{aligned}$$

e

$$\begin{aligned} x \in \operatorname{Dom}(\mathcal{S}\circ\mathcal{R}) &\Rightarrow \exists\ z \in C \text{ tal que } (x,z) \in \mathcal{S}\circ\mathcal{R} \\ &\Rightarrow \exists\ y \in B \text{ tal que } (x,y) \in \mathcal{R} \text{ e } (y,z) \in \mathcal{S} \\ &\Rightarrow x \in \operatorname{Dom}\mathcal{R}. \end{aligned}$$

■

Definição 2.13 *Uma relação $\mathcal{R}$ em um conjunto não-vazio A é uma* relação de equivalência *em A se as seguintes condições são satisfeitas:*

1. $x\mathcal{R}x, \forall\ x \in A$ (*reflexividade e* $Dom\mathcal{R} = A$);
2. *Se* $x\mathcal{R}y$, *então* $y\mathcal{R}x, \forall\ x, y \in A$ (*simetria*);
3. *Se* $x\mathcal{R}y$ *e* $y\mathcal{R}z$, *então* $x\mathcal{R}z$ (*transitividade*).

Observação 2.14 *Quando uma relação $\mathcal{R}$ em um conjunto A for uma relação de equivalência, adotaremos, em geral, a notação $\sim$ em vez de $\mathcal{R}$ e dizemos que x* é equivalente a *y* módulo $\sim$; *quando não existir perigo de ambiguidade, escreveremos simplesmente $x \sim y$.*

Exemplo 2.15 *Seja A um conjunto não-vazio. Para $x, y \in A$, definimos*

$$x \sim y \Leftrightarrow x = y.$$

Então é fácil verificar que $\sim$ é uma relação de equivalência em A.

Exemplo 2.16 *Seja $A = \mathbb{R}\times\mathbb{R}$. Para $(a,b),(c,d) \in A$, definimos*

$$(a,b) \sim (c,d) \Leftrightarrow a-c, b-d \in \mathbb{Z}.$$

Então $\sim$ é uma relação de equivalência em A.

Solução. $(a,b) \sim (a,b)$, pois $a-a = b-b = 0 \in \mathbb{Z}$. Se $(a,b) \sim (c,d)$, então $(c,d) \sim (a,b)$, pois

$$c-a = -(a-c), d-b = -(b-d) \in \mathbb{Z}.$$

Finalmente, se $(a,b) \sim (c,d)$ e $(c,d) \sim (x,y)$, então $(a,b) \sim (x,y)$, pois

$$a-x = (a-c)-(x-c), y-b = (y-d)-(b-d) \in \mathbb{Z}.$$

Exemplo 2.17 *Seja $A = \mathbb{N}$. Para $x, y \in A$, definimos*

$$x \sim y \Leftrightarrow x+y = 10.$$

Então $\sim$ não é uma relação de equivalência em A, pois $\sim$ não é reflexiva:

$$4+4 \neq 10 \Rightarrow 4 \nsim 4.$$

Exemplo 2.18 *Seja $A = \mathbb{Z}$. Para $x, y \in A$, definimos*

$$x \sim y \Leftrightarrow x-y = 3n, n \in \mathbb{Z}.$$

Então é fácil verificar que $\sim$ é uma relação de equivalência em A.

Seja $\sim$ uma relação de equivalência em A. Para $x \in A$, $\overline{x}$ denota o subconjunto de A formado pelos elementos de A que são equivalentes a x, isto é,

$$\overline{x} = \{y \in A : y \sim x\}.$$

Esse conjunto é chamado a *classe de equivalência de x módulo $\sim$ determinada por x.*

O *conjunto quociente* de A pela relação de equivalência $\sim$, em símbolos

$$\frac{A}{\sim},$$

é o conjunto de todas as classes de equivalências módulo $\sim$. Assim,

$$\frac{A}{\sim} = \{\overline{x} : x \in A\}.$$

Exemplo 2.19 *Seja $A = \{0,1,2,3,4\}$. Então*

$$\begin{aligned} \mathcal{R} \;=\; & \{(0,0),(1,0),(0,1),(1,1),(2,2),(2,3),(3,2), \\ & (2,4),(4,2),(3,3),(3,4),(4,3),(4,4)\} \end{aligned}$$

é uma relação de equivalência em A e

$$\overline{0} = \overline{1} = \{0,1\} \;\; e \;\; \overline{2} = \overline{3} = \overline{4} = \{2,3,4\}.$$

Assim,

$$\frac{A}{\sim} = \{\overline{0}, \overline{2}\}.$$

Exemplo 2.20 *Seja $\sim$ a relação do Exemplo* 2.18. *Então*

$$\frac{A}{\sim} = \{\overline{0}, \overline{1}, \overline{2}\}.$$

Solução.

$$\begin{array}{rcccl} \overline{0} & = & \{x \in A : x \sim 0\} & = & \{x \in A : x = 3n, n \in \mathbb{Z}\}, \\ \overline{1} & = & \{x \in A : x \sim 1\} & = & \{x \in A : x = 3n+1, n \in \mathbb{Z}\}, \\ \overline{2} & = & \{x \in A : x \sim 2\} & = & \{x \in A : x = 3n+2, n \in \mathbb{Z}\}, \end{array}$$

e $\overline{0} = \overline{3}$, $\overline{1} = \overline{4}$, $\overline{2} = \overline{5}$, etc.

Teorema 2.21 *Seja $\sim$ uma relação de equivalência em A. Então*:

1. $\overline{x} \neq \emptyset$, *para todo* $x \in A$.
2. *Se* $y \in \overline{x}$, *então* $\overline{x} = \overline{y}$.
3. $\overline{x} = \overline{y} \Leftrightarrow x \sim y$, $\forall\ x, y \in A$.
4. $\overline{x} \cap \overline{y} = \emptyset$ *ou* $\overline{x} = \overline{y}$, $\forall\ x, y \in A$.
5. $A = \bigcup_{x \in A} \overline{x}$.

Prova. (1) Como $x \in \overline{x}$, para todo $x \in A$, temos que $\overline{x} \neq \emptyset$. (2) Se $y \in \overline{x}$, então $y \sim x$. Agora,

$$z \in \overline{y} \Leftrightarrow z \sim y \text{ e } y \sim x \Leftrightarrow z \sim x \Leftrightarrow z \in \overline{x}.$$

Logo, $\overline{x} = \overline{y}$. (3) direto do item (2). (4) direto do item (3). Para provar (5), como $\overline{x} \subseteq A$, $\forall\ x \in A$ temos que

$$\bigcup_{x \in A} \overline{x} \subseteq A.$$

Reciprocamente, $x \in \overline{x} \Rightarrow \{x\} \subseteq \overline{x}$. Assim,

$$A = \bigcup_{x \in A} \{x\} \subseteq \bigcup_{x \in A} \overline{x}.$$

■

Definição 2.22 *Seja A um conjunto não-vazio. Dizemos que um conjunto $\mathcal{P} \subset \mathcal{P}(A)$ é uma* partição *de A se as seguintes condições são satisfeitas*:

1. $\emptyset \notin \mathcal{P}$;
2. $X = Y$ *ou* $X \cap Y = \emptyset$, *para todos* $X, Y \in \mathcal{P}$ (*disjuntos aos pares*);
3. $\bigcup_{X \in \mathcal{P}} X = A$.

Note que a definição acima é equivalente a: cada elemento de A pertence a um e somente um elemento (ou bloco) de $\mathcal{P}$. Note, também, que cada subconjunto próprio e não-vazio X de A determina uma partição de A em dois subconjuntos, a saber,

$$\mathcal{P} = \{X, A - X\}.$$

Exemplo 2.23 *Seja* $A = \{1, 2, 3, 4, 5, 6, 7\}$. *Então*

$$\mathcal{P}_1 = \{\{1, 3, 5\}, \{2, 7\}, \{4, 6\}\}$$

é uma partição de A *mas*

$$\mathcal{P}_2 = \{\{1, 2, 3\}, \{2, 3, 4, 5\}, \{5, 6, 7\}\} \ e \ \mathcal{P}_3 = \{\{1, 3\}, \{4, 7\}\}$$

não o são.

Exemplo 2.24 *Se* $A = \mathbb{R}$, *então* $\mathcal{P} = \{X, Y, Z\}$, *onde*

$$X = \ ]-\infty, 0[, \ \ Y = [0, 3] \ \ e \ \ Z = \ ]3, +\infty[,$$

é uma partição de A.

Exemplo 2.25 *Se* $A = \mathbb{Z}$, *então* $\mathcal{P} = \{X, Y\}$, *onde*

$$X = \{0, \pm 2, \pm 4, \ldots\} \ \ e \ \ Y = \{\pm 1, \pm 3, \pm 5, \ldots\},$$

é uma partição de A, *pois todo inteiro é par ou ímpar. Note que*

$$\mathcal{R} = \{(x, y) \in A \times A : \exists \ n \in A \ \ tal \ que \ x - y = 2n\}$$

é uma relação de equivalência em A *tal que* $\overline{0} = X$ *e* $\overline{1} = Y$. *Mais geralmente, temos*:

Teorema 2.26 *Se* $\mathcal{P}$ *é uma partição do conjunto* A, *então existe uma única relação de equivalência em* A *cujas classes de equivalência são precisamente os elementos de* $\mathcal{P}$.

Prova. (Existência) Dados $a, b \in A$, definimos

$$a\mathcal{R}b \Leftrightarrow \ \text{existe} \ X \in \mathcal{P} \ \text{tal que} \ a, b \in X.$$

Então $\mathcal{R}$ é uma relação de equivalência em A. De fato, dados $a, b, c \in A$ temos que: $a\mathcal{R}a$, por definição. Se $a\mathcal{R}b$, então existe $X \in \mathcal{P}$ tal que $a, b \in X$; como $b, a \in X$ temos que $b\mathcal{R}a$. Finalmente, se $a\mathcal{R}b$ e $b\mathcal{R}c$, então existem $X, Y \in \mathcal{P}$ tais que $a, b \in X$ e $b, c \in Y$. Como $b \in X \cap Y$ temos, por definição, que $X = Y$. Logo, $a, c \in X$ e $a\mathcal{R}c$.

Agora, vamos mostrar que

$$\frac{A}{\mathcal{R}} = \mathcal{P}.$$

Se $X \in \mathcal{P}$, então existe $a \in A$ tal que $a \in X$, pois $X \neq \emptyset$; assim,

$$b \in X \Leftrightarrow b\mathcal{R}a \Leftrightarrow b \in \overline{a};$$

isto é, $X = \overline{a}$; logo, $\mathcal{P} \subseteq \frac{A}{\mathcal{R}}$. Reciprocamente, sejam $\overline{a} \in \frac{A}{\mathcal{R}}$ e X o elemento de $\mathcal{P}$ tal que $a \in X$. Então

$$b \in \overline{a} \Leftrightarrow b\mathcal{R}a \Leftrightarrow b \in X;$$

isto é, $\overline{a} = X$; logo, $\frac{A}{\mathcal{R}} \subseteq \mathcal{P}$.

(Unicidade) Sejam $\mathcal{R}_1$ e $\mathcal{R}_2$ duas relações de equivalências em A tais que

$$\frac{A}{\mathcal{R}_1} = \mathcal{P} = \frac{A}{\mathcal{R}_2}.$$

Então, para todos $a, b \in A$,

$$(a,b) \in \mathcal{R}_1 \Leftrightarrow \text{ existe } X \in \mathcal{P} \text{ tal que } a, b \in X \Leftrightarrow (a,b) \in \mathcal{R}_2.$$

Portanto, $\mathcal{R}_1 = \mathcal{R}_2$. ■

Exemplo 2.27 *Seja $A = \mathbb{R} \times \mathbb{R}$. Para $(a,b),(x,y) \in A$, definimos*

$$(a,b) \sim (x,y) \Leftrightarrow a - x = b - y.$$

Então é fácil verificar que $\sim$ é uma relação de equivalência em A. Agora, para $(a,b) \in A$,

$$\overline{(a,b)} = \{(x,y) \in A : y = x + b - a\},$$

isto é, as classes de equivalência em A são retas de coeficiente angular igual a 1 passando pelo ponto (a,b). Assim, a relação $\sim$ pode ser vista como uma partição de A numa família de retas paralelas.

EXERCÍCIOS

1. Teste a validade das propriedades reflexiva, simétrica e transitiva para as relações R em $A = \{1,2,3\}$ dadas abaixo. Descreva a partição associada a cada relação de equivalência:

   (a) $R = \{(1,1),(1,2),(2,1),(2,2),(3,3)\}$;

   (b) $R = \{(1,1),(1,2),(2,1),(2,2),(2,3)\}$;

   (c) $R = \{(1,1),(2,2),(2,3),(3,2),(1,3),(3,1)\}$;

   (d) $R = A \times A$.

2. Seja $A = \mathbb{N} \times \mathbb{N}$. Para $(a,b),(c,d) \in A$, definimos

   $$(a,b) \sim (c,d) \Leftrightarrow a + d = b + c.$$

   Mostrar que $\sim$ é uma relação de equivalência em A. Descreva suas classes de equivalência e o conjunto quociente.

3. Seja $A = \mathbb{Z} \times \mathbb{Z}^*$, onde $\mathbb{Z}^* = \mathbb{Z} - \{0\}$. Para $(a, b), (c, d) \in A$, definimos

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Mostrar que $\sim$ é uma relação de equivalência em A. Descreva suas classes de equivalência e o conjunto quociente.

4. Seja $A = \mathbb{C}$. Para $z = a + bi, w = c + id \in A$, definimos

$$z \sim w \Leftrightarrow a^2 + b^2 = c^2 + d^2.$$

Mostrar que $\sim$ é uma relação de equivalência em A. Descreva a classe $\overline{1+i}$.

5. Teste a validade das propriedades reflexiva, simétrica e transitiva para as relações $\sim$ em $\mathbb{Z}$ dadas abaixo. Descreva a partição associada a cada relação de equivalência:

   (a) $x \sim y \Leftrightarrow x < y$;

   (b) $x \sim y \Leftrightarrow xy \geq 0$;

   (c) $x \sim y \Leftrightarrow x - y = 2n + 1$ com $n \in \mathbb{Z}$;

   (d) $x \sim y \Leftrightarrow x^2 = y^2$;

   (e) $x \sim y \Leftrightarrow |x - y| \leq 1$;

   (f) $x \sim y \Leftrightarrow y = x + 1$;

   (g) $x \sim y \Leftrightarrow \frac{x}{y} = 2^n$, para algum $n \in \mathbb{Z}$.

6. Teste a validade das propriedades reflexiva, simétrica e transitiva para as relações binárias através dos seguintes subconjuntos R se $\mathbb{R}^2$. Descreva a partição associada a cada relação de equivalência:

   (a) $R = \{(x, y) \in \mathbb{R}^2 : x \geq 0 \text{ e } y \geq 0\}$;

   (b) $R = \{(x, y) \in \mathbb{R}^2 : y = x\}$;

   (c) $R = \{(x, y) \in \mathbb{R}^2 : x \leq 0 \text{ e } y \geq 0\}$;

   (d) $R = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 4\}$;

   (e) $R = \{(x, y) \in \mathbb{R}^2 : -1 \leq y - x \leq 1\}$.

7. Seja $\mathcal{R}$ uma relação em A. Dê um exemplo para mostrar que o seguinte argumento é falso. Se $x\mathcal{R}y$, então por simetria $y\mathcal{R}x$ e por transitividade $x\mathcal{R}x$, isto é, reflexividade é uma condição supérflua na definição de relação de equivalência em A. (Sugestão: Observe o domínio da relação $\mathcal{R}$.)

8. Sejam $\mathcal{R}$ uma relação em A e $D = \{(x, x) : x \in A\}$. Mostrar que:

   (a) $\mathcal{R}$ é reflexiva se, e somente se, $D \subseteq \mathcal{R}$;

(b) $\mathcal{R}$ é simétrica se, e somente se, $\mathcal{R} = \mathcal{R}^{-1}$;

(c) $\mathcal{R}$ é transitiva se, e somente se, $\mathcal{R} \circ \mathcal{R} \subseteq \mathcal{R}$.

9. Seja $\mathcal{R}$ uma relação reflexiva em A. Mostrar que $\mathcal{R}$ é uma relação de equivalência em A se, e somente se, $\mathcal{R} \circ \mathcal{R}^{-1} = \mathcal{R}$.

10. Seja $A = \mathbb{R}$. Para $a, b \in A^*$, definimos

$$a \sim b \Leftrightarrow ab = x^2 + y^2,$$

para alguns $x, y \in A$. Mostrar que $\sim$ é uma relação de equivalência em A^*.

11. Seja $\mathcal{R}$ uma relação reflexiva em A. Mostrar que $\mathcal{S} \subseteq \mathcal{R} \circ \mathcal{S}$ e $\mathcal{S} \subseteq \mathcal{S} \circ \mathcal{R}$ para qualquer relação $\mathcal{S}$ em A.

12. Sejam $\mathcal{R}$ e $\mathcal{S}$ duas relações de equivalência em A. Mostrar que $\mathcal{S} \circ \mathcal{R}$ é uma relação de equivalência em A se, e somente se, $\mathcal{S} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{S}$.

13. Sejam $\mathcal{R}$ e $\mathcal{S}$ duas relações de equivalência em A. Mostrar que $\mathcal{R} \cup \mathcal{S}$ é uma relação de equivalência em A se, e somente se, $\mathcal{S} \circ \mathcal{R} \subseteq \mathcal{R} \cup \mathcal{S}$ e $\mathcal{R} \circ \mathcal{S} \subseteq \mathcal{R} \cup \mathcal{S}$.

14. Seja $\{\mathcal{R}_i\}_{i \in I}$ uma família indexada de relações de equivalência em A. Mostrar que $\bigcap_{i \in I} \mathcal{R}_i$ é uma relação de equivalência em A.

15. Seja $A \subseteq B$ fixado. Para $X, Y \in \mathcal{P}(B)$, definimos

$$X \sim Y \Leftrightarrow A \cap X = A \cap Y.$$

Mostrar que $\sim$ é uma relação de equivalência em $\mathcal{P}(B)$.

16. Mostrar que as seguintes relações $\sim$ são relações de equivalência em $\mathbb{R}^2$.

(a) $(a, b) \sim (c, d) \Leftrightarrow ad = bc$, com $b, d \in \mathbb{R}^*$;

(b) $(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$;

(c) $(a, b) \sim (c, d) \Leftrightarrow a - c \in \mathbb{Z}$ e $b = d$;

(d) $(a, b) \sim (c, d) \Leftrightarrow ab = cd$;

(e) $(a, b) \sim (c, d) \Leftrightarrow a^2 + b^2 = c^2 + d^2$;

(f) $(a, b) \sim (c, d) \Leftrightarrow xa^2 + yb^2 = xc^2 + yd^2$, com $y > x > 0$.

17. Dê exemplos de relações de equivalência $\sim$ em um conjunto A tais que:

(a) $\frac{A}{\sim} = \{A\}$;

(b) $\overline{x} = \{x\}, \forall\ x \in A$;

(c) A seja um conjunto infinito e o conjunto $\frac{A}{\sim}$ contenha exatamente 5 elementos;

(d) A seja um conjunto infinito e $\frac{A}{\sim}$ também o seja.

18. Seja L o conjunto de todas as retas no plano. Sejam $\mathcal{R}_1$ e $\mathcal{R}_2$ as seguintes relações em L:

$$\mathcal{R}_1 = \{(r,s) : r \parallel s\}, \mathcal{R}_2 = \{(r,s) : r \perp s\}.$$

Mostrar, argumentando informalmente, que:

(a) $\mathcal{R}_1$ é uma relação de equivalência em L;

(b) $\mathcal{R}_2 \circ \mathcal{R}_1 = \mathcal{R}_2$ e $\mathcal{R}_1 \circ \mathcal{R}_2 = \mathcal{R}_2$;

(c) $\mathcal{R}_1 \cup \mathcal{R}_2$ é uma relação de equivalência em L; descreva suas classes de equivalência.

19. Uma relação $\sim$ em A é chamada *circular* se $x \sim y$ e $y \sim z$ implica que $z \sim x$ para todos $x, y, z \in A$. Mostrar que $\sim$ é uma relação de equivalência se, e somente se, $\sim$ é reflexiva e circular.

20. Sejam $\mathcal{R}$ uma relação em A e

$$\mathcal{S} = \{(a,b) : \exists\ n \in \mathbb{N} \text{ e } x_1 = a, x_2, \ldots, x_n = b \text{ tal que } (x_i, x_{i+1}) \in \mathcal{R}\}.$$

Mostrar que:

(a) $\mathcal{S}$ é um relação transitiva em A e se $\mathcal{T}$ é uma relação transitiva em A tal que $\mathcal{R} \subseteq \mathcal{T}$, então $\mathcal{S} \subseteq \mathcal{T}$.

(b) Se $\mathcal{R}$ é reflexiva e simétrica, então $\mathcal{S}$ é uma relação de equivalência em A.

21. Seja $a \in \mathbb{N}$. Mostrar que a família indexada $\{A_n\}_{n\in\mathbb{Z}}$, onde $A_n = [na, (n+1)a[$, é uma partição de $\mathbb{R}$.

22. Descreva a relação de equivalência correspondente a seguinte partição de $\mathbb{Z}$:

$$\{\ldots, -8, -4, 0, 4, 8, \ldots\} \cup \{\ldots, -7, -3, 1, 5, \ldots\} \cup$$
$$\{\ldots, -6, -2, 2, 6, \ldots\} \cup \{\ldots, -5, -1, 3, 7, \ldots\}$$

2.2 Funções

O conceito de função é um dos mais básicos em toda a Matemática. Uma função é, geralmente, definida como segue: Se A e B são dois conjuntos, então uma função de A em B é uma "regra" que a todo elemento $x \in A$ associa um único elemento $y \in B$; para indicar a conexão entre x e y usualmente escreve-se $y = f(x)$.

Se f é uma função de A em B, então o *gráfico* de f é o conjunto de todos os pares ordenados (x, y) tais que $y = f(x)$, isto é,

$$\text{graf}(f) = \{(x,y) \in A \times B : y = f(x)\}.$$

Exemplo 2.28 *Sejam* $A = \{-1, 0, 1, 2\}$, $B = \{0, 1, 2\}$ *e* f *a função definida pela tabela*

x	-1	0	1	2
$f(x)$	0	0	2	1

Então o gráfico de f *é*

$$\text{graf}(f) = \{(-1, 0), (0, 0), (1, 2), (2, 1)\}.$$

Claramente, podemos usar as informações contidas na tabela para construir o gráfico de f e usar as informações contidas no gráfico para construir a tabela de f. Assim, uma função determina completamente seu gráfico e, reciprocamente, seu gráfico determina completamente a função. Logo, não existe necessidade de distinguir entre uma função e seu gráfico. Por essa razão usaremos um tratamento rigoroso para definir função.

Definição 2.29 *Uma* função *ou* aplicação *de* A *em* B *é uma relação* f *de* A *em* B *tal que se* $(x, y_1) \in f$ *e* $(x, y_2) \in f$, *então* $y_1 = y_2$.

Escrevemos $f : A \to B$ para indicar que f é uma função com domínio A e contradomínio B. Se $(x, y) \in f$ dizemos que y é *o valor* ou *a imagem* de x com respeito a f, em símbolos $y = f(x)$, também dizemos que x é a *pré-imagem* de y com respeito a f. Assim, a definição acima é equivalente a: para cada elemento $x \in A$ corresponde a uma única imagem $y \in B$. Note que, se $y_1 = f(x_1)$, $y_2 = f(x_2)$ e $x_1 = x_2$, então $y_1 = y_2$; dizemos que a função f está bem definida, isto é, se $x_1 = x_2$, então $f(x_1) = f(x_2)$. O leitor, sempre que possível, deve fazer o gráfico de uma função, pois é muito importante ter uma idéia geométrica da mesma.

Exemplo 2.30 *Se* $f = \{(-1, 0), (0, 0), (1, 2), (2, 1)\}$, *então* f *é uma função com*

$$Dom f = \{-1, 0, 1, 2\}, \text{Im}\, f = \{0, 1, 2\}$$

e

$$f(-1) = 0, f(0) = 0, f(1) = 2, f(2) = 1.$$

Exemplo 2.31 *Se* $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 = 25\}$, *então* $\mathcal{R}$ *é uma relação, mas* $\mathcal{R}$ *não é uma função, pois* $(3, -4) \in \mathcal{R}$ *e* $(3, 4) \in \mathcal{R}$ *com* $-4 \neq 4$.

Exemplo 2.32 *Sejam* $f : \mathbb{R} \to \mathbb{R}$ *e* $g : \mathbb{R} \to \mathbb{R}$ *duas funções definidas por* $f(x) = \sqrt{x^2}$ *e* $g(x) = |x|$, *respectivamente. Então* $f = g$, *pois* $\sqrt{x^2} = |x|$, $\forall\ x \in \mathbb{R}$.

Exemplo 2.33 *Sejam* $f : \mathbb{R} \to \mathbb{R}$ *e* $g : \mathbb{R} \to \mathbb{R}_+ = \{x \in \mathbb{R} : x \geq 0\}$ *duas funções definidas por* $f(x) = x^2$ *e* $g(x) = x^2$, *respectivamente. Então* $f \neq g$, *pois* $\mathbb{R} \neq \mathbb{R}_+$.

Seja $f : A \to B$ uma função. Então $\text{Im}\, f \subseteq B$. Se $\text{Im}\, f = B$ dizemos que f aplica A *sobre* B ou que f é *sobrejetora*, isto é, dado qualquer $y \in B$ existe pelo menos um $x \in A$ tal que $y = f(x)$.

Exemplo 2.34 *Seja* $f : \mathbb{R} \to \mathbb{R}_+$ *uma função definida por* $f(x) = x^2$. *Então* f *é sobrejetora, pois dado* $y \in \mathbb{R}_+$ *sempre existe* $x \in \mathbb{R}$ *tal que*

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

Uma função $f : A \to B$ é chamada *injetora* se f satisfaz a seguinte condição:

$$(x_1, y) \in f \ \text{ e } \ (x_2, y) \in f \Rightarrow x_1 = x_2, \forall \ x_1, x_2 \in A$$

ou, equivalentemente,

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2, \forall \ x_1, x_2 \in A.$$

Exemplo 2.35 *Seja* $f : \mathbb{R} \to \mathbb{R}$ *uma função definida por* $f(x) = x^3$. *Então* f *é injetora, pois*

$$f(x_1) = f(x_2) \Rightarrow x_1^3 = x_2^3 \Rightarrow x_1^3 - x_2^3 = 0 \Rightarrow (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2) = 0.$$

Logo,

$$x_1 - x_2 = 0 \ \ ou \ \ x_1^2 + x_1x_2 + x_2^2 = 0.$$

Assim, $x_1 = x_2$ *ou*

$$x_1^2 + x_1x_2 + x_2^2 = (x_1 + \frac{x_2}{2})^2 + 3(\frac{x_2}{2})^2 = 0 \Rightarrow x_1 = x_2 = 0.$$

Uma função $f : A \to B$ é chamada *bijetora* ou *casada* se f é sobrejetora e injetora. Note que, se $f : A \to B$ é bijetora, então todo elemento de A tem exatamente uma imagem em B e todo elemento de B tem exatamente uma pré-imagem em A. Assim, todos os elementos de A e todos os elementos de B são associados aos pares. Por essa razão, se $f : A \to B$ é bijetora, dizemos, às vezes, que f é uma *correspondência biunívoca* entre A e B. Em particular, se $f : A \to A$ é bijetora, dizemos que f é uma *permutação* de A.

Exemplo 2.36 *Seja* $f : \mathbb{R} \to \mathbb{R}$ *uma função definida por* $f(x) = \lfloor x \rfloor$, *onde* $\lfloor x \rfloor$ *é igual ao maior inteiro menor do que ou igual a* x, *isto é,*

$$\lfloor x \rfloor = \max\{n \in \mathbb{Z} : n \leq x\}.$$

Então f *não é bijetora, pois*

$$\lfloor \frac{1}{2} \rfloor = \lfloor \frac{3}{4} \rfloor = 0 \ \ e \ \ \frac{1}{2} \neq \lfloor x \rfloor, \forall \ x \in \mathbb{R}.$$

Dizemos que $\lfloor x \rfloor$ *é a* parte inteira *de* x *e que o número real* $x_0 = x - \lfloor x \rfloor$ *é a* parte fracionária *de* x. *Além disso,* x_0 *satisfaz a propriedade*

$$0 \leq x_0 < 1.$$

Seja A um conjunto não-vazio. A função $I_A : A \to A$ dada por

$$I_A(x) = x, \forall\ x \in A$$

é chamada a *função identidade*. Note que I_A é sempre bijetora.

Sejam A, B dois conjuntos e $b \in B$. A função $k : A \to B$ dada por

$$k(x) = b, \forall\ x \in A$$

é chamada a *função constante*. Note que, se A tem pelo menos dois elementos, então k não é injetora e se B tem pelo menos dois elementos, então k não é sobrejetora.

Sejam A um conjunto e $X \subseteq A$. A função $i : X \to A$ dada por

$$i(x) = x, \forall\ x \in X$$

é chamada a *função inclusão*. Note que, i é sempre injetora, portanto, se $X \neq A$, então i não é sobrejetora.

Sejam $f : A \to B$ uma função e $X \subseteq A$. Então f induz uma função $f_X : X \to B$ dada por

$$f_X(x) = f(x), \forall\ x \in X,$$

a qual é chamada a *restrição* de f para X, em símbolos $f_X = f\mid_X$. Por outro lado, se $A \subseteq C$, então a função $F : C \to B$ dada por

$$F(x) = f(x), \forall\ x \in A$$

é chamada a *extensão* de f para C. Note que, $f = F\mid_A$.

Sejam $f : A \to A$ uma função e $X \subseteq A$. Dizemos que X é *invariante sob* f se $f(x) \in X$, para cada $x \in X$, isto é, $f(X) \subseteq X$. Assim, se X é invariante sob f, então a f_X é uma função de X em X. O conjunto

$$A_f = \{x \in A : f(x) = x\}$$

é o conjunto de *pontos fixos* de f e é claramente invariante sob f.

Teorema 2.37 *Sejam $f : A \to B$ e $g : B \to C$ duas funções. Então $g \circ f : A \to C$ é uma função.*

Prova. Pelo Teorema 2.12, temos que

$$\mathrm{Dom}(g \circ f) \subseteq \mathrm{Dom} f = A \text{ e } \mathrm{Im}(g \circ f) \subseteq \mathrm{Im}\, g \subseteq C.$$

Agora, se $x \in \mathrm{Dom} f$, então existe $y \in B$ tal que $(x, y) \in f$. Como $\mathrm{Dom} g = B$ temos que existe $z \in C$ tal que $(y, z) \in g$. Assim, existe $y \in B$ tal que $(x, y) \in f$ e $(y, z) \in g$, para algum $z \in C$, isto é, $(x, z) \in g \circ f$. Logo, $\mathrm{Dom} f \subseteq \mathrm{Dom}(g \circ f)$. Finalmente, suponhamos que $(x, z_1) \in g \circ f$ e $(x, z_2) \in g \circ f$. Então existem $y_1, y_2 \in B$ tais que $(x, y_1) \in f$ e

$(y_1, z_1) \in g$, $(x, y_2) \in f$ e $(y_2, z_2) \in g$, isto é, $(x, y_1) \in f$ e $(x, y_2) \in f$, $(y_1, z_1) \in g$ e $(y_2, z_2) \in g$. Como, por hipótese f é uma função, temos que $y_1 = y_2$. Logo, $(y_1, z_1) \in g$ e $(y_1, z_2) \in g$. Como, por hipótese g é uma função, temos que $z_1 = z_2$. Portanto, $g \circ f$ é uma função. ■

A função $g \circ f$ é chamada a *composição de f com g*. Note que $z = (g \circ f)(x)$ se, e somente se, $(x, z) \in g \circ f$ se, e somente se, existe $y \in B$ tal que $(x, y) \in f$ e $(y, z) \in g$ se, e somente se, existe $y \in B$ tal que $y = f(x)$ e $z = g(y)$. Logo,

$$(g \circ f)(x) = g(f(x)).$$

Assim, para obter o valor da composição de f com g em x primeiro encontramos o valor de f em x para depois encontrarmos o valor de g em $f(x)$.

A compoição de duas funções $f : A \to B$ e $g : B \to C$ pode ser representada pelo diagrama

$$\begin{array}{ccc} A & \to & B \\ \downarrow & & \downarrow \\ A & \to & C \end{array}$$

Se $h : A \to C$ é uma função tal que $h \circ I_A(x) = g \circ f(x)$, $\forall\ x \in A$, dizemos que o *diagrama comuta*. É claro que o diagrama comuta se, e somente se, $h = g \circ f$.

Uma função $f : A \to B$ é chamada *invertível* se $f^{-1} : B \to A$ for uma função. Seja $f : A \to B$ uma função invertível. Então

$$y = f(x) \Leftrightarrow (x, y) \in f \Leftrightarrow (y, x) \in f^{-1} \Leftrightarrow x = f^{-1}(y).$$

Teorema 2.38 *Se $f : A \to B$ é uma função bijetora, então $f^{-1} : B \to A$ é uma função bijetora.*

Prova. Pelo Teorema 2.12, temos que

$$\text{Im}\, f^{-1} = \text{Dom} f = A \text{ e } \text{Dom} f^{-1} = \text{Im}\, f = B.$$

Agora, vamos mostrar que f^{-1} é uma função.

$$(y, x_1) \in f^{-1} \text{ e } (y, x_2) \in f^{-1} \Rightarrow (x_1, y) \in f \text{ e } (x_2, y) \in f \Rightarrow x_1 = x_2,$$

pois f é injetora. Como $\text{Im}\, f^{-1} = A$ temos que f^{-1} é sobrejetora. Finalmente, dados $y_1, y_2 \in B$,

$$\begin{array}{rcl} x = f^{-1}(y_1) = f^{-1}(y_2) & \Rightarrow & (y_1, x) \in f^{-1} \text{ e } (y_2, x) \in f^{-1} \\ & \Rightarrow & (x, y_1) \in f \text{ e } (x, y_2) \in f \\ & \Rightarrow & y_1 = y_2, \end{array}$$

pois f é uma função. Logo, f^{-1} é injetora. ■

Teorema 2.39 *Se $f : A \to B$ é uma função invertível, então $f : A \to B$ é uma função bijetora.*

Prova. Como, por hipótese $f : A \to B$ é uma função invertível, temos que $f^{-1} : B \to A$ é uma função. Assim, pelo Teorema 2.12, temos que $\text{Im}\, f = \text{Dom} f^{-1} = B$. Como $\text{Im}\, f = B$ temos que f é sobrejetora. Finalmente, dados $x_1, x_2 \in A$,

$$\begin{aligned} y = f(x_1) = f(x_2) &\Rightarrow (x_1, y) \in f \text{ e } (x_2, y) \in f \\ &\Rightarrow (y, x_1) \in f^{-1} \text{ e } (y, x_2) \in f^{-1} \\ &\Rightarrow x_1 = x_2, \end{aligned}$$

pois f^{-1} é uma função. Logo, f é injetora. ■

Teorema 2.40 *Seja $f : A \to B$ uma função invertível. Então*:

1. $f^{-1} \circ f = I_A$.
2. $f \circ f^{-1} = I_B$.

Prova. Provaremos apenas o item (1).

Dado $x \in A = \text{Dom} f$. Então existe $y \in B$ tal que $y = f(x)$. Como f é invertível temos que $x = f^{-1}(y)$. Logo,

$$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(y) = x = I_A(x), \forall\ x \in A,$$

isto é, $f^{-1} \circ f = I_A$. ■

Teorema 2.41 *Sejam $f : A \to B$ e $g : B \to A$ duas funções. Se $g \circ f = I_A$ e $f \circ g = I_B$, então $f : A \to B$ é bijetora e $g = f^{-1}$.*

Prova. Exercício. ■

Sejam $f : A \to B$ uma função e $X \subseteq A$. A *imagem direta de X sob f*, em símbolos $f(X)$, é o seguinte subconjunto de B:

$$\begin{aligned} f(X) &= \{y \in B : \exists\ x \in X \text{ tal que } y = f(x)\} \\ &= \{f(x) : x \in X\} \subseteq \text{Im}\, f. \end{aligned}$$

Sejam $f : A \to B$ uma função e $Y \subseteq B$. A *pré-imagem* ou *imagem inversa* de Y sob f, em símbolos $f^{-1}(Y)$, é o seguinte subconjunto de A:

$$f^{-1}(Y) = \{x \in A : f(x) \in Y\}.$$

Observação 2.42 *$f^{-1}(Y)$ faz sentido sempre, mesmo quando f não é injetora e nem sobrejetora. Se f não é injetora, então $f^{-1}(Y)$ pode ter mais de um elemento, mesmo sendo Y um conjunto unitário*; *se f não é sobrejetora, então $f^{-1}(Y)$ pode ser vazio com $Y \neq \emptyset$. Quando $Y = \{y\}$, denotaremos $f^{-1}(\{y\})$ por $f^{-1}(y)$ e, neste caso, $f^{-1}(y)$ é chamada a* fibra *de f sob y.*

Exemplo 2.43 *Sejam* $A = \{1,2,3,4,5,6\}$, $B = \{0,4,6,8\}$ *e*

$$f = \{(1,0),(2,0),(3,0),(4,4),(5,6),(6,6)\}.$$

Então

$$f(\{1,2,3,4\}) = \{0,4\}, f^{-1}(\{6\}) = \{5,6\} \text{ e } f^{-1}(8) = \emptyset.$$

Exemplo 2.44 *Seja* $f : \mathbb{R} \to \mathbb{R}$ *uma função definida por* $f(x) = x^2 - 3x + 2$. *Então*:

$$\begin{aligned} f^{-1}(0) &= \{1,2\}, \\ f^{-1}([0,+\infty[) &=]-\infty,1] \cup [2,+\infty[, \\ f^{-1}(]-\infty,0]) &= [1,2], \\ f^{-1}([1,2]) &= [0,\tfrac{3-\sqrt{5}}{2}] \cup [\tfrac{3+\sqrt{5}}{2},3]. \end{aligned}$$

Exemplo 2.45 *Seja* $f : A \to B$ *uma função. Para* $x, y \in A$, *definimos*

$$x \sim y \Leftrightarrow f(x) = f(y).$$

Então $\sim$ *é uma relação de equivalência em* A *chamada* relação de equivalência associada à função f *ou o* núcleo de equivalência *de* f. *Reciprocamente, se* $\sim$ *é uma relação de equivalência em* A, *definimos uma função*

$$f : A \to \frac{A}{\sim}, \text{ por } f(x) = \overline{x}.$$

É fácil verificar que f *é bem definida e sobrejetora*; f *é chamada a* função canônica *de* A *sobre* $\frac{A}{\sim}$.

Teorema 2.46 *Seja* $f : A \to B$ *uma função. Então*:

1. $f(f^{-1}(Y)) \subseteq Y$, *para todo* $Y \subseteq B$.
2. $X \subseteq f^{-1}(f(X))$, *para todo* $X \subseteq A$.
3. $f(f^{-1}(Y)) = Y$, *para todo* $Y \subseteq B \Leftrightarrow f$ *é sobrejetora.*
4. $X = f^{-1}(f(X))$, *para todo* $X \subseteq A \Leftrightarrow f$ *é injetora.*

Prova. Provaremos apenas o item (3). Suponhamos que $f(f^{-1}(Y)) = Y$, para todo $Y \subseteq B$. Dado $y \in B = f(f^{-1}(B))$, temos que $y = f(x)$, para algum $x \in f^{-1}(B) \subseteq A$; logo, $y = f(x)$, para algum $x \in A$, isto é, f é sobrejetora.

Reciprocamente, pelo item (1), $f(f^{-1}(Y)) \subseteq Y$, para todo $Y \subseteq B$. Por outro lado, se $y \in Y \subseteq B$, então existe, por hipótese, $x \in A$ tal que $y = f(x)$ e, portanto, para algum $x \in f^{-1}(Y)$, pois $f(x) \in Y$; assim,

$$y = f(x) \in f(f^{-1}(Y)).$$

Logo, $Y \subseteq f(f^{-1}(Y))$. ■

O produto cartesiano de dois subconjuntos A e B de U foi definido como o conjunto

$$A \times B = \{(x, y) : x \in A, y \in B\}.$$

Essa definição pode ser estendida, de modo natural, para um número finito de subconjuntos $A_1, A_2, \ldots, A_n$ de U. O produto cartesiano

$$A_1 \times A_2 \times \cdots \times A_n$$

é o conjunto de todas as n-uplas ordenadas

$$(x_1, x_2, \ldots, x_n),$$

onde $x_i \in A_i$ para cada $i = 1, 2, \ldots, n$, isto é,

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \ldots, x_n) : x_i \in A_i, \ \ i = 1, 2, \ldots, n\}.$$

É claro que $\{A_i\}_{i \in I}$ é uma família indexada de subconjuntos de U, onde $I = \{1, 2, \ldots, n\}$. Assim, uma n-upla ordenada pode ser vista como uma função que associa a cada $i \in I$ um elemento $x_i \in A_i$. Se f é essa função, então f é descrita pela tabela abaixo. Usando a tabela abaixo podemos construir a n-upla ordenada $(x_1, x_2, \ldots, x_n)$; reciprocamente, se foi dada a n-upla ordenada $(x_1, x_2, \ldots, x_n)$, então podemos construir a tabela

x	1	2	$\cdots$	n
$f(x)$	x_1	x_2	$\cdots$	x_n

Portanto, a função f e a n-upla ordenada $(x_1, x_2, \ldots, x_n)$ são, essencialmente, a mesma coisa. De um modo geral temos a seguinte definição:

Definição 2.47 *Sejam $\{A_i\}_{i \in I}$ uma família indexada de subconjuntos de U e $A = \bigcup_{i \in I} A_i$. O* produto cartesiano *dos subconjuntos A_i é*

$$\prod_{i \in I} A_i = \{f : I \to A : f \ \text{é uma função e} \ f(i) \in A_i, \forall \ i \in I\}.$$

Exemplo 2.48 *Sejam $I = \{1, 2\}$, $A_1 = \{a, b\}$ e $A_2 = \{c, d\}$. Então $\prod_{i=1}^{2} A_i$ consiste de todas as funções $f : \{1, 2\} \to \{a, b, c, d\}$ tais que $f(1) \in A_1$ e $f(2) \in A_2$. É fácil verificar que existem quatro funções. Assim, podemos identificá-las com os quatro pares ordenados*

$$(a, c), (a, d), (b, c) \ \text{e} \ (b, d),$$

repectivamente. Portanto,

$$\prod_{i=1}^{2} A_i = A_1 \times A_2.$$

Se

$$\mathbf{x} = (x_1, x_2, \ldots, x_n, \ldots) \in \prod_{i \in I} A_i,$$

dizemos que A_i é a *i-ésima componente* de $\prod_{i \in I} A_i$ e $x_i \in A_i$ é a *i-ésima coordenada da família*

$$\mathbf{x} = (x_1, x_2, \ldots, x_n, \ldots).$$

Quando $I \subseteq \mathbb{N}$, dizemos que

$$\mathbf{x} = (x_1, x_2, \ldots, x_n, \ldots)$$

é uma *seqüência*. Seja $A = \prod_{i \in I} A_i$. Para cada índice $i \in I$ definimos uma função p_i de A em A_i por

$$p_i(\mathbf{x}) = x_i, \forall\ \mathbf{x} \in A.$$

A função p_i é chamada a *i-ésima projeção* de A sobre A_i.

EXERCÍCIOS

1. Determinar todas as funções de $A = \{1, 2, 3\}$ em $B = \{1, 2\}$.

2. Verificar se as seguintes funções f são bem definidas:

   (a) $f : \mathbb{Q} \to \mathbb{Z}$ definida por $f(\frac{m}{n}) = m$;

   (b) $f : \mathbb{Q} \to \mathbb{Q}$ definida por $f(\frac{m}{n}) = \frac{m^2}{n^2}$.

3. Dê exemplo de uma função $f : \mathbb{R} \to \mathbb{R}$ que

   (a) seja injetora mas não seja sobrejetora;

   (b) seja sobrejetora mas não seja injetora.

4. Mostrar que as seguintes funções são bijetoras:

   (a) $f : \mathbb{R} \to\ ]0, +\infty[$ definida por $f(x) = e^x$;

   (b) $g :\ ]0, +\infty[\ \to]0, 1[$ definida por $g(x) = \frac{x}{1+x}$;

   (c) $h : \mathbb{R} \to\ ]0, 1[$ definida por $h(x) = \frac{e^x}{1+e^x}$.

5. Para $a, b \in \mathbb{R}$, defina $f_{ab} : \mathbb{R} \to \mathbb{R}$ pela fórmula $f_{ab}(x) = ax + b$ para cada $x \in \mathbb{R}$. Mostrar que:

   (a) $f_{1b} \circ f_{a0} = f_{ab}$;

   (b) Se $a \neq 0$, então f_{ab} é bijetora. Obtenha f_{ab}^{-1}.

6. Seja $f : \mathbb{R} \to \mathbb{R}$ uma função. Sendo $f(2x - 3) = x^2$, determinar $f(x)$.

7. Seja $f : \mathbb{R} \to \mathbb{R}$ a função definida por

$$f(x) = x^2 - 2cx + c^2 - 2c - 1.$$

Sabendo que k e m são as raízes de f, determinar todos os valores reais de c tais que

$$\frac{(k-m)^2 - 2}{(k+m)^2 + 2}$$

seja um número inteiro.

8. Seja $f : [0, 1] \to [a, b]$ a função definida por

$$f(x) = a(1 - x) + bx.$$

Mostrar que f é bijetora. Definir sua inversa.

9. Seja $f : \mathbb{R} - \{-\frac{d}{c}\} \to \mathbb{R} - \{-\frac{a}{c}\}$ a função definida por

$$f(x) = \frac{ax + b}{cx + d},$$

onde $ad - bc \neq 0$. Mostrar que f é bijetora. Definir sua inversa e mostrar que f pode ser escrita como compostas de funções da forma

$$T_k(x) = x + k \text{ e } S_m(x) = \frac{m}{x}.$$

10. Seja $f :]-1, 1[\to \mathbb{R}$ a função definida por

$$f(x) = \frac{x}{1 - |x|}.$$

Mostrar que f é bijetora. Definir sua inversa.

11. Seja $f : [0, +\infty[\to [12, +\infty[$ a função definida por

$$f(x) = x^2 + 2kx + k^2 - 4,$$

onde a constante real k faz com que a função f admita inversa. Sabendo-se que g é a função inversa de f, calcular $g(21)$.

12. Sejam $f : A \to B$ e $g : B \to C$ duas funções. Mostrar que:

(a) Se $g \circ f$ é sobrejetora, então g também o é;

(b) Se $g \circ f$ é injetora, então f também o é;

(c) Se f e g são ambas bijetoras, então $g \circ f$ também o é e, além disso, $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

13. Seja $f : A \to B$ uma função. Mostrar que:

$$f \circ I_A = f = I_B \circ f.$$

14. Sejam $f : A \to B$ uma função e $X_1, X_2 \subseteq A$. Mostrar que:

(a) $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$;

(b) $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$;

(c) $f(X_1) - f(X_2) \subseteq f(X_1 - X_2)$;

(d) Se $X_1 \subseteq X_2$, então $f(X_1) \subseteq f(X_2)$.

15. Seja $f : A \to B$ uma função. Mostrar que f é injetora se, e somente se,

$$f(X_1 \cap X_2) = f(X_1) \cap f(X_2),$$

para todos os subconjuntos $X_1, X_2 \subseteq A$.

16. Sejam $f : A \to B$ uma função e $Y_1, Y_2 \subseteq B$. Mostrar que:

(a) $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$;

(b) $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$;

(c) $f^{-1}(Y_1) - f^{-1}(Y_2) = f^{-1}(Y_1 - Y_2)$;

(d) Se $Y_1 \subseteq Y_2$ então $f^{-1}(Y_1) \subseteq f^{-1}(Y_2)$.

17. Sejam $f : A \to B$ e $g : B \to A$ duas funções tais que $g \circ f = I_A$ e f é sobrejetora ou g é injetora. Mostrar que f e g são bijetoras. Conclua que $f \circ g = I_B$.

18. Seja $f : A \to B$ uma função com A não-vazio. Mostrar que: $f : A \to B$ é injetora se, e somente se, existe uma função $g : B \to A$ tal que $g \circ f = I_A$. (Sugestão: Se $f : A \to B$ é injetora, então $f : A \to C$ é bijetora, onde $C = \operatorname{Im} f$. Assim, $f^{-1} : C \to A$ é uma função. Seja $a \in A$ fixado. Então defina $g : B \to A$ por

$$g(y) = \begin{cases} f^{-1}(y), & \text{se } y \in C \\ a, & \text{se } y \notin C. \end{cases}$$

Continue.)

19. Seja $f : \mathbb{N} \to \mathbb{N}$ definida por $f(n) = n + 1$. Mostrar que existem infinitas funções $g : \mathbb{N} \to \mathbb{N}$ tais que $g \circ f = I_{\mathbb{N}}$ mas não existe inversa à direita.

20. Seja $f : A \to B$ uma função com A não-vazio. Mostrar que: $f : A \to B$ é sobrejetora se, e somente se, existe uma função $g : B \to A$ tal que $f \circ g = I_B$. (Sugestão: Se $f : A \to B$ é sobrejetora, então $f^{-1}(y) \neq \emptyset$, para todo $y \in B$. Logo, para cada $y \in B$, podemos escolher $x = x(y) \in f^{-1}(y)$. Agora, defina $g : B \to A$ por $g(y) = x$, continue.)

21. Seja $f : \mathbb{N} \to \mathbb{N}$ definida por

$$f(n) = \begin{cases} \frac{n}{2}, & \text{se } n \text{ é par} \\ \frac{n+1}{2}, & \text{se } n \text{ é ímpar.} \end{cases}$$

Mostrar que existem infinitas funções $g : \mathbb{N} \to \mathbb{N}$ tais que $f \circ g = I_{\mathbb{N}}$ mas não existe inversa à esquerda.

22. Mostrar que as seguintes afirmações são equivalentes:

(a) $f : A \to B$ é sobrejetora;

(b) Para todas as funções $g, h : B \to C$,

$$g \circ f = h \circ f \Rightarrow g = h;$$

(c) Para cada subconjunto

$$X \subseteq A, \;\; B - f(X) \subseteq f(A - X).$$

(Sugestão: Suponha, por absurdo, que exista $X \subseteq A$ tal que $B - f(X) \nsubseteq f(A - X)$, isto é, existe $y_0 \in B - f(X)$ e $y_0 \notin f(A - X)$. Então $y_0 \neq f(x)$, para todo $x \in A$. Agora, fixado $b \in B$ com $b \neq y_0$, defina $g : B \to B$ por

$$g(y) = \begin{cases} y, & \text{se } y \neq y_0 \\ b, & \text{se } y = y_0 \end{cases}$$

e seja $h = I_B$. Então

$$f(x) = (g \circ f)(x) \;\text{ e }\; f(x) = (h \circ f)(x), \forall \; x \in A,$$

isto é, $g \circ f = h \circ f$. Logo, $h = g$, o que é uma contradição.)

23. Mostrar que as seguintes afirmações são equivalentes:

(a) $f : A \to B$ é injetora;

(b) Para todas as funções $g, h : C \to A$,

$$f \circ g = f \circ h \Rightarrow g = h;$$

(c) Para cada subconjunto $X \subseteq A$,

$$f(A - X) \subseteq B - f(X).$$

24. Sejam $f : A \to B$, $g : B \to A$ duas funções e $X \subseteq A$, $Y \subseteq B$. Mostrar que:

(a) $(g \circ f) \mid_X = g \circ (f \mid_X)$;

(b) $(f\mid_X)^{-1}(Y) = X \cap f^{-1}(Y)$.

25. Sejam $f : A \to C$ e $g : A \to B$ duas funções. Mostrar que existe uma função $h : B \to C$ tal que $f = h \circ g$ se, e somente se,

$$g(x) = g(y) \Rightarrow f(x) = f(y), \forall\ x, y \in A.$$

Mostrar que h é única.

26. Sejam $f : C \to A$ e $g : B \to A$ duas funções com g bijetora. Mostrar que existe uma função $h : C \to B$ tal que $f = g \circ h$ se, e somente se, $\operatorname{Im} f \subseteq \operatorname{Im} g$. Mostrar que h é única.

27. Seja $f : \mathbb{Z} \to \mathbb{Z}$ uma função tal que:

(a) $f(x + y) = f(x) + f(y), \forall\ x, y \in \mathbb{Z}$;

(b) $f(x \cdot y) = f(x) \cdot f(y), \forall\ x, y \in \mathbb{Z}$. Mostrar que $f = I_{\mathbb{Z}}$ ou $f = 0$.

28. Seja $f : \mathbb{Q} \to \mathbb{Q}$ uma função tal que:

(a) $f(x + y) = f(x) + f(y), \forall\ x, y \in \mathbb{Q}$;

(b) $f(x \cdot y) = f(x) \cdot f(y), \forall\ x, y \in \mathbb{Q}$. Mostrar que $f = I_{\mathbb{Q}}$ ou $f = 0$.

29. Seja $f : \mathbb{R} \to \mathbb{R}$ uma função contínua tal que:

(a) $f(x + y) = f(x) + f(y), \forall\ x, y \in \mathbb{R}$;

(b) $f(x \cdot y) = f(x) \cdot f(y), \forall\ x, y \in \mathbb{R}$. Mostrar que $f = I_{\mathbb{R}}$ ou $f = 0$.

30. Seja $f : A \to B$ uma função bijetora. Mostrar que $\widetilde{f} : \mathcal{P}(A) \to \mathcal{P}(B)$ também o é. (Sugestão: Mostrar que $\widetilde{f} : \mathcal{P}(A) \to \mathcal{P}(B)$ definida como $\widetilde{f}(X) = f(X)$, para todo $X \subseteq A$ é uma função bijetora.)

31. Seja A um conjunto qualquer. Mostrar que não existe uma correspondência biunívoca entre A e $\mathcal{P}(A)$. (Sugestão: Primeiro note que a função $i : A \to \mathcal{P}(A)$ definida por $i(x) = \{x\}$ injetora. Agora, suponha, por absurdo, que exista uma função $f : A \to \mathcal{P}(A)$ bijetora. Então para cada $x \in A$, temos que $f(x) \subseteq A$, assim, $x \in f(x)$ ou $x \notin f(x)$. Agora, seja

$$X = \{x \in A : x \notin f(x)\}.$$

Então $X \in \mathcal{P}(A)$ continue.)

32. Seja $f : A \to A$ uma função injetora tal que $f(A) \neq A$. Tomando $x \in A - f(A)$, mostrar que x, $f(x)$, $f(f(x))$, ... são dois a dois distintos.

33. Seja $f : A \to A$ uma função injetora com A finito. Mostrar que f é sobrejetora.

34. Para cada subconjunto $A \subseteq U$, seja $\chi_A : U \to \{0, 1\}$ a função dada por

$$\chi_A(x) = \begin{cases} 1, & \text{se } x \in A \\ 0, & \text{se } x \notin A. \end{cases}$$

Mostrar que:

(a) $\chi_{A\cap B} = \chi_A \cdot \chi_B, \forall\ A, B \subseteq U$;

(b) $\chi_{A\cup B} = \chi_A + \chi_B - \chi_A \cdot \chi_B, \forall\ A, B \subseteq U$;

(c) $\chi_{A\cup B} = \chi_A + \chi_B \Leftrightarrow A \cap B = \emptyset, \forall\ A, B \subseteq U$;

(d) $\chi_{U-A} = 1 - \chi_A$ e $A \subseteq B \Leftrightarrow \chi_A \leq \chi_B, \forall\ A, B \subseteq U$.

35. Seja $\mathcal{F} = \{f : U \to \{0, 1\} : f \text{ é uma função}\}$. Mostrar que existe uma correspondência biunívoca entre $\mathcal{F}$ e $\mathcal{P}(U)$. (Sugestão: Note que $\chi_A \in \mathcal{F}$ e dado $f \in \mathcal{F}$ temos que

$$A_f = f^{-1}(1) = \{x \in U : f(x) = 1\} \subseteq U$$

e $\chi_{A_f} = f$. Agora, defina $\widetilde{f} : \mathcal{P}(U) \to \mathcal{F}$ por $\widetilde{f}(A) = \chi_A = f$, para todo $A \in \mathcal{P}(U)$.)

36. Seja $f : A \to B$ uma função sobrejetora. Para $x, y \in A$, definimos

$$x \sim y \Leftrightarrow f(x) = f(y).$$

Mostrar que $\sim$ é uma relação de equivalência em A cujas classes de equivalência são as fibras de f.

37. Descreva as classes de equivalência e os conjuntos quocientes em relação a $\sim$, associadas as seguintes funções:

(a) $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x^2 - 5x + 6$;

(b) $f : \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = x^2 - 7x + 10$;

(c) $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ definida por $f((x, y)) = y$;

(d) $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ definida por $f((x, y)) = \sqrt{x^2 + y^2}$.

38. Para $x, y \in \mathbb{R}$, definimos

$$x \sim y \Leftrightarrow x - y \in \mathbb{Z}.$$

Mostrar que $\sim$ é uma relação de equivalência em $\mathbb{R}$ e que existe uma correspondência biunívoca entre $\frac{\mathbb{R}}{\sim}$ e

$$\mathbf{S}^1 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}.$$

(Sugestão: Seja $x \in \mathbb{R}$. Então, tomando $\lfloor x \rfloor$ a função maior inteiro, obtemos

$$x \sim x - \lfloor x \rfloor \text{ e } x - \lfloor x \rfloor \in [0, 1[.$$

Assim, para cada $x \in \mathbb{R}$ existe $x_0 = x - \lfloor x \rfloor \in [0,1[$ tal que $\overline{x} = \overline{x}_0$, isto é,

$$\frac{\mathbb{R}}{\sim} = [0,1[.$$

Agora defina

$$f : [0,1[\ \to \mathbf{S}^1 \ \text{ por } \ f(\overline{x}_0) = \exp(2\pi i x_0),$$

onde $i^2 = -1$.)

39. Seja $f : \mathbb{Z} \to \mathbf{S}^1$ definida por $f(n) = \exp(2\pi i n x)$. Mostrar que f é injetora se e somente se $x \notin \mathbb{Q}$. Conclua que

$$\{n \in \mathbb{Z} : f(n) = 1\} = \{km : k \in \mathbb{Z}\} = \mathbb{Z}m,$$

para algum $m \in \mathbb{Z}$ fixado.

40. Seja $x \in \mathbb{R}$. Mostrar que $\lfloor x + n \rfloor = \lfloor x \rfloor + n$, para todo $n \in \mathbb{Z}$.

41. Para $(a,b),(x,y) \in \mathbb{R} \times \mathbb{R}$, definimos

$$(a,b) \sim (x,y) \Leftrightarrow a - x, b - y \in \mathbb{Z}.$$

Mostrar que existe uma correspondência biunívoca entre

$$\frac{\mathbb{R} \times \mathbb{R}}{\sim} \ \text{ e } \ \mathbf{S}^1 \times \mathbf{S}^1.$$

42. Sejam

$$\mathcal{C}[0,1] = \{f : [0,1] \to \mathbb{R} : f \ \text{ é uma função contínua}\}$$

e

$$\mathcal{C}^1[0,1] = \{f : [0,1] \to \mathbb{R} : f(0) = 0 \ \text{ e } \ f' \in \mathcal{C}[0,1]\}.$$

Mostrar que a função $D : \mathcal{C}^1[0,1] \to \mathcal{C}[0,1]$ definida por $D(f) = f'$ é bijetora.

43. Sejam $\{A_i\}_{i \in I}$ e $\{B_j\}_{j \in J}$ duas famílias indexadas. Mostrar que:

(a) $(\bigcup_{i \in I} A_i) \cap (\bigcup_{j \in J} B_j) = \bigcup_{(i,j) \in I \times J} (A_i \cap B_j)$;
(b) $(\bigcap_{i \in I} A_i) \cup (\bigcap_{j \in J} B_j) = \bigcap_{(i,j) \in I \times J} (A_i \cup B_j)$;
(c) $(\bigcap_{i \in I} A_i) \times (\bigcap_{j \in J} B_j) = \bigcap_{(i,j) \in I \times J} (A_i \times B_j)$;
(d) $(\bigcup_{i \in I} A_i) \times (\bigcup_{j \in J} B_j) = \bigcup_{(i,j) \in I \times J} (A_i \times B_j)$.

44. Dizemos que uma família indexada $\{A_i\}_{i \in I}$ é uma *cobertura* de A se $A \subseteq \bigcup_{i \in I} A_i$. Sejam $\{A_i\}_{i \in I}$ e $\{B_j\}_{j \in J}$ duas coberturas distintas de A. Mostrar que a família $\{A_i \cap B_j\}_{(i,j) \in I \times J}$ é uma cobertura de A.

45. Sejam $\{A_i\}_{i \in I}$ e $\{B_j\}_{j \in J}$ partições de A e B, respectivamente. Mostrar que a família $\{A_i \times B_j\}_{(i,j) \in I \times J}$ é uma partição de $A \times B$.

46. Sejam $f : A \to B$ uma função e $\{A_i\}_{i\in I}$, $\{B_j\}_{j\in J}$ famílias indexadas de subconjuntos de A e B, respectivamente. Mostrar que:

    (a) $f(\bigcap_{i\in I} A_i) = \bigcap_{i\in I} f(A_i)$;

    (b) $f^{-1}(\bigcap_{j\in J} B_j) = \bigcap_{j\in J} f^{-1}(B_j)$;

    (c) $f^{-1}(\bigcup_{j\in J} B_j) = \bigcup_{j\in J} f^{-1}(B_j)$.

47. Sejam $f : A \to B$ uma função sobrejetora e $\{B_j\}_{j\in J}$ uma partição de B. Mostrar que $\{f^{-1}(B_j)\}_{j\in J}$ é uma partição de A.

48. Sejam $f : A \to B$ uma função injetora e $\{A_i\}_{i\in I}$ uma partição de A. Mostrar que $\{f(A_i)\}_{i\in I}$ é uma partição de $f(A)$.

Capítulo 3

Relação de Ordem e Enumerabilidade

Neste capítulo apresentaremos o Princípio de Indução Finita (1.^{a} e 2.^{a} Forma), algumas definições e resultados clássicos sobre conjuntos bem ordenados, finitos, infinitos, enumeráveis e não enumeráveis que serão necessários para cursos subsequentes. O leitor interessado em mais detalhes pode consultar [6,17].

3.1 Conjuntos Ordenados

Definição 3.1 *Uma relação binária $\mathcal{R}$ em um conjunto não-vazio A é uma* ordem parcial *em A se as seguintes condições são satisfeitas*:

1. $x\mathcal{R}x, \forall\ x \in A$ (*reflexividade*).

2. *se* $x\mathcal{R}y$ *e* $y\mathcal{R}x$, *então* $x = y$ (*anti-simetria*).

3. *se* $x\mathcal{R}y$ *e* $y\mathcal{R}z$, *então* $x\mathcal{R}z$ (*transitividade*).

Quando uma relação $\mathcal{R}$ em um conjunto A for uma ordem parcial, em geral, adotaremos a notação $\preceq$ em vez de $\mathcal{R}$ e dizemos que x *é menor do que ou igual a* y ou x *precede* y. A notação $\prec$ significa que $x \preceq y$ e $x \neq y$, neste caso, $\prec$ não é uma relação de ordem parcial em A.

Exemplo 3.2 *Seja* $A = \mathbb{R}$. *Para* $x, y \in A$, *definimos*

$$x \preceq y \Leftrightarrow x \leq y,$$

onde "$\leq$*" é a ordem natural em* $\mathbb{R}$. *Então é fácil verificar que* $\preceq$ *é uma ordem parcial em* A.

Exemplo 3.3 *Seja* $A = \mathbb{R} \times \mathbb{R}$. *Para* $(a, b), (c, d) \in A$, *definimos*

$$(a, b) \preceq (c, d) \Leftrightarrow a < c \ \ ou \ \ a = c \ \ e \ \ b \leq d.$$

Então $\preceq$ *é uma ordem parcial em* A.

Solução. $(a, b) \preceq (a, b)$, pois $a = a$ e $b \leq b$. Se $(a, b) \preceq (c, d)$ e $(c, d) \preceq (a, b)$, então

$$a < c \ \text{ ou } \ a = c \ \text{ e } \ b \leq d.$$

e

$$c < a \ \text{ ou } \ a = c \ \text{ e } \ d \leq b.$$

Como a possibilidade $a < c$ e $c < a$ não pode ocorrer, temos que $a = c$, $b \leq d$ e $d \leq b$. Logo, $a = c$ e $b = d$. Portanto, $(a, b) = (c, d)$. Finalmente, Se $(a, b) \preceq (c, d)$ e $(c, d) \preceq (x, y)$, então $(a, b) \preceq (x, y)$. (Prove isto!)

Exemplo 3.4 *Seja* $A = \mathbb{N}$. *Para* $x, y \in A$, *definimos*

$$x \preceq y \Leftrightarrow x \ \ é \ um \ múltiplo \ de \ \ y.$$

Então é fácil verificar que $\preceq$ *é uma ordem parcial em* A.

Exemplo 3.5 *Sejam* A *um conjunto não-vazio e* $\mathcal{P}(A)$ *o conjunto de potências de* A. *Para* $X, Y \in \mathcal{P}(A)$, *definimos*

$$X \preceq Y \Leftrightarrow X \subseteq Y.$$

Então é fácil verificar que $\preceq$ *é uma ordem parcial em* A.

Um *conjunto parcialmente ordenado* é um conjunto A munido com uma ordem parcial. Se B é um subconjunto de A, então A induz uma ordem parcial em B do seguinte modo:

$$x \preceq y, \ \ \forall \ \ x, y \in B \Leftrightarrow x \preceq y \ \text{ em } \ A.$$

Um conjunto parcialmente ordenado A é *totalmente ordenado* ou *uma cadeia* ou *linearmente ordenado* se

$$x \preceq y \ \text{ ou } \ y \preceq x, \forall \ \ x, y \in A.$$

isto é, quaisquer dois elementos de A são comparáveis. Por exemplos, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ são totalmente ordenados pela ordem natural, enquanto os exemplos 3.4 e 3.5, acima, não são totalmente ordenados.

Sejam A conjunto parcialmente ordenado e X um subconjunto de A. O *menor* (*maior*) *elemento* de X é um elemento $a \in X$ tal que $a \preceq x$ ($x \preceq a$) para todo $x \in X$. Dizemos que X é *limitado inferiormente* (*superiormente*) se existir $a \in A$ tal que $a \preceq x$ ($x \preceq a$) para todo $x \in X$. Note que o elemento a não necessariamente pertence a X. O elemento a é chamado de *cota inferior* (*superior*) de X. Um subconjunto de A é *limitado* se ele é limitado inferior e superiormente.

Observação 3.6 *Para mostrar que um elemento $a \in A$ não é cota inferior de $X \subseteq A$ devemos exibir um elemento $x_0 \in X$ tal que $x_0 \prec a$.*

Exemplo 3.7 $\mathbb{N}$ *contém um menor elemento* 1 *com a ordem natural, não contém maior elemento, pois $a < a + 1$ para todo $a \in \mathbb{N}$ (cf. teorema* 3.11 *a seguir), enquanto $\mathbb{Z}$ não contém menor nem maior elemento.*

Um conjunto parcialmente ordenado A é *bem ordenado* se todo subconjunto não-vazio de A contém um menor elemento.

Note que qualquer conjunto A bem ordenado é totalmente ordenado, pois se $a, b \in A$, então o subconjunto

$$\{a, b\} \subseteq A$$

contém um menor elemento a ou b, isto é, $a \preceq b$ ou $b \preceq a$.

Exemplo 3.8 *Os conjuntos $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ com a ordem natural não são bem ordenados, pois o subconjunto*

$$X = \{\ldots, -3, -2, -1, 0\}$$

é não-vazio mas não contém menor elemento. Embora, sejam todos totalmente ordenados. Portanto, há conjuntos totalmente ordenados que não são bem ordenados.

Um dos axiomas que será usado implicitamente muitas vezes, é o seguinte:

Axioma 3.9 (da Boa Ordenação) *Todo subconjunto não-vazio de $\mathbb{N}$ contém um menor elemento.*

Exemplo 3.10 *Sejam $a, b \in \mathbb{N}$. Mostrar que existe $n \in \mathbb{N}$ tal que $na \geq b$.*

Solução. Suponhamos, por absurdo, que $na < b$, para todo $n \in \mathbb{N}$. Seja

$$X = \{b - na : n \in \mathbb{N}\}.$$

Então $X \neq \emptyset$. Assim, pelo Axioma 3.9, existe $x_0 = b - n_0 a \in X$ tal que $x_0 \leq x$, para todo $x \in X$. Como $b - (n_0 + 1)a \in X$, pois X contém todos os inteiros desta forma, temos que

$$b - (n_0 + 1)a = x_0 - a < x_0,$$

o que é uma contradição.

Teorema 3.11 *Se $x, y \in \mathbb{N}$ com $x < y$, então $x + 1 \leq y$.*

Prova. Se $x < y$, então $y - x > 0$. Assim, basta mostrar que o conjunto

$$X = \{x \in \mathbb{N} : 0 < x < 1\}$$

é vazio. Suponhamos, por absurdo, que $X \neq \emptyset$. Como $X \subseteq \mathbb{N}$ e $\mathbb{N}$ é bem ordenado temos, pelo Axioma 3.9, que existe $x_0 \in X$ tal que $x_0 \leq x$, $\forall\ x \in X$. Sendo $x_0 \in X$ temos que

$$0 < x_0 < 1 \Rightarrow 0 < x_0^2 < x_0 < 1.$$

Mas então x_0^2 é um elemento de X menor do que que x_0, o que é uma contradição. Portanto, $y - x \geq 1$, isto é, $x + 1 \leq y$. ■

Exemplo 3.12 *Todo subconjunto de* $\mathbb{N}$ *limitado superiormente possui um maior elemento.*

Solução. Seja X um subconjunto de $\mathbb{N}$ limitado superiormente. Seja

$$Y = \{a \in \mathbb{N} : x \leq a, \forall\ x \in X\} \subseteq \mathbb{N}.$$

Então $Y \neq \emptyset$. Assim, pelo Axioma 3.9, existe $y_0 \in Y$ tal que $y_0 \leq y$, $\forall\ y \in Y$. Agora, vamos mostrar que $y_0 \in X$. Suponhamos, por absurdo, que $y_0 \notin X$. Então $x < y_0$, $\forall\ x \in X$. Assim, pelo Teorema 3.11, $x \leq y_0 - 1$, $\forall\ x \in X$. Logo, $y_0 - 1 \in Y$, o que contradiz a minimalidade de y_0.

Teorema 3.13 (Princípio de Indução $1.^a$ **Forma)** *Seja* X *um subconjunto de* $\mathbb{N}$ *com as seguintes propriedades*:

1. $1 \in X$.

2. *Para cada* $n \in \mathbb{N}$, $n \in X \Rightarrow n + 1 \in X$. *Então* $X = \mathbb{N}$.

Prova. Seja

$$Y = \{y \in \mathbb{N} : y \notin X\} \subseteq \mathbb{N}.$$

Vamos mostrar que $Y = \emptyset$. Suponhamos, por absurdo, que $Y \neq \emptyset$. Então, pelo Axioma 3.9, existe $y_0 \in Y$ tal que $y_0 \leq y$, $\forall\ y \in Y$. Como $1 \in X$ temos que $y_0 \neq 1$ e, pelo Teorema 3.11, $y_0 > 1$, pois $y_0 > 0$. Logo, $0 < y_0 - 1 < y_0$. Pela escolha de y_0 temos que $y_0 - 1 \notin Y$ ou, equivalentemente, $y_0 - 1 \in X$. Assim, pela condição *2*, $y_0 = (y_0 - 1) + 1 \in X$, o que é uma contradição. Portanto, $X = \mathbb{N}$. ■

Exemplo 3.14 *Mostrar que*

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}, \forall\ n \in \mathbb{N}.$$

Solução. Seja

$$X = \left\{ n \in \mathbb{N} : 1 + 2 + \cdots + n = \frac{n(n+1)}{2} \right\} \subseteq \mathbb{N}.$$

Então:

1. $1 \in X$, pois
$$1 = \frac{1(1+1)}{2}.$$

2. Suponhamos, como hipótese de indução, que o resultado seja válido para algum $k > 1$, isto é, $k \in X$.
$$\begin{aligned} 1+2+\cdots+k+(k+1) &= \tfrac{k(k+1)}{2}+(k+1) \\ &= \tfrac{k(k+1)+2(k+1)}{2} \\ &= \tfrac{(k+1)(k+2)}{2}. \end{aligned}$$
Logo, $k+1 \in X$. Portanto, $X = \mathbb{N}$.

Teorema 3.15 (Princípio de Indução 2.ª Forma) *Seja X um subconjunto de $\mathbb{N}$ com as seguintes propriedades*:

1. $1 \in X$.

2. Para cada $n \in \mathbb{N}$, $\{1, 2, \ldots, n\} \subseteq X \Rightarrow n+1 \in X$. Então $X = \mathbb{N}$.

Prova. Seja
$$Y = \{y \in \mathbb{N} : y \notin X\} \subseteq \mathbb{N}.$$
Vamos mostrar que $Y = \emptyset$. Suponhamos, por absurdo, que $Y \neq \emptyset$. Então, pelo Axioma 3.9, existe $y_0 \in Y$ tal que $y_0 \leq y, \forall\ y \in Y$. Como $1 \in X$ temos que $y_0 \neq 1$ e, pelo Teorema 3.11, $y_0 > 1$, pois $y_0 > 0$. Logo, $0 < y_0 - 1 < y_0$. Pela escolha de y_0 temos que $y_0 - 1 \notin Y$ ou, equivalentemente, $k \in X$, $1 \leq k \leq y_0 - 1$, isto é, $\{1, 2, \ldots, y_0 - 1\} \subseteq X$. Assim, pela condição *2*, $y_0 = (y_0 - 1) + 1 \in X$, o que é uma contradição. Portanto, $X = \mathbb{N}$. ■

Exemplo 3.16 *Seja a seqüência $a_1 = 1$, $a_2 = 3$ e $a_n = a_{n-1} + a_{n-2}$, para todo $n \in \mathbb{N}$ com $n \geq 3$. Mostrar que*
$$a_n < \left(\frac{7}{4}\right)^n, \forall\ n \in \mathbb{N}.$$

Solução. Seja
$$X = \{n \in \mathbb{N} : a_n < \left(\frac{7}{4}\right)^n\} \subseteq \mathbb{N}.$$
Então:

1. $1 \in X$, pois $a_1 = 1 < \frac{7}{4}$.

2. Suponhamos, como hipótese de indução, que o resultado seja válido para todo k, $1 \leq k \leq n$, isto é, $\{1, 2, \ldots, n\} \subseteq X$.

$$\begin{aligned} a_{n+1} &= a_n + a_{n-1} \\ &< \left(\frac{7}{4}\right)^n + \left(\frac{7}{4}\right)^{n-1} \\ &= \frac{11}{4}\left(\frac{7}{4}\right)^{n-1} \\ &< \frac{49}{16}\left(\frac{7}{4}\right)^{n-1} = \left(\frac{7}{4}\right)^{n+1}. \end{aligned}$$

Logo, $n+1 \in X$. Portanto, $X = \mathbb{N}$.

Exemplo 3.17 *Mostrar que* $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$, $\forall\ n \in \mathbb{N}$.

Solução. Seja

$$X = \{n \in \mathbb{N} : x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)\} \subseteq \mathbb{N}.$$

Então:

1. $1 \in X$, pois $x^1 - 1 = x - 1$.

2. Suponhamos, como hipótese de indução, que o resultado seja válido para todo k, $1 \leq k \leq n$, isto é, $\{1, 2, \ldots, n\} \subseteq X$.

$$\begin{aligned} x^{n+1} - 1 &= x \cdot x^n - 1 \\ &= x \cdot x^n - x^n + x^n - 1 \\ &= (x-1)x^n + x^n - 1 \\ &= (x-1)x^n + (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1) \\ &= (x-1)(x^n + x^{n-1} + x^{n-2} + \cdots + x + 1) \end{aligned}$$

Logo, $n+1 \in X$. Portanto, $X = \mathbb{N}$.

EXERCÍCIOS

1. Sejam $\mathcal{R}$ uma relação em A e $D = \{(x, x) : x \in A\}$. Mostrar que $\mathcal{R}$ é anti-simétrica se, e somente se, $\mathcal{R} \cap \mathcal{R}^{-1} \subseteq D$.

2. Seja $a \in \mathbb{Z}$. Mostrar que o conjunto $X = \{x \in \mathbb{Z} : a < x < a+1\}$ é vazio.

3. Seja $a \in \mathbb{Z}$. Mostrar que $a - 1$ é o maior inteiro menor do que a.

4. Sejam $a, b \in \mathbb{Z}$ tais que $a^2 < b < (a+1)^2$. Mostrar que não existe $x \in \mathbb{Z}$ tal que $x^2 = b$.

5. Para $m, n \in \mathbb{N}$, definimos

$$m \preceq n \Leftrightarrow \exists\ k \in \mathbb{N} \text{ tal que } n = km.$$

Mostrar que $\preceq$ é uma ordem parcial em $\mathbb{N}$ que não é total.

6. Seja

$$A = \{x \in \mathbb{R} : 0 < x < 1\} =]0, 1[$$

com a ordem natural de $\mathbb{R}$. Mostrar que A é totalmente ordenado e não contém menor nem maior elemento.

7. Seja $\{\mathcal{R}_i\}_{i \in I}$ uma família indexada de ordem parcial em A. Mostrar que $\bigcap_{i \in I} \mathcal{R}_i$ é uma ordem parcial em A.

8. Seja

$$A = \{f : \mathbb{R} \to \mathbb{R} : f \text{ é uma função}\}.$$

Para $f, g \in A$, definimos

$$f \preceq g \Leftrightarrow f(x) \leq g(x), \forall\ x \in \mathbb{R}.$$

Mostrar que $\preceq$ é uma ordem parcial em A que não é total.

9. Seja X um subconjunto de $\mathbb{Z}$ contendo uma cota inferior. Mostrar que X contém uma quantidade infinita de cotas inferiores.

10. Seja X um subconjunto de $\mathbb{Z}$ contendo uma cota inferior. Mostrar que o conjunto

$$Y = \{a \in \mathbb{Z} : a \text{ é uma cota inferior de } X\}$$

é limitado superiormente. Conclua que $X \cap Y$ tem no máximo um elemento.

11. Sejam X e Y dois subconjuntos de $\mathbb{Z}$ limitados inferiormente. Mostrar que $X \cap Y$ e $X \cup Y$ são subconjuntos de $\mathbb{Z}$ limitados inferiormente.

12. Seja $A = \mathbb{N} \times \mathbb{N}$. Para $(a, b), (c, d) \in A$, definimos

$$(a, b) \preceq (c, d) \Leftrightarrow a < c \text{ ou } a = c \text{ e } b \leq d.$$

Então $\preceq$ é uma ordem parcial em A. Mostrar que A é bem ordenado. (Sugestão: Seja $X \subseteq A$ com $X \neq \emptyset$. Então

$$Y = \{a \in \mathbb{N} : (a, b) \in X\} \neq \emptyset \text{ e } Y \subseteq \mathbb{N}.$$

assim, pelo Axioma 3.9, existe $a_0 \in Y$ tal que $a_0 \leq a$, $\forall\ a \in Y$. Agora, seja $V = \{b \in \mathbb{N} : (a_0, b) \in X\}$. Então $V \neq \emptyset$ e $V \subseteq \mathbb{N}$. assim, pelo Axioma 3.9, existe $b_0 \in V$ tal que $b_0 \leq b$, $\forall\ b \in V$. Finalmente, Mostrar que (a_0, b_0) é o menor elemento de X.)

13. Seja A um conjunto totalmente ordenado. Seja $B \subseteq A$ e $b \in B$. mostrar que B contém um menor elemento se, e somente se,

$$C = \{x \in A : x \preceq b\} \cap B$$

contém um menor elemento. (Sugestão: Suponha que $c_0 \in C$ seja o menor de C. Como A é totalmente ordenado temos que

$$b \preceq x \text{ ou } b \succeq x, \forall\ x \in B.$$

Se $b \preceq x$, então $x \in C$ e $c_0 \preceq x$. Se $b \succeq x$, então $c_0 \preceq x$, pois $c_0 \preceq b$. Portanto, pela unicidade do menor elemento, temos que c_0 é o menor elemento de B.)

14. Seja A um conjunto totalmente ordenado. Mostrar que A é bem ordenado se, e somente se, $\{x \in A : x \preceq a\}$ é bem ordenado para todo $a \in A$. (Sugestão: Use o exercício precedente.)

15. Usando o Princípio de Indução Finita, mostrar que $\mathbb{N}$ é bem ordenado. (Sugestão: Suponha, por absurdo, que X é um subconjunto não-vazio de $\mathbb{N}$ sem menor elemento. Seja

$$Y = \{k \in \mathbb{N} : k \leq x, \forall\ x \in X\} \subseteq \mathbb{N}.$$

Então:

   (a) $1 \in Y$, pois 1 é o menor elemento de $\mathbb{N}$.

   (b) Suponha, como hipótese de indução, que o resultado seja válido para algum $k > 1$, isto é, $k \in Y$ e $k \leq x$ para todo $x \in X$. Como $k \notin X$, pois X não contém menor elemento, temos que $k < x$ para todo $x \in X$. Pelo Teorema 3.11, $k+1 \leq x$ para todo $x \in X$. assim, $k+1 \in Y$. Logo, $Y = \mathbb{N}$. Finalmente, como $X \cap Y = \emptyset$ continue.)

16. Mostrar que todo subconjunto de $\mathbb{Z}$ limitado inferiormente é bem ordenado. (Sugestão: Sejam $X \subseteq \mathbb{Z}$ um subconjunto limitado inferiormente e a uma cota inferior de X. Se $a \in X$, nada há para ser provado. Se $a \notin X$ e $b \in X$, então $a+(b-a) = b \in X$ e $b - a > 0$. Assim, $S = \{n \in \mathbb{N} : a + n \in X\}$ é não-vazio e pelo Axioma 3.9, existe $n_0 \in S$ tal que $n_0 \leq k$, $\forall\ k \in S$. Continue.)

17. Sejam A um conjunto bem ordenado, $x_0 \in A$ e X um subconjunto de A com as seguintes propriedades:

   (a) $x_0 \in X$.

   (b) $\{x \in A : x \prec a\} \subseteq X \Rightarrow a \in X$. Mostrar que $X = A$.

18. Se $m, n \in \mathbb{N}$ com $m < n$, então existe um único $p \in \mathbb{N}$ tal que $m + p = n$.

19. Para cada $n \in \mathbb{N}$ mostrar que:

(a) $1 + 3 + \cdots + (2n-1) = n^2$.

(b) $1^3 + 3^3 + \cdots + (2n-1)^3 = n^2(2n^2-1)$.

(c) $1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + n(n+1)(n+2) = \frac{n(n+1)(n+2)(n+3)}{4}$.

(d) $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n(n+1)} = 1 - \frac{1}{n+1}$.

(e) $\sum_{k=1}^{n} (-1)^k \frac{k+1}{(2k+1)(2k+3)} = (-1)^n \frac{1}{4(2n+3)} - \frac{1}{12}$.

(f) $4^n + 15n - 1$ é um múltiplo de 9.

(g) $n(n^2+5)$ é um múltiplo de 6.

(h) $5^n - 4n - 1$ é um múltiplo de 16.

(i) $n^3 + (n+1)^3 + (n+2)^3$ é um múltiplo de 9.

20. Sejam $a, b, n, k \in \mathbb{Z}$ tais que $0 \leq k \leq n$. O coeficiente binomial é dado pela fórmula

$$\binom{n}{k} = \frac{n!}{k!(n-k)!},$$

onde $0! = 1$ e $(n+1)! = (n+1)n!$. Mostrar que:

(a) $\binom{n}{k} = \binom{n}{n-k}$.

(b) $\binom{n}{k} < \binom{n}{k+1} \Leftrightarrow 0 \leq k < \frac{1}{2}(n-1)$. (Sugestão: $\binom{n}{k}\frac{n-k}{k+1} = \binom{n}{k+1}$.)

(c) $\binom{n}{k} = \binom{n}{k+1} \Leftrightarrow k$ é ímpar e $k = \frac{1}{2}(n-1)$.

(d) $k < n \Rightarrow \binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$.

(e) $\binom{n}{k} \in \mathbb{N}$.

(f) $n\binom{n-1}{k} = (k+1)\binom{n}{k+1}$.

(g) $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$.

(h) $2\binom{n}{2} + n = n^2, \forall\ n \in \mathbb{N}, n \geq 2$.

(i) $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n$.

(j) $\binom{n}{1} + 2\binom{n}{2} + \cdots + (n-1)\binom{n}{n-1} + n\binom{n}{n} = n2^{n-1}$.

21. Sejam $a_1, \ldots, a_m, n \in \mathbb{Z}$ com $n \geq 0$. Mostrar que

$$(a_1 + \cdots + a_m)^n = \sum_{\substack{k_i \geq 0 \\ k_1 + \cdots + k_m = n}} \frac{n!}{k_1! \cdots k_m!} a_1^{k_1} \cdots a_m^{k_m}.$$

(Sugestão: Note que

$$(a_1 + a_2)^n = \sum_{k=0}^{n} \binom{n}{k} a_1^{n-k} a_2^k = \sum_{j+k=n} \frac{n!}{j!k!} a_1^j a_2^k$$

e use indução sobre m.)

22. Para cada $n \in \mathbb{N}$ mostrar que:

    (a) $n < 2^n$.

    (b) $n \geq 4 \Rightarrow 2^n < n!$.

    (c) $n \geq 5 \Rightarrow 2n - 3 < 2^{n-2}$.

    (d) $n \geq 2 \Rightarrow \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n}$.

23. Para cada $n \in \mathbb{N}$ mostrar que:

    (a) $\sum_{k=1}^{n} (k \cdot k!) = (n+1)! - 1$.

    (b) $\sum_{k=1}^{n} \left[(-1)^k (k-1)^2 + (-1)^{k+1} k^2\right] = (-1)^{n+1} n$.

    (c) $\sum_{k=1}^{n} \left[\frac{(k-1)k}{2} + \frac{k(k+1)}{2}\right] = \frac{n(n+1)(2n+1)}{6}$.

24. Para cada $n \in \mathbb{N}$ mostrar que:

    (a) $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

    (b) $1^3 + 2^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2$.

    (c) Encontre uma fórmula para $1^k + 2^k + \cdots + n^k$ com $k \in \mathbb{N}$. (Sugestão: $(1+1)^2 = 1^2 + 2 \cdot 1 \cdot 1 + 1^2, \ldots, (n+1)^2 = n^2 + 2 \cdot n \cdot 1 + 1^2$, agora somando obtemos

    $$(n+1)^2 = 1^2 + 2(1 + 2 + \cdots + n) + n.$$

    Assim,

    $$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

    $(1+1)^3 = 1^3 + 3 \cdot 1^2 \cdot 1 + 3 \cdot 1 \cdot 1^3 + 1^3$, continue.)

25. Seja P_n um polígono convexo com n lados ($n \geq 3$). Mostrar que a soma dos ângulos internos de P_n é dada por $(n-2)180°$. (Sugestão: Note que $P_{n+1} = P_n \cup P_3$.)

26. Seja $f : \mathbb{N} \to \mathbb{N}$ uma função definida por

$$f(n) = \begin{cases} \frac{n}{2}, & \text{se } n = 2k \\ 3n + 1, & \text{se } n = 4k + 1 \\ 3n - 1, & \text{se } n = 4k - 1. \end{cases}$$

    Mostrar que para todo $n \in \mathbb{N}$ existe $m \in \mathbb{N}$ tal que $f^m(n) = 1$, onde $f^m = f^{m-1} \circ f$.

27. Sejam $a, b \in \mathbb{Z}^*$ e $n \in \mathbb{N}$. Definimos a *potência n-ésima* de a por $a^n = a^{n-1}a$ e $a^0 = 1$. Mostrar que:

(a) $a^m a^n = a^{m+n}$, $\forall\ m, n \in \mathbb{N}$. (Sugestão: Vamos fixar m e considerar o conjunto

$$X = \{n \in \mathbb{N} : a^m a^n = a^{m+n}\}.$$

Então $1 \in X$, pois por definição $a^{m+1} = a^m a$. Continue.).

(b) $(a^m)^n = a^{mn}$, $\forall\ m, n \in \mathbb{N}$.

(c) $(ab)^n = a^n b^n$, $\forall\ n \in \mathbb{N}$.

28. Seja $z = r(\cos\theta + i\,\mathrm{sen}\,\theta)$ com $r > 0$. Mostrar que

$$z^n = r^n(\cos n\theta + i\,\mathrm{sen}\,n\theta), \forall\ n \in \mathbb{N}.$$

29. Para cada $n \in \mathbb{N}$ mostrar que

$$\mathrm{sen}\,x + \mathrm{sen}\,2x + \cdots + \mathrm{sen}\,nx = \frac{\mathrm{sen}\,\frac{(n+1)x}{2} \cdot \mathrm{sen}\,\frac{nx}{2}}{\mathrm{sen}\,\frac{x}{2}},\ \text{se}\ x \neq 2k\pi.$$

30. Para cada $n \in \mathbb{N}$ mostrar que

$$\cos x + \cos 2x + \cdots + \cos nx = \frac{\mathrm{sen}\,\frac{(n+1)x}{2} \cdot \cos\frac{nx}{2}}{\mathrm{sen}\,\frac{x}{2}},\ \text{se}\ x \neq 2k\pi.$$

31. Para cada $n \in \mathbb{N}$ mostrar que

$$1 + \frac{k}{n} \leq \left(1 + \frac{1}{n}\right)^k < 1 + \frac{k}{n} + \frac{k^2}{n^2}, \forall\ k, 1 \leq k \leq n.$$

32. Para cada $n \in \mathbb{N}$ mostrar que

$$2 \leq \left(1 + \frac{1}{n}\right)^n < 3.$$

33. Para cada $n \in \mathbb{N}$, com $n \geq 6$, mostrar que

$$\frac{\left(\frac{n+1}{3}\right)^{n+1}}{\left(\frac{n}{3}\right)^n} \leq n + 1 \leq \frac{\left(\frac{n+1}{2}\right)^{n+1}}{\left(\frac{n}{2}\right)^n}.$$

34. Para cada $n \in \mathbb{N}$, com $n \geq 2$, mostrar que

$$\left(\frac{n+1}{3}\right)^n < n! < \left(\frac{n+1}{2}\right)^n.$$

35. Para cada $n \in \mathbb{N}$, com $n \geq 6$, mostrar que

$$2^n n! < n^n < 3^n n!.$$

36. Para cada $n \in \mathbb{Z}_+$ mostrar que:

(a) $(1+x)^n \geq 1+nx, \forall\ x \in \mathbb{R}$ com $x > -1$.

(b) $(1+x)^{2n} \geq 1+2nx, \forall\ x \in \mathbb{R} - \{-1\}$.

(c) $1 - x + \cdots + (-1)^n x^{n-1} + (-1)^{n+1} x^n = \frac{1+x^{n+1}}{1+x}, \forall\ x \in \mathbb{R} - \{-1\}$ e n ímpar.

(d) $(1+x)(1+x^2)(1+x^{2^2})\cdots(1+x^{2^n}) = \frac{1-x^{2^{n+1}}}{1-x}, \forall\ x \in \mathbb{R} - \{1\}$.

37. Para cada $n \in \mathbb{N}$ mostrar que:

(a) $1 + 2 \cdot \frac{1}{2} + 3 \cdot \frac{1}{4} + \cdots + n \cdot \frac{1}{2^{n-1}} = 4 - \frac{n+2}{2^{n-1}}$.

(b) $\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\cdots\left(1 - \frac{1}{n+1}\right) = \frac{1}{n+1}$.

(c) $\left(1 + \frac{1}{1}\right)\left(1 + \frac{1}{2}\right)\cdots\left(1 + \frac{1}{n}\right) = n + 1$.

38. Ache a falha na seguinte "prova". Mostraremos que quaisquer dois elementos de $\mathbb{N}$ são iguais. Seja

$$\max\{m,n\} = \begin{cases} m, & \text{se } n \leq m \\ n, & \text{se } m < n. \end{cases}$$

Seja

$$X = \{k \in \mathbb{N} : \forall\ m,n \in \mathbb{N},\ \max\{m,n\} = k \Rightarrow m = n\}.$$

Então:

(a) $1 \in X$, pois $\max\{m,n\} = 1 \Rightarrow m = n$.

(b) Suponha, como hipótese de indução, que o resultado seja válido para algum $k > 1$. Seja $m, n \in \mathbb{N}$ tais que $\max\{m,n\} = k+1$. Então $\max\{m-1, n-1\} = k$. Logo, pela hipótese de indução, $m - 1 = n - 1$. Assim, $m = n$ e $k + 1 \in X$. Portanto, $X = \mathbb{N}$.

39. Se A tem n elementos, então $\mathcal{P}(A)$ tem 2^n elementos para todo $n \in \mathbb{Z}_+$. (Sugestão: Seja

$$X = \{n \in \mathbb{Z}_+ : \mathcal{P}(A)\ \text{tem}\ 2^n\ \text{elementos}\} \subseteq \mathbb{Z}_+.$$

Então:

(a) $0 \in X$.

(b) Suponha, como hipótese de indução, que o resultado seja válido para algum $k > 0$, isto é, $k \in X$. Sejam B um conjunto com $k + 1$ elementos e $b \in B$. Então $B = \{b\} \cup B - \{b\}$, isto é, B é dividido em dois subconjuntos: um que contém b e outro que não contém b, continue.)

3.2 Conjuntos Finitos e Infinitos

Nesta seção apresentaremos uma das distinções fundamentais em matemática, qual seja, entre conjuntos finitos e infinitos. A distinção é intuitivamente forçada, mesmo na ausência de uma definição precisa, não pode existir qualquer dúvida se um dado conjunto é finito ou infinito. Informalmente, um conjunto é finito se ele contém n elementos, com $n \in \mathbb{N}$. Entretanto, para conjuntos infinitos a resposta depende da "aproximação cardinal." Dizemos que dois conjuntos A e B têm o mesmo *número cardinal* se existir uma correspondência biunívoca de A sobre B.

Para cada $k \in \mathbb{N}$, $\mathbb{N}_k$ denota o subconjunto $\{1, 2, \ldots, k\}$ de $\mathbb{N}$, isto é,

$$\mathbb{N}_k = \{n \in \mathbb{N} : 1 \leq n \leq k\}.$$

Teorema 3.18 *Sejam $k, l \in \mathbb{N}$. Se $k < l$, então não existe bijeção de $\mathbb{N}_k$ sobre $\mathbb{N}_l$.*

Prova. Vamos usar indução sobre k.

1. Se $k = 1$, nada há para provar.

2. Suponhamos, como hipótese de indução, que o teorema seja válido para algum $k > 1$ e todo $l > k$.

Seja $\mathbb{N}_{k+1} = \mathbb{N}_k \cup \{k+1\}$ e suponhamos, por absurdo, que exista uma bijeção

$$f : \mathbb{N}_{k+1} \to \mathbb{N}_l$$

para algum $l > k+1$. Sejam $m = f(k+1)$ e $h : \mathbb{N}_l \to \mathbb{N}_l$ definida por

$$h(n) = \begin{cases} m, & \text{se } n = l \\ l, & \text{se } n = m \\ n, & \text{se } n \notin \{l, m\}. \end{cases}$$

Se $m = l$, então $h = I_{\mathbb{N}_l}$. Caso contrário, $h \circ h = I_{\mathbb{N}_l}$. Logo, h é uma função bijetora. Assim, a função

$$g = h \circ f : \mathbb{N}_{k+1} \to \mathbb{N}_l$$

é também bijetora e $g(k+1) = l$. Portanto,

$$g_1 : \mathbb{N}_k \to \mathbb{N}_{l-1} \text{ dada por } g_1(n) = g(n)$$

é bijetora com $k < l - 1$, o que contradiz a hipótese de indução. ■

Lema 3.19 *Seja $k \in \mathbb{N}$. Se $f : \mathbb{N}_k \to \mathbb{N}_k$ é injetora, então f é sobrejetora.*

Prova. Vamos usar indução sobre k.

1. Se $k = 1$, nada há para provar.

2. Suponhamos, como hipótese de indução, que o lema seja válido para algum $k > 1$ e consideremos $f : \mathbb{N}_{k+1} \to \mathbb{N}_{k+1}$ injetora.

Sejam $k = f(k+1)$ e $h : \mathbb{N}_{k+1} \to \mathbb{N}_{k+1}$ definida por

$$h(n) = \begin{cases} k, & \text{se } n = k+1 \\ k+1, & \text{se } n = k \\ n, & \text{se } n \notin \{k, k+1\}. \end{cases}$$

Então $g = h \circ f$ é injetora e $g(k+1) = k+1$. Como $\mathbb{N}_{k+1} = \mathbb{N}_k \cup \{k+1\}$ temos que

$$g_1 : \mathbb{N}_k \to \mathbb{N}_k \text{ dada por } g_1(n) = g(n)$$

é injetora. Logo, pela hipótese de indução, g_1 é bijetora e, assim, g também o é. Portanto,

$$f = h^{-1} \circ g = h \circ g$$

é sobrejetora. ■

Definição 3.20 *Um conjunto A é* finito *quando é vazio ou quando ele tem o mesmo número cardinal de $\mathbb{N}_k$. Caso contrário, dizemos que A é* infinito.

Sejam A conjunto finito e $f : \mathbb{N}_k \to A$ uma bijeção. Então se existir também uma bijeção $g : \mathbb{N}_l \to A$, então a função $g^{-1} \circ f : \mathbb{N}_k \to \mathbb{N}_l$ é bijetora. Logo, pelo Teorema 3.18, $k = l$. Portanto, para cada conjunto finito A existe um único $k \in \mathbb{N}$ tal que existe uma bijeção $f : \mathbb{N}_k \to A$, note que se $k > 1$, então existe mais de uma bijeção. Chamamos $k \in \mathbb{N}$ o *número cardinal* de A, em símbolos $\#(A) = k$. Quando $A = \emptyset$ temos que $\#(A) = 0$.

Observação 3.21 *Uma correspondência biunívoca*

$$f : \mathbb{N}_k \to A$$

significa uma contagem dos elementos de A. Assim, fazendo

$$f(1) = x_1, \ldots, f(k) = x_k$$

temos que

$$A = \{x_1, \ldots, x_k\}.$$

Exemplo 3.22 *Todo subconjunto finito de $\mathbb{Z}$ possui um menor elemento.*

Solução. Seja

$$X = \{k \in \mathbb{N} : \forall\ A \subseteq \mathbb{Z}, \text{ com } \#(A) = k, \text{ possua um menor elemento}\} \subseteq \mathbb{N}.$$

Então:

1. $1 \in X$, pois todo subconjunto unitário possui um menor elemento.

2. Suponhamos, como hipótese de indução, que o resultado seja válido para algum $k > 1$, isto é, $k \in X$.

Seja $A = \{x_1, \ldots, x_{k+1}\} \subseteq \mathbb{Z}$. Então, pela hipótese de indução, o conjunto $A' = \{x_1, \ldots, x_k\} \subseteq \mathbb{Z}$ possui um menor elemento, digamos x_0'. Assim, $x_0 = \min\{x_0', x_{k+1}\}$ é tal que $x_0 \leq x, \forall\ x \in A$, isto é, A possui um menor elemento. Logo, $k+1 \in X$. Portanto, $X = \mathbb{N}$. De modo análogo, mostra-se que todo subconjunto finito de $\mathbb{Z}$ possui um maior elemento. Assim, todo subconjunto finito de $\mathbb{Z}$ é limitado.

Exemplo 3.23 $\mathbb{N}$ *é um conjunto infinito.*

Solução. Suponhamos, por absurdo, que $\mathbb{N}$ seja um conjunto finito. Então existe um bijeção $f : \mathbb{N} \to \mathbb{N}_k$. Assim, $f\ |_{\mathbb{N}_{k+1}}$é injetora. Logo, pelo exercício 1 abaixo, $k + 1 = \#(X) \leq \#(\mathbb{N}_k) = k$, o que é uma contradição.

Exemplo 3.24 *O conjunto*

$$A = \{x \in \mathbb{R} : x^2 - 4x + 3 = 0\}$$

é finito, pois existe uma correspondência biunívoca de A sobre $\mathbb{N}_2$.

Teorema 3.25 *Sejam A e B dois conjuntos finitos e disjuntos. Então*

$$\#(A \cup B) = \#(A) + \#(B).$$

Prova. Suponhamos que $\#(A) = m$ e $\#(B) = n$. Então existem bijeções $f : A \to \mathbb{N}_m$ e $g : B \to \mathbb{N}_n$. Seja $h : A \cup B \to \mathbb{N}_{m+n}$ definida por

$$h(x) = \begin{cases} f(x) & \text{se } x \in A \\ m + g(x) & \text{se } x \in B. \end{cases}$$

Agora, é fácil verificar que h é bijetora (prove isto!). ■

Corolário 3.26 *Sejam A e B dois conjuntos finitos. Então*

$$\#(A \cup B) = \#(A) + \#(B) - \#(A \cap B).$$

Prova. Sejam

$$C = A - (A \cap B) \text{ e } D = B - (A \cap B).$$

Então é claro que

$$A = C \cup (A \cap B) \text{ e } B = D \cup (A \cap B)$$

são uniões disjuntas. Assim,

$$\#(A) = \#(C) + \#(A \cap B) \text{ e } \#(B) = \#(D) + \#(A \cap B).$$

Como

$$C \cap D \subseteq A \cap B \text{ e } C \cap (A \cap B) = \emptyset$$

temos que $C \cap D = \emptyset$. Portanto,

$$A \cup B = (C \cup D) \cup (A \cap B) \text{ e } (C \cup D) \cap (A \cap B) = \emptyset.$$

Logo,

$$\#(A \cup B) = \#(C \cup D) + \#(A \cap B).$$

Sendo

$$\#(C \cup D) = \#(C) + \#(D), \ \ \#(C) = \#(A) - \#(A \cap B)$$

e

$$\#(D) = \#(B) - \#(A \cap B)$$

temos que

$$\#(A \cup B) = \#(A) + \#(B) - \#(A \cap B).$$

■

Teorema 3.27 *Seja A um conjunto finito. Então $f : A \to A$ é injetora se, e somente se, ela é sobrejetora.*

Prova. Suponhamos que $f : A \to A$ seja injetora. Então, como A é finito temos que existe uma bijeção $g : \mathbb{N}_k \to A$. Logo, $h = g^{-1} \circ f \circ g : \mathbb{N}_k \to \mathbb{N}_k$ é injetora. Assim, pelo Lema 3.19, h é bijetora. Portanto, $f = g \circ h \circ g^{-1}$ é sobrejetora.

Reciprocamente, suponhamos que $f : A \to A$ seja sobrejetora. Então existe uma função $g : A \to A$ tal que $f \circ g = I_A$. além disso, g é injetora, assim, pelo o mesmo argumento anterior, g é bijetora. Portanto, $f = g^{-1}$ é injetora. ■

Definição 3.28 *Um conjunto A é* enumerável *quando existe uma correspodência biunívoca de $\mathbb{N}$ sobre A. Um conjunto A é* contável *quando é finito ou enumerável. Caso contrário, dizemos que A é* não contável *ou* não enumerável.

Observação 3.29 *Uma correspondência biunívoca*

$$f : \mathbb{N} \to A$$

significa que é possível enumerar todos os elementos de A em uma seqüência infinita, de modo que cada elemento de A apareça exatamente uma vez. Assim, fazendo

$$f(1) = x_1, \ldots, f(k) = x_k, \ldots$$

temos que

$$A = \{x_1, \ldots, x_k, \ldots\}.$$

Exemplo 3.30 *O conjunto* $\mathbb{Z}$ *é enumerável.*

Solução. Seja

$$f : \mathbb{N} \to \mathbb{Z} \text{ dada por } f(k) = (-1)^k \lfloor \frac{k}{2} \rfloor,$$

onde $\lfloor \cdot \rfloor$ é a função maior inteiro. Dados $k, l \in \mathbb{N}$.

$$f(k) = f(l) \Rightarrow (-1)^k \lfloor \frac{k}{2} \rfloor = (-1)^l \lfloor \frac{l}{2} \rfloor.$$

Assim, ou k e l são ambos pares ou ambos ímpares. Se $k = 2m$ e $l = 2n$, então

$$(-1)^k \lfloor \frac{k}{2} \rfloor = (-1)^l \lfloor \frac{l}{2} \rfloor \Rightarrow \lfloor m \rfloor = \lfloor n \rfloor \Rightarrow m = n \Rightarrow k = l.$$

Se $k = 2m + 1$ e $l = 2n + 1$, então

$$(-1)^k \lfloor \frac{k}{2} \rfloor = (-1)^l \lfloor \frac{l}{2} \rfloor \Rightarrow \lfloor m + \frac{1}{2} \rfloor = \lfloor n + \frac{1}{2} \rfloor \Rightarrow m = n \Rightarrow k = l.$$

Logo, f é injetora. Dado $n \in \mathbb{Z}$. Então $n > 0$ ou $n \leq 0$. Se $n > 0$, então existe $k = 2n \in \mathbb{N}$ tal que $f(k) = n$. Se $n \leq 0$, então existe $k = 2\,|n| + 1 \in \mathbb{N}$ tal que $f(k) = n$. Logo, f é sobrejetora. Portanto, f é uma correspondência biunívoca de $\mathbb{N}$ sobre $\mathbb{Z}$.

Teorema 3.31 *Se* A *é enumerável e* $x \in A$*, então* $A - \{x\}$ *é enumerável.*

Prova. Suponhamos que A seja enumerável. Então existe uma bijeção

$$f : \mathbb{N} \to A.$$

Como f é sobrejetora temos que existe $n \in \mathbb{N}$ tal que $x = f(n)$. Seja

$$g : \mathbb{N} \to A - \{x\} \text{ dada por } g(k) = \begin{cases} f(k), & \text{se } k < n \\ f(k+1), & \text{se } k \geq n. \end{cases}$$

Então g é uma bijeção (prove isto!). Portanto, $A - \{x\}$ é enumerável. ■

Corolário 3.32 *Para cada* $k \in \mathbb{N}$*,* $\mathbb{N}_k$ *não contém subconjunto enumerável.*

Prova. Vamos usar indução sobre k.

1. Se $k = 1$, nada há para provar.

2. Suponhamos, como hipótese de indução, que o resultado seja válido para algum $k > 1$.

Agora, suponhamos, por absurdo, que $\mathbb{N}_{k+1}$ contenha um subconjunto enumerável X. Assim, se $k + 1 \notin X$, então $X \subseteq \mathbb{N}_k$, o que é uma contradição. Se $k + 1 \in X$, então $X - \{k+1\} \subseteq \mathbb{N}_k$ e $X - \{k+1\}$ é enumerável, o que é uma contradição. Portanto, $\mathbb{N}_{k+1}$ não contém subconjunto enumerável. ■

Teorema 3.33 *O conjunto A é infinito se, e somente se, A contém um subconjunto enumerável.*

Prova. Suponhamos que A seja infinito. Assim, basta mostrar que

$$f : \mathbb{N} \to A$$

é injetora, pois $f(\mathbb{N})$ é um subconjunto enuméravel de A (prove isto!). Dado $x_1 \in A$. Seja

$$X = \{k \in \mathbb{N} : f(k) = x_k \text{ e } x_k \in A - \{x_1, \ldots, x_{k-1}\}\} \subseteq \mathbb{N}.$$

Então:

1. $1 \in X$, pois $f(1) = x_1$ e $x_1 \in A$.
2. Suponhamos, como hipótese de indução, que o resultado seja válido para algum $k > 1$, isto é, $k \in X$.

Como A é um conjunto infinito,

$$A - \{x_1, \ldots, x_k\}$$

nunca pode ser vazio. assim, podemos sempre escolher

$$x_{k+1} \in A - \{x_1, \ldots, x_k\}$$

e definir $f(k+1) = x_{k+1}$. ou seja, $k+1 \in X$. Portanto, $X = \mathbb{N}$.

Note que f assim definida é injetora, pois dados $k, l \in \mathbb{N}$, $k \neq l$, digamos $k < l$, então

$$f(l) \in A - \{x_1, \ldots, x_{l-1}\} \text{ e } f(k) \in \{x_1, \ldots x_k, \ldots, x_{l-1}\}.$$

Portanto, $f(k) \neq f(l)$.

Reciprocamente, suponhamos que A contenha um subconjunto enumerável B e que A seja finito. Então existem bijeções

$$f : \mathbb{N} \to B \text{ e } g : \mathbb{N}_k \to A,$$

respectivamente. Logo, $h = g^{-1} \circ i \circ f$ é uma função injetora de $\mathbb{N}$ em $\mathbb{N}_k$, o que é, pelo Corolário 3.32, uma contradição. ■

Corolário 3.34 *Qualquer conjunto que contém um subconjunto infinito é infinito.* ■

Corolário 3.35 *Qualquer subconjunto de um conjunto finito é finito.* ■

Corolário 3.36 *Se A é infinito e B é não-vazio, então $A \times B$ e $B \times A$ são infinitos.*

Prova. Seja $b \in B$ fixado. Então

$$g : A \to A \times B \text{ dada por } g(x) = (x, b)$$

é claramente injetora. Assim, se $f : \mathbb{N} \to A$ é uma função injetora, então

$$g \circ f : \mathbb{N} \to A \times B$$

é injetora. Logo, $A \times B$ contém um subconjunto enumerável. Portanto, $A \times B$ é infinito. ■

Teorema 3.37 *O conjunto A é infinito se, e somente se, existe uma bijeção de A com um subconjunto próprio de A.*

Prova. Suponhamos que A seja infinito. Então A contém um subconjunto enumerável, digamos

$$B = \{x_1, \ldots, x_k, \ldots\}.$$

Seja

$$f : A \to A - \{x_1\} \text{ dada por } f(x) = \begin{cases} x, & \text{se } x \in A - B \\ x_{k+1}, & \text{se } x = x_k, \forall\ k \in \mathbb{N}. \end{cases}$$

Então f é uma função bijetora (prove isto!).

Reciprocamente, suponhamos que A seja finito. Então existe uma bijeção

$$g : \mathbb{N}_k \to A.$$

Assim, pelo Teorema 3.18, não existe uma bijeção de A com um subconjunto próprio de A. ■

Teorema 3.38 *Qualquer subconjunto de $\mathbb{N}$ é contável.*

Prova. Seja B um subconjunto qualquer de $\mathbb{N}$. Se $B = \emptyset$, então B é claramente finito. Suponhamos que $B \neq \emptyset$. Como $B \neq \emptyset$ e $B \subseteq \mathbb{N}$ temos, pelo Axioma 3.9, que existe $x_1 \in B$ tal que $x_1 \leq x$, $\forall\ x \in B$. Suponhamos, como hipótese de indução, que existam

$$x_1, x_2, \ldots, x_k \in B \text{ tais que } x_1 < x_2 < \cdots < x_k.$$

Seja

$$X = \{x \in B : x \notin \{x_1, x_2, \ldots, x_k\}\}.$$

Então, se $X = \emptyset$ temos que B é finito. Se $X \neq \emptyset$, então existe, pelo Axioma 3.9, $x_0 \in X$ tal que $x_0 \leq x$, para todo $x \in X$. É claro que $x_i < x_0$. Assim, tomando $x_{k+1} = x_0$, obtemos

$$x_1, x_2, \ldots, x_k, x_{k+1}, \ldots \in B \text{ tais que } x_1 < x_2 < \cdots < x_k < x_{k+1} < \cdots$$

Seja

$$f : \mathbb{N} \to B \text{ dada por } f(k) = x_k.$$

Então f é uma bijeção (prove isto!). Portanto, B é enumerável. ■

Teorema 3.39 *O produto cartesiano* $\mathbb{N} \times \mathbb{N}$ *é enumerável.*

Prova. Seja

$$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \text{ definida por } f((k,l)) = k + \frac{1}{2}(k+l-1)(k+l-2).$$

Então, dado $n \in \mathbb{N}$, escolhendo $m \in \mathbb{N}$ tal que

$$\frac{(m-1)m}{2} < n \leq \frac{m(m+1)}{2},$$

obtemos

$$k = n - \frac{(m-1)m}{2} \in \mathbb{N} \text{ e } l = 1 - n + \frac{m(m+1)}{2} \in \mathbb{N}.$$

Assim, dado $n \in \mathbb{N}$ existe $(k,l) \in \mathbb{N} \times \mathbb{N}$ tal que $f((k,l)) = n$. Logo, f é sobrejetora.

Dados $(k,l),(m,n) \in \mathbb{N} \times \mathbb{N}$, se $(k,l) \neq (m,n)$, então há dois casos a ser considerado:

1.º **Caso**. Se $k+l = m+n$ e $k < m$, então $f((k,l)) < f((m,n))$.

2.º **Caso**. Se $k+l < m+n$, então $k+l \geq 2$ e $m+n \geq 3$. Note, pelo primeiro caso, que

$$f((k,l)) \leq f((k+l-1,1)) \text{ e } f((1,m+n-1)) \leq f((m,n)).$$

Assim, basta mostrar que

$$f((k+l-1,1)) \neq f((1,m+n-1)).$$

Pelo Teorema 3.11 temos que $k+l \leq m+n-1$. Assim,

$$(k+l-1)(k+l) \leq (m+n-2)(m+n-1)$$

e

$$(k+l-1)(k+l) - (m+n-2)(m+n-1) < 2.$$

Logo,

$$(k+l-1) + \frac{1}{2}(k+l-1)(k+l-2) < 1 + \frac{1}{2}(m+n-1)(m+n-2),$$

isto é,

$$f((k+l-1,1)) < f((1,m+n-1)).$$

Portanto, em qualquer caso, $f((k,l)) \neq f((m,n))$, isto é, f é injetora. ■

Teorema 3.40 *Seja* $\{A_n\}_{n=1}^{\infty}$ *uma família indexada de conjuntos enumeráveis. Então*

$$A = \bigcup_{n=1}^{\infty} A_n$$

é enumerável.

Prova. Como os A_n são enumeráveis existem bijeções

$$f_n : \mathbb{N} \to A_n$$

para cada $n \in \mathbb{N}$. Seja

$$f : \mathbb{N} \times \mathbb{N} \to A \text{ dada por } f((m,n)) = f_n(m).$$

Então f é sobrejetora, pois dado $y \in A$ existe $n \in \mathbb{N}$ tal que $y \in A_n$. assim, existe $m \in \mathbb{N}$ tal que $y = f_n(m)$, isto é, existe $(m,n) \in \mathbb{N} \times \mathbb{N}$ tal que $y = f((m,n))$. Pelo Teorema 3.39, existe uma bijeção

$$g : \mathbb{N} \to \mathbb{N} \times \mathbb{N},$$

logo

$$f \circ g : \mathbb{N} \to A$$

é sobrejetora. Para $k, l \in \mathbb{N}$, definimos

$$k \sim l \Leftrightarrow f \circ g(k) = f \circ g(l).$$

Então $\sim$ é uma relação de equivalência em $\mathbb{N}$ associada a $f \circ g$ (prove isto!). Logo,

$$h : \frac{\mathbb{N}}{\sim} \to A, \text{ definida por } h(\overline{k}) = f \circ g(k)$$

é uma função bijetora. Pelo Teorema 3.38, $\frac{\mathbb{N}}{\sim}$ é contável. assim, A é contável. Mas, pelo Corolário 3.34, A é infinito. Portanto, A é enumerável. ■

Corolário 3.41 *Seja $\{A_n\}_{n=1}^{\infty}$ uma família indexada de conjuntos contáveis. Então*

$$A = \bigcup_{n=1}^{\infty} A_n$$

é contável. ■

Corolário 3.42 *Sejam A e B dois conjuntos enumeráveis. Então $A \cup B$ é enumerável.*

Prova. Podemos supor, sem perda de generalidade, que A e B sejam disjuntos, pois existem correspondências biunívocas de A sobre $A \times \{1\}$ e de B sobre $B \times \{2\}$ com

$$A \times \{1\} \cap B \times \{2\} = \emptyset.$$

Seja $\{X_1, X_2\}$ uma partição de $\mathbb{N}$, por exemplo,

$$X_1 = \{2, 4, 6, \ldots\} \text{ e } X_2 = \{1, 3, 5, \ldots\}.$$

Assim, existem bijeções

$$f_1 : X_1 \to A \text{ e } f_2 : X_2 \to B.$$

Logo, $f : \mathbb{N} \to A \cup B$ definida por

$$f(n) = \begin{cases} f_1(n), & \text{se } n \in X_1 \\ f_2(n), & \text{se } n \in X_2 \end{cases}$$

é sobrejetora. Portanto, pela prova do Teorema 3.40, $A \cup B$ é enumerável. ■

Exemplo 3.43 *O conjunto* $\mathbb{Q}$ *é enumerável.*

Solução. Basta mostrar que $\mathbb{Q}_+^*$ é enumerável, pois

$$\mathbb{Q} = \mathbb{Q}_-^* \cup \{0\} \cup \mathbb{Q}_+^*.$$

Seja

$$f : \mathbb{N} \times \mathbb{N} \to \mathbb{Q}_+^*, \text{ dada por } f((m,n)) = \frac{m}{n}.$$

Dados $(k,l),(m,n) \in \mathbb{N} \times \mathbb{N}$,

$$(k,l) = (m,n) \Rightarrow k = m \text{ e } l = n \Rightarrow \frac{k}{l} = \frac{m}{n} \Rightarrow f((k,l)) = f((m,n)).$$

Logo, f é bem definida. Finalmente, dado $r = \frac{m}{n} \in \mathbb{Q}_+^*$, existe $(m,n) \in \mathbb{N} \times \mathbb{N}$ tal que

$$f((m,n)) = r.$$

Portanto, f é sobrejetora. Assim, pela prova do Teorema 3.40, $\mathbb{Q}_+^*$ é enumerável.

Teorema 3.44 *O conjunto* $\mathbb{R}$ *é não enumerável.*

Prova. Como

$$f : \mathbb{R} \to]0,1[\text{ definida por } f(x) = \frac{e^x}{1+e^x}$$

é uma função bijetora (prove isto!), basta mostrar que o intervalo aberto $]0,1[$ é não enumerável. Suponhamos, por absurdo, que $]0,1[$ seja enumerável, isto é,

$$]0,1[\ = \{x_1, x_2, \ldots, x_k, \ldots\}.$$

Vamos admitir como sendo conhecido o seguinte fato (cf. Apêndice): todo $x \in]0,1[$ admite uma representação decimal da forma

$$x = 0, a_1 a_2 a_3 \cdots,$$

onde $a_i \in \mathbb{N}_9 \cup \{0\}$. É claro que todo número racional admite duas representações desta forma, por exemplo,

$$\frac{1}{5} = 0,200\cdots \text{ e } \frac{1}{5} = 0,199\cdots$$

Assim,

$$\begin{array}{rcc} x_1 & = & 0, a_{11}a_{12}a_{13}\cdots \\ x_2 & = & 0, a_{21}a_{22}a_{23}\cdots \\ \vdots & \vdots & \vdots \\ x_k & = & 0, a_{k1}a_{k2}a_{k3}\cdots \\ \vdots & \vdots & \vdots \end{array}$$

Seja agora

$$b_i \in \mathbb{N}_9 \cup \{0\} \text{ e } b_i \neq a_{ii}.$$

Então

$$b = 0, b_1 b_2 b_3 \cdots \in]0,1[,$$

o que é uma contradição, pois $b \neq x_k, \forall\ k \in \mathbb{N}$. ■

EXERCÍCIOS

1. Mostrar que existe $f : \mathbb{N}_k \to \mathbb{N}_l$ é injetora se, e somente se, $k \leq l$. (Sugestão: Suponha que exista uma função injetora $f : \mathbb{N}_k \to \mathbb{N}_l$. Agora, vamos usar indução sobre l.

   (a) Se $l = 1$, nada há para provar.

   (b) Suponhamos, como hipótese de indução, que o resultado seja válido para $l-1$. Dado $y \in \mathbb{N}_l$. Há dois casos a ser considerado: (1) Se $y \in f(\mathbb{N}_k)$, então existe um único $x \in \mathbb{N}_k$ tal que $y = f(x)$, pois f é injetora. Sejam $A = \mathbb{N}_k - \{x\}$ e $B = \mathbb{N}_l - \{y\}$. Então, $g : A \to B$ dada por $g = f\mid_A$ é injetora. Como $\#(B) = l-1$ temos, pela hipotese de indução, que $\#(A) = k-1 \leq \#(B) = l-1$, isto é, $k \leq l$. (2) Se $y \notin f(\mathbb{N}_k)$, então $f(\mathbb{N}_k) \subseteq B$. Logo, $f : \mathbb{N}_k \to B$ é injetora. Como $\#(B) = l-1$ temos, pela hipotese de indução, que $k \leq l-1$, isto é, $k < l$.)

2. Mostrar que existe $f : \mathbb{N}_k \to \mathbb{N}_l$ é sobrejetora se, e somente se, $k \geq l$. (Sugestão: Suponha que exista uma função sobrejetora $f : \mathbb{N}_k \to \mathbb{N}_l$. Seja

   $$r_i = \#(\{x \in \mathbb{N}_k : f(x) = y_i \text{ com } y_i \in \mathbb{N}_l\})$$

   Então, por hipótese, $r_i \geq 1$. Como cada x está associado a um único y_i temos que

   $$k = \sum_{i=1}^{l} r_i \geq \sum_{i=1}^{l} 1 = l.)$$

3. Seja A um conjunto finito. Mostrar que $\mathcal{P}(A)$ é um conjunto finito.

4. Seja A um conjunto finito. Mostrar que o número de relações em A é finito.

5. Seja A qualquer conjunto contendo pelo menos dois elementos. Mostrar que o conjunto $\mathcal{P}(A)$, munido com a ordem parcial

   $$X \preceq Y \Leftrightarrow X \subseteq Y, \forall\ X, Y \in \mathcal{P}(A),$$

   não é bem ordenado.

6. Mostrar que $f : \mathbb{N}_k \times \mathbb{N}_l \to \mathbb{N}_{kl}$ definida por $f((i,j)) = l(i-1) + j$ é uma correspondência biunívoca.

7. Sejam A e B dois conjuntos finitos. Mostrar que $\#(A \times B) = \#(A) \cdot \#(B)$.

8. Seja A um conjunto finito com $\#(A) = k$. Mostrar que:

   (a) Existem 2^{k^2} relações em A. (Sugestão: O núnero total de relações é o número de subconjuntos de um conjunto com k^2 elementos. Continue.)

(b) Existem 2^{k^2-k} relações reflexivas em A.

(c) Existem $2^{\frac{k^2+k}{2}}$ relações simétricas em A.

(d) Existem $2^{\frac{k^2-k}{2}}$ relações reflexivas e simétricas em A.

9. Se a seqüência $x_1, x_2, \ldots, x_n, \ldots$ forma uma P.A. de razão r. Mostrar que

$$x_n = x_1 + (n-1)r.$$

10. Seja $S_n = x_1 + x_2 + \cdots + x_n$ a soma dos n primeiros termos de uma P.A. de razão r. Mostrar que

$$S_n = \frac{n(x_1 + x_n)}{2}.$$

11. Se a seqüência $x_1, x_2, \ldots, x_n, \ldots$ forma uma P.G. de razão q. Mostrar que

$$x_n = x_1 q^{n-1}.$$

12. Seja $S_n = x_1 + x_2 + \cdots + x_n$ a soma dos n primeiros termos de uma P.G. de razão $q \notin \{0, 1\}$. Mostrar que

$$S_n = \frac{x_1 - x_n q}{1 - q}.$$

13. Seja a seqüência $x_1, x_2, \ldots, x_n, \ldots$ com $x_1 = 7$ e

$$x_n = x_{n-1} + 2x_{n-2} + \cdots + (n-1)x_1.$$

Mostrar que x_n é um múltiplo de 7.

14. Seja a seqüência $a_1 = 1$, $a_2 = 2$ e

$$a_{n+2} = \frac{a_{n+1} + a_n}{2},$$

para todo $n \in \mathbb{N}$. Mostrar que

$$1 \leq a_n \leq 2, \forall\ n \in \mathbb{N}.$$

15. Mostrar que se A é um conjunto finito e b não pertence a A, então $A \cup \{b\}$ é finito.

16. Mostrar que se A é um conjunto infinito e B é um subconjunto finito de A, então $A - B$ é infinito.

17. Seja $a \in A$. Mostrar que A é um conjunto infinito se, e somente se, existe uma correspondência biunívoca de $A - \{a\}$ sobre A. (Sugestão: Como $A - \{a\}$ é infinito, existe $B \subseteq A - \{a\}$ enumerável. Logo, $B \cup \{a\}$ é enumerável e existe uma bijeção de B sobre $B \cup \{a\}$, digamos $f : B \to B \cup \{a\}$. Agora, mostrar que a função $g : A - \{a\} \to A$ definida por

$$g(x) = \begin{cases} f(x), & \text{se } x \in B \\ x, & \text{se } x \notin B \cup \{a\} \end{cases}$$

é bijetora.)

18. Mostrar que se A é um conjunto infinito e B é um conjunto contável, então existe uma correspondência biunívoca de A sobre $A \cup B$. (Sugestão: Como A é infinito, existe $C \subseteq A$ enumerável. Logo, $C \cup (B - A)$ é enumerável e existe uma bijeção de C sobre $C \cup (B - A)$, continue.)

19. Seja $A \subseteq \mathbb{N}$ um subconjunto infinito. Mostrar que existe uma única bijeção crescente $f : \mathbb{N} \to A$.

20. Mostrar que A é um conjunto infinito se, e somente se, existem uma quantidade infinita de relações de equivalência em A. (Sugestão: Sejam $a, b \in A$ com $a \neq b$. Mostre que

$$\mathcal{R}_{ab} = \{(x, y) \in A^2 : x = y, (x, y) = (a, b) \text{ ou } (x, y) = (b, a)\}$$

é uma relação de equivalência em A e $\mathcal{R}_{ab} = \mathcal{R}_{cd} \Leftrightarrow \{a, b\} = \{c, d\}$.)

21. Mostrar que $f : \mathbb{N} \to \mathbb{Z}$ definida por

$$f(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ é par} \\ \frac{1-n}{2} & \text{se } n \text{ é ímpar} \end{cases}$$

é uma correspondência biunívoca. Conclua novamente que $\mathbb{Z}$ é enumerável.

22. Mostrar que o conjunto de todos os múltiplos inteiros de 5 é enumerável.

23. Mostrar que todo subconjunto de um conjunto enumerável é contável.

24. Seja A um conjunto enumerável. Mostrar que A possui um subconjunto enumerável B tal que $A - B$ é enumerável.

25. Mostrar que o conjunto de decimais terminando em uma seqüência infinita que consiste exclusivamente em 9's é enumerável. (Sugestão: Por exemplo,

$$0, x_1 \cdots x_k 999 \cdots = \frac{x_1}{10} + \cdots + \frac{x_k}{10^k} + \sum_{n=k+1}^{\infty} \frac{9}{10^n},$$

onde $x_i \in \mathbb{N}_9 \cup \{0\}$.)

26. Seja $J = \{J_i\}_{i \in I}$ uma família indexada de intervalos disjuntos aos pares. Mostrar que J é contável.

27. Mostrar que o conjunto de pontos no plano com coordenadas racionais é enumerável.

28. Seja $f : A \to B$ uma função injetora. Mostrar que se B é enumerável, então A também o é.

29. Seja $f : A \to B$ uma função sobrejetora. Mostrar que se A é enumerável, então B contável. (Sugestão: Dado $y \in B$, existe $x_y \in A$ tal que $f(x_y) = y$. Agora, mostre que a função $g : B \to A$ definida por $g(y) = x_y$ é injetora, continue.)

30. Sejam $A_1, \ldots, A_k$ conjuntos enumeráveis. Mostrar que $A_1 \times \cdots \times A_k$ é enumerável.

31. Mostrar que a função

$$f : \mathbb{Z} \times \mathbb{N} \to \mathbb{Q}, \text{ definida por } f((m,n)) = \frac{m}{n}$$

é sobrejetora. Conclua novamente que $\mathbb{Q}$ é enumerável.

32. Seja

$$A = \{X \subseteq \mathbb{N} : X \text{ é um conjunto finito}\}.$$

Mostrar que A é um conjunto enumerável. (Sugestão: Seja

$$A_n = \{X \subseteq \mathbb{N} : \#(X) = n\}.$$

Então

$$A = \dot{\bigcup_{n\in\mathbb{N}}} A_n.$$

Agora, mostre que a função $g : A_n \to \mathbb{N}^n$ definida por $g(X) = (x_1, \ldots, x_n)$ é injetora, onde

$$X = \{x_1, \ldots, x_n\},$$

continue.)

33. Seja A um conjunto enumerável. Mostrar que

$$B = \{X \subseteq A : X \text{ é um conjunto finito}\}$$

é um conjunto enumerável.

34. Mostrar que o corpo $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ é enumerável.

35. Mostrar que o anel dos inteiros de Gauss $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, onde $i^2 = -1$, é enumerável.

36. Seja A um conjunto infinito. Mostrar que A é enumerável se, e somente se, existe uma correspondência biunívoca de A sobre B, para todo subconjunto infinito $B \subseteq A$.

37. Sejam A um conjunto finito não-vazio e B um conjunto enumerável. Mostrar que $A \times B$ é enumerável.

38. Mostrar $\mathcal{F} = \{f : \mathbb{N} \to \{0,1\} : f \text{ é uma função}\}$ é não enumerável. Conclua que $\mathcal{P}(\mathbb{N})$ é não enumerável. (Sugestão: Suponha, por absurdo, que $\mathcal{F}$ seja enumerável, digamos

$$\mathcal{F} = \{f_1, f_2, \ldots, f_n, \ldots\}.$$

Consideremos a função $f : \mathbb{N} \to \{0,1\}$ definida por $f(n) = 1 - f_n(n)$. É fácil verificar que $f \neq f_n, \forall\ n \in \mathbb{N}$, o que é uma contradição, pois $f \in \mathcal{F}$.)

39. Seja A qualquer conjunto contendo mais do que um elemento. Mostrar $\mathcal{F} = \{f : \mathbb{N} \to A : f \text{ é uma função}\}$ é não enumerável.

40. Seja A um conjunto enumerável. Mostrar que $\prod_{n=1}^{\infty} A$ é não enumerável.

41. Seja A qualquer conjunto contendo pelo menos dois elementos. Mostrar que não existe bijeção de A sobre $\mathcal{F} = \{f : A \to A : f \text{ é uma função}\}$.

42. Mostrar que o anel $\mathbb{Z}[x]$ de todos os polinômios com coeficientes inteiros é enumerável. (Sugestão: Seja

$$P_{m,n} = \{f \in \mathbb{Z}[x] : f = \sum_{i=0}^{n} a_i x^i \text{ e } \mid a_0 \mid + \mid a_1 \mid + \cdots + \mid a_n \mid = m\}.$$

Então note que cada $P_{m,n}$ é um conjunto finito e

$$\mathbb{Z}[x] = \bigcup_{(m,n)\in\mathbb{N}\times\mathbb{N}} P_{m,n}.)$$

43. Um *número algébrico* é qualquer raiz real da equação

$$a_0 + a_1 x + \cdots + a_n x^n = 0,$$

onde os coeficientes a_i são inteiros. Mostrar que o conjunto A dos números algébricos é enumerável. (Sugestão: Defina para cada $n \in \mathbb{N}$ o conjunto

$$A_n = \{\alpha \in \mathbb{R} : f_n(\alpha) = 0\}.$$

Agora, note que cada A_n é finito e

$$A = \bigcup_{n\in\mathbb{N}} A_n.)$$

44. Um número real é chamado *transcendente* se ele não é algébrico. Mostre que o conjunto dos números transcendentes é não enumerável.

45. Sejam A um conjunto não enumerável. Mostrar que $A \times B$ é não enumerável qualquer que seja o conjunto $B \neq \emptyset$.

46. Mostrar que $f : [0,1] \to]0,1[$ definida por

$$f(x) = \begin{cases} \frac{1}{2}, & \text{se } x = 0 \\ \frac{1}{n+2}, & \text{se } x = \frac{1}{n}, n \in \mathbb{N} \\ x, & \text{se } x \notin \{0, \frac{1}{n}\}, n \in \mathbb{N}, \end{cases}$$

é uma correspondência biunívoca. Conclua que $[0,1]$ é não enumerável.

47. Mostrar que existe uma correspondência biunívoca entre $[0,1]$ e $[0,1[$.

48. Mostrar que $\mathbf{S}^1 = \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ é não enumerável.

Capítulo 4

A origem das frações

O método tradicional de descrever o conjunto $\mathbb{N}$ dos números naturais axiomaticamente é por meio dos seguintes axiomas de Peano:

1. $1 \in \mathbb{N}$.
2. Para cada $n \in \mathbb{N}$ existe um único $n' \in \mathbb{N}$, chamado o *sucessor* de n, isto é, existe uma função $s : \mathbb{N} \to \mathbb{N}$ definida pela regra $s(n) = n'$, chamada *função sucessor*.
3. $s(n) \neq 1$, para todo $n \in \mathbb{N}$.
4. s é injetora, isto é, se $s(m) = s(n)$, então $m = n$, para todos $m, n \in \mathbb{N}$.
5. Seja X um subconjunto de $\mathbb{N}$ tal que

   (a) $1 \in X$.

   (b) $n \in X \Rightarrow s(n) \in X$.

   Então $X = \mathbb{N}$.

O quinto axioma é conhecido como o axioma de indução ou o primeiro princípio de indução e é a base da prova de vários teoremas em matemática.

Escreveremos $s(1) = 2$, $s(2) = 3$, $s(3) = 4$ e, assim por diante.

Podemos re-afirmar o primeiro princípio de indução como segue:

5' Suponhamos que a cada $n \in \mathbb{N}$ temos associado uma proposição $P(n)$ tal que

   (a) $P(1)$ é verdadeira.

   (b) $P(n)$ sendo verdadeira implica que $P(s(n))$ também seja verdadeira.

   Então $P(n)$ é verdadeira, para todo $n \in \mathbb{N}$.

Proposição 4.1 *$s(a) \neq a$, para todo $a \in \mathbb{N}$.*

Prova. Seja

$$X = \{n \in \mathbb{N} : s(n) \neq n\}.$$

Então:

1. Pelos axiomas (1) e (3), $1 \in X$.

2. Suponhamos que $n \in X$, isto é, $s(n) \neq n$. Então, pelo axioma (4), $s(s(n)) \neq s(n)$. Logo, $s(n) \in X$.

Portanto, pelo axioma (5), $X = \mathbb{N}$. ■

Proposição 4.2 *Seja $a \in \mathbb{N}$, com $a \neq 1$. Então existe um único $b \in \mathbb{N}$ tal que $s(b) = a$.*

Prova. Seja

$$X = \{n \in \mathbb{N} : n = 1 \text{ ou } n = s(m) \text{ para algum } m \in \mathbb{N}\}.$$

Então:

1. $1 \in X$, por definição de X.

2. Suponhamos que $n \in X$. Então $s(m) = n$, para algum $m \in \mathbb{N}$. Assim, $s(s(m)) = s(n)$. Logo, $s(n) \in X$.

Portanto, pelo axioma (5), $X = \mathbb{N}$. Finalmente, se $s(b) = a$ e $s(c) = a$, então pelo axioma (4), $b = c$. ■

Teorema 4.3 *Existe exatamente uma operação binária $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ satisfazendo as seguintes condições*:

1. $s(m) = m + 1$, $\forall\ m \in \mathbb{N}$.

2. $s(m + n) = m + s(n)$, $\forall\ m, n \in \mathbb{N}$.

Prova. (Existência) Seja

$$\begin{aligned} X \ = \ & \{m \in \mathbb{N} : m + n \text{ possa ser definida para todo } n \in \mathbb{N} \\ & \text{e 1, 2 sejam satisfeitos}\}. \end{aligned}$$

Então:

1. Definindo $s(n) = 1 + n$, para cada $n \in \mathbb{N}$, temos que $s(1) = 1 + 1$ e

$$s(1 + n) = s(s(n)) = 1 + s(n).$$

Logo, $1 \in X$.

2. Suponhamos que $m \in X$. Então $m+n$ é definida para cada $n \in \mathbb{N}$. Agora, definimos

$$s(m+n) = s(m) + n.$$

Então

$$s(s(m)) = s(m+1) = s(m) + 1$$

e

$$\begin{aligned} s(m) + s(n) &= s(m + s(n)) \\ &= s(s(m+n)) \\ &= s(s(m) + n). \end{aligned}$$

Assim, $s(m) \in X$.

Portanto, pelo axioma (5), $X = \mathbb{N}$.

(Unicidade) Suponhamos que $\oplus$ seja outra operação binária em $\mathbb{N}$ satisfazendo (1) e (2). Para cada $m \in \mathbb{N}$ fixado, seja

$$X = \{n \in \mathbb{N} : m + n = m \oplus n\}.$$

Então:

1. $1 \in X$, pois

$$m + 1 = s(m) = m \oplus 1.$$

2. Suponhamos que $n \in X$. Então

$$\begin{aligned} m + s(n) &= s(m+n) \\ &= s(m \oplus n) \\ &= m \oplus s(n). \end{aligned}$$

Assim, $s(n) \in X$. Portanto, pelo axioma (5), $X = \mathbb{N}$. Assim, $+$ e $\oplus$ são as mesmas operações binárias. ■

Teorema 4.4 *A operação binária $+$ em $\mathbb{N}$ satisfaz as seguintes condições*:

1. $(k+m)+n = k+(m+n)$, *para todos* $k, m, n \in \mathbb{N}$.
2. $m+n = n+m$, *para todos* $m, n \in \mathbb{N}$.

Prova. Provaremos apenas o item (1). Para cada $k, m \in \mathbb{N}$ fixados, seja

$$X = \{n \in \mathbb{N} : (k+m)+n = k+(m+n)\}.$$

Então:

1. $1 \in X$, pois

$$\begin{aligned}(k+m)+1 &= s(k+m)\\ &= k+s(m)\\ &= k+(m+1).\end{aligned}$$

2. Suponhamos que $n \in X$. Então

$$\begin{aligned}(k+m)+s(n) &= s[(k+m)+n]\\ &= s[k+(m+n)]\\ &= k+s(m+n)\\ &= k+(m+s(n)).\end{aligned}$$

Assim, $s(n) \in X$. Portanto, pelo axioma (5), $X = \mathbb{N}$. ■

Teorema 4.5 *Sejam $a, b \in \mathbb{N}$. Então exatamente uma das seguintes condições é satisfeita:*

1. *$a = b$.*
2. *$a = b + k$, para algum $k \in \mathbb{N}$.*
3. *$b = a + l$, para algum $l \in \mathbb{N}$.*

Prova. Primeiro provaremos que os itens (1) e (2) não podem ocorrer simultaneamente. Suponhamos, por absurdo, que $a = b$ e $a = b + k$, para algum $k \in \mathbb{N}$. Então $a = a + k$. Seja

$$X = \{n \in \mathbb{N} : n \neq n + k\}.$$

Então:

1. Como $s(n) = n + 1$ e pelo axioma (3), $s(n) \neq 1$, temos que $1 \in X$.
2. Suponhamos que $n \in X$. Então $n \neq n + k$. Suponhamos, por absurdo, que $s(n) = s(n) + k$. Como $s(n) + k = k + s(n)$ temos que $s(n) = s(n + k)$. Assim, pelo axioma (4), $n = n + k$, o que é uma contradição. Logo, $s(n) \neq s(n) + k$ e $s(n) \in X$.

Portanto, pelo axioma (5), $X = \mathbb{N}$. Em particular, $a \neq a+k$. De modo análogo, prova-se que os itens (1) e (3) (2 e 3) não pode ocorrer simultaneamente. Agora provaremos que uma das três afirmações vale.

Sejam $a \in \mathbb{N}$ fixado e

$$X = \{b \in \mathbb{N} : \text{uma das três afirmações vale}\}.$$

Então:

1. Como $a = 1$ ou $a \neq 1$ temos, pela Proposição 4.2, que $s(m) = a$, para algum $m \in \mathbb{N}$. Logo, por definição, $a = m + 1$. Assim, em qualquer caso, $1 \in X$.

2. Suponhamos que $b \in X$. Se $b = a$, então $s(b) = s(a) = a + 1$. Assim, (3) vale e $s(b) \in X$. Se $b = a + l$, para algum $l \in \mathbb{N}$, então $s(b) = s(a + l) = a + s(l)$. Assim, (3) vale novamente e $s(b) \in X$. Se $a = b + k$, para algum $k \in \mathbb{N}$, há dois casos a ser considerado:

   (a) Se $k = 1$, então $a = b + 1 = s(b)$. Assim, (1) vale e $s(b) \in X$.

   (b) Se $k \neq 1$, então, pela Proposição 4.2, $s(m) = k$, para algum $m \in \mathbb{N}$. Assim,

$$\begin{aligned} a &= b + k \\ &= b + s(m) \\ &= b + (m + 1) \\ &= (b + 1) + m \\ &= s(b) + m. \end{aligned}$$

   e $s(b) \in X$. Portanto, pelo axioma (5), $X = \mathbb{N}$. ■

Teorema 4.6 *Sejam $a, b, c \in \mathbb{N}$. Então*:

1. *$a \neq a + c$.*

2. *Se $a + c = b + c$, então $a = b$.*

Prova. Provaremos apenas o item (2). Suponhamos, por absurdo, que $a \neq b$. Então há dois casos a ser considerado:

1.º **Caso**. Se $a = b + k$, para algum $k \in \mathbb{N}$, então

$$\begin{aligned} (a + c) + k &= (b + c) + k \\ &= b + (c + k) \\ &= (b + k) + c \\ &= a + c, \end{aligned}$$

o que contradiz o item (1).

2.º **Caso**. Se $b = a + l$, para algum $l \in \mathbb{N}$, então

$$\begin{aligned} (b + c) + l &= (a + c) + l \\ &= a + (c + l) \\ &= (a + l) + c \\ &= b + c, \end{aligned}$$

o que contradiz o item (1). Portanto, $b = c$. ■

Sejam $a, b \in \mathbb{N}$. Dizemos que b é *maior do que* a, em símbolos $b > a$, se $b = a + l$, para algum $l \in \mathbb{N}$. Dizemos que b é *menor do que* a, em símbolos $b < a$, se $a = b + k$, para algum $k \in \mathbb{N}$. Note que, $a < b$ se, e somente se $b > a$. A notação $a \leq b$, significa que $a = b$ ou $a < b$.

Observação 4.7 *Sejam $a, b, c \in \mathbb{N}$. Então*:

1. *Exatamente uma das seguintes condições é satisfeita*

   (a) $a = b$.

   (b) $a > b$.

   (c) $a < b$.

2. *Se $a < b$ e $b < c$, então $a < c$.*

3. *Se $a < b$, então $a + c < b + c$.*

Corolário 4.8 *Seja $a \in \mathbb{N}$, com $a \neq 1$ Então $a > 1$.*

Prova. Se $a \neq 1$, então, pela Proposição 4.2, $s(m) = a$, para algum $m \in \mathbb{N}$. Assim, $a = 1 + m$. Portanto, $a > 1$. ■

Teorema 4.9 *Sejam $a, b \in \mathbb{N}$. Então $a < b$ se, e somente se, $a + 1 \leq b$.*

Prova. Suponhamos que $a < b$. Então $b = a + l$, para algum $l \in \mathbb{N}$. Se $l = 1$, então $b = a + 1$. Se $l \neq 1$, então, pela Proposição 4.2, $s(m) = l$, para algum $m \in \mathbb{N}$. Assim,

$$\begin{aligned} b &= a + l \\ &= a + s(m) \\ &= a + (m + 1) \\ &= (a + 1) + m. \end{aligned}$$

Logo, $a + 1 < b$. Portanto, em qualquer caso, $a + 1 \leq b$. ■

Teorema 4.10 (Princípio da Boa Ordenação) *Todo subconjunto não-vazio de $\mathbb{N}$ contém um menor elemento.*

Prova. Sejam S um subconjunto arbitrário e não-vazio de $\mathbb{N}$ e

$$X = \{n \in \mathbb{N} : n \leq a, \forall\ a \in S\}.$$

Então, pelo Corolário 4.8, temos que $1 \in X$. Suponhamos que $n \in X$. Como $a < s(a)$, para cada $a \in S$, temos que $s(a) \notin X$. Assim, $X \neq \mathbb{N}$ e pelo axioma (5), existe $b \in X$ tal que $s(b) \notin X$. Vamos provar que $b \in S$, isto é, b é o menor elemento de S. Suponhamos, por absurdo, que $b \notin S$. Então $b < a$, para cada $a \in S$, pois $b \in X$. Logo, pelo Teorema 4.9, $b + 1 \leq a$, para cada $a \in S$. Portanto, $s(b) = b + 1 \in X$, o que é uma contradição. ■

Teorema 4.11 *Existe exatamente uma operação binária* $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *satisfazendo as seguintes condições*:

1. $m \cdot 1 = m$, $\forall\ m \in \mathbb{N}$.
2. $m \cdot s(n) = m \cdot n + m$, $\forall\ m, n \in \mathbb{N}$.

Prova. Exercício. ■

Com o propósito de simplificar, vamos denotar $m \cdot n$ por mn e chamá-lo de *produto* de m por n.

Teorema 4.12 *O produto em* $\mathbb{N}$ *satisfaz as seguintes condições*:

1. $(km)n = k(mn)$, *para todos* $k, m, n \in \mathbb{N}$.
2. $mn = nm$, *para todos* $m, n \in \mathbb{N}$.
3. $k(m+n) = km + kn$, *para todos* $k, m, n \in \mathbb{N}$.
4. $km = kn \Rightarrow m = n$, *para todos* $k, m, n \in \mathbb{N}$.
5. $m < n \Rightarrow km < kn$, *para todos* $k, m, n \in \mathbb{N}$.

Prova. Provaremos apenas o item (3). Para cada $k, m \in \mathbb{N}$ fixados, seja

$$X = \{n \in \mathbb{N} : k(m+n) = km + kn\}.$$

Então:

1. $1 \in X$, pois

$$\begin{aligned} k(m+1) &= ks(m) \\ &= km + k \\ &= km + k \cdot 1. \end{aligned}$$

2. Suponhamos que $n \in X$. Então

$$\begin{aligned} k(m+s(n)) &= k[s(m+n)] \\ &= k(m+n) + k \\ &= (km + kn) + k \\ &= km + (kn + k) \\ &= km + ks(n). \end{aligned}$$

Assim, $s(n) \in X$. Portanto, pelo axioma (5), $X = \mathbb{N}$. ■

Depois de termos dado um desenvolvimento sistemático do conjunto dos números naturais $\mathbb{N}$, agora estendemos esse conjunto para o conjunto $\mathbb{Z}$ dos inteiros. A necessidade de se fazer isto deve-se ao fato de que o conjunto dos números naturais $\mathbb{N}$ originalmente, ele tinha a capacidade de representar "todas" as quantidades e, posteriormente, com o advento das operações elementares, em particular a adição e a multiplicação, foi possível somar e multiplicar dois números quaisquer de $\mathbb{N}$, obtendo-se um número de $\mathbb{N}$, o que em linguagem moderna significa dizer que $\mathbb{N}$ é fechado em relação à soma e à multiplicação. Com a subtração surgiu um problema, que era o da impossibilidade de se subtrair um número do outro quando o primeiro era menor do que o segundo ou de resolver equações do tipo $x + 2 = 0$.

Seja $I = \mathbb{N} \times \mathbb{N}$. Para $(a, b), (c, d) \in I$, definimos

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c.$$

Então $\sim$ é uma relação de equivalência em I (prove isto!).

Vamos equipar $\frac{I}{\sim}$ com as seguintes operações binárias:

1. $\overline{(a, b)} + \overline{(c, d)} = \overline{(a + c, b + d)}$.
2. $\overline{(a, b)} \bullet \overline{(c, d)} = \overline{(ac + bd, ad + bc)}$.

Provaremos apenas que a operação (2) está bem definida, ficando a outra como exercício.

Suponhamos que

$$\overline{(a, b)} = \overline{(x, y)} \text{ e } \overline{(c, d)} = \overline{(z, w)}.$$

Então devemos provar que

$$\overline{(ac + bd, ad + bc)} = \overline{(xz + yw, xw + yz)}.$$

De fato, como

$$\overline{(a, b)} = \overline{(x, y)} \Leftrightarrow a + y = b + x \text{ e } \overline{(c, d)} = \overline{(z, w)} \Leftrightarrow c + w = d + z$$

temos que

$$\begin{aligned} (ac + bd) + (xw + yz) - [(ad + bc) + (xz + yw)] &= \\ a(c - d) + b(d - c) + x(z - w) + y(w - z) &= \\ (a - b)(c - d) - (x - y)(z - w) &= \\ (x - y)(z - w) - (x - y)(z - w) &= 0. \end{aligned}$$

Portanto,

$$(ac + bd) + (xw + yz) = (ad + bc) + (xz + yw),$$

isto é,

$$\overline{(ac + bd, ad + bc)} = \overline{(xz + yw, xw + yz)}.$$

Essas operações satisfazem as seguintes propriedades:

1. $[\overline{(a,b)} + \overline{(c,d)}] + \overline{(e,f)} = \overline{(a,b)} + [\overline{(c,d)} + \overline{(e,f)}]$, pois

$$\begin{aligned}
[\overline{(a,b)} + \overline{(c,d)}] + \overline{(e,f)} &= \overline{[(a+c,b+d)]} + \overline{(e,f)} \\
&= \overline{((a+c)+e,(b+d)+f)} \\
&= \overline{(a+(c+e),b+(d+f))} \\
&= \overline{(a,b)} + \overline{(c+e,d+f)} \\
&= \overline{(a,b)} + [\overline{(c,d)} + \overline{(e,f)}].
\end{aligned}$$

2. Existe único $\overline{(1,1)} \in \frac{I}{\sim}$ tal que $\overline{(a,b)} + \overline{(1,1)} = \overline{(a,b)}$, $\forall\ \overline{(a,b)} \in \frac{I}{\sim}$, pois

$$\overline{(a,b)} + \overline{(1,1)} = \overline{(a+1,b+1)} = \overline{(a,b)}.$$

   Note que, $(a,b) \in \overline{(1,1)}$ se, e somente se, $a+1 = b+1$ se, e somente se, $a = b$. Portanto, $\overline{(a,a)} = \overline{(1,1)}$, para todo $a \in \mathbb{N}$.

3. Para cada $\overline{(a,b)} \in \frac{I}{\sim}$ existe único $\overline{(b,a)} \in \frac{I}{\sim}$ tal que $\overline{(a,b)} + \overline{(b,d)} = \overline{(1,1)}$, pois

$$\overline{(a,b)} + \overline{(b,d)} = \overline{(a+b,a+b)} = \overline{(1,1)}.$$

4. $\overline{(a,b)} + \overline{(c,d)} = \overline{(c,d)} + \overline{(a,b)}$, pois

$$\begin{aligned}
\overline{(a,b)} + \overline{(c,d)} &= \overline{(a+c,b+d)} \\
&= \overline{(c+a,d+b)} \\
&= \overline{(c,d)} + \overline{(a,b)};
\end{aligned}$$

5. $[\overline{(a,b)} \cdot \overline{(c,d)}] \cdot \overline{(e,f)} = \overline{(a,b)} \cdot [\overline{(c,d)} \cdot \overline{(e,f)}]$ (prove isto!).

6. Existe único $\overline{(1+1,1)} \in \frac{I}{\sim}$ tal que $\overline{(a,b)} \cdot \overline{(1+1,1)} = \overline{(a,b)}$, $\forall\ \overline{(a,b)} \in \frac{I}{\sim}$, pois

$$\begin{aligned}
\overline{(a,b)} \cdot \overline{(1+1,1)} &= \overline{(a(1+1)+b,a+b(1+1)} \\
&= \overline{(a+a+b,a+b+b)} \\
&= \overline{(a,b)}.
\end{aligned}$$

   Note que, $(a,b) \in \overline{(1+1,1)}$ se, e somente se, $a+1 = (b+1)+1$ se, e somente se, $a = b+1$. Portanto, $\overline{(b+1,b)} = \overline{(1,1)}$, para todo $b \in \mathbb{N}$.

7. $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(c,d)} \cdot \overline{(a,b)}$ (prove isto!).

8. $\overline{(a,b)} \cdot [\overline{(c,d)} + \overline{(e,f)}] = \overline{(a,b)} \cdot \overline{(c,d)} + \overline{(a,b)} \cdot \overline{(e,f)}]$ (prove isto!).

Denotaremos o conjunto quociente $\frac{I}{\sim}$ por $\mathbb{Z}$ e $\overline{(1,1)}$ por 0. Com o propósito de simplificar, vamos denotar $\overline{(a,b)} \cdot \overline{(c,d)}$ por $\overline{(a,b)(c,d)}$.

Teorema 4.13 *Sejam $x, y \in \mathbb{Z}$. Se $xy = 0$, então $x = 0$ ou $y = 0$.*

Prova. Sejam $x = \overline{(a,b)}$ e $y = \overline{(c,d)}$. Então

$$xy = 0 \Rightarrow (ac + bd) + 1 = (ad + bc) + 1.$$

Suponhamos que $x \neq 0$. Então $a \neq b$. Assim, há dois casos a ser considerado:

1.º **Caso**. Se $a = b + k$, para algum $k \in \mathbb{N}$, então

$$\begin{aligned}(ac + bd) + 1 &= [(b + k)c + bd] + 1 \\ &= [(bc + bd) + 1] + kc\end{aligned}$$

e

$$\begin{aligned}(ad + bc) + 1 &= [(b + k)d + bc] + 1 \\ &= [(bc + bd) + 1] + kd.\end{aligned}$$

Logo,

$$[(bc + bd) + 1] + kc = [(bc + bd) + 1] + kd.$$

Assim, pelo Teorema 4.6, $kc = kd$. Suponhamos, por absurdo, que $c \neq d$. Então $c = d+l$, para algum $l \in \mathbb{N}$ ou $d = c + m$, para algum $m \in \mathbb{N}$. Se $c = d + l$, então

$$\begin{aligned}kd &= kc \\ &= k(d + l) \\ &= kd + kl,\end{aligned}$$

o que contradiz o Teorema 4.6. Se $d = c + m$, então

$$\begin{aligned}kc &= kd \\ &= k(c + m) \\ &= kc + km,\end{aligned}$$

o que contradiz o Teorema 4.6. Logo, $c = d$ e $y = 0$.

2.º **Caso**. Se $b = a + n$, para algum $n \in \mathbb{N}$, então prova-se, de modo análogo que, $y = 0$. Portanto, em qualquer caso, $y = 0$. ■

Teorema 4.14 *Seja $f : \mathbb{N} \to \mathbb{Z}$ uma função definida pela regra $f(a) = \overline{(a + 1, 1)}$. Então f é injetora e*

1. $f(a + b) = f(a) + f(b), \forall\ a, b \in \mathbb{N}$;
2. $f(ab) = f(a)f(b), \forall\ a, b \in \mathbb{N}$.

Prova. Provaremos apenas que f é injetora, e o item (2). Dados $a, b \in \mathbb{N}$,

$$\begin{aligned}f(a) = f(b) &\Rightarrow \overline{(a + 1, 1)} = \overline{(b + 1, 1)} \\ &\Rightarrow (a + 1) + 1 = (b + 1) + 1.\end{aligned}$$

Assim, pelo Teorema 4.6, $a = b$. Portanto, f é injetora. Finalmente,

$$\begin{aligned} f(ab) &= \overline{(ab+1,1)} \\ &= \overline{(ab+1,1)} + \overline{(a+b+1,a+b+1)} \\ &= \overline{(ab+1+a+b+1,1+a+b+1)} \\ &= \overline{((a+1)(b+1)+1,(a+1)+(b+1))} \\ &= \overline{(a+1,1)(b+1,1)} \\ &= f(a)f(b). \end{aligned}$$

■

O Teorema acima permite-nos identificar cada $a \in \mathbb{N}$ com sua imagem $\overline{(a+1,1)}$ em $\mathbb{Z}$. Portanto, denotaremos, com abuso de notação, $\overline{(a+1,1)}$ por a e $\overline{(1,a+1)}$ por $-a$. Além disso,

$$\begin{aligned} \overline{(a,b)} &= \overline{(a+1,1)} + \overline{(1,b+1)} \\ &= a + (-b). \end{aligned}$$

Assim, denotaremos $\overline{(a,b)}$ por $a - b$. Também, a cópia de $\mathbb{N}$ em $\mathbb{Z}$ sob essa imersão é denotada por $\mathbb{Z}_+$, a qual é chamada de *inteiros positivos* de $\mathbb{Z}$. Neste caso, o conjunto

$$\mathbb{Z}_- = \{-n : n \in \mathbb{Z}_+\}$$

é chamado de conjunto dos *inteiros negativos*.

Teorema 4.15 *Seja $x \in \mathbb{Z}$. Então exatamente uma das seguintes condições é satisfeita*:

1. $x = 0$;
2. $x \in \mathbb{Z}_+$;
3. $-x \in \mathbb{Z}_+$.

Prova. Seja $x = \overline{(a,b)} \in \mathbb{Z}$ e $x \neq 0$. Então $a \neq b$. Assim, $a = b + k$, para algum $k \in \mathbb{N}$ ou $b = a + l$, para algum $l \in \mathbb{N}$. Agora, provaremos que

$$a = b + k \Leftrightarrow x \in \mathbb{Z}_+$$

e

$$b = a + l \Leftrightarrow -x \in \mathbb{Z}_+$$

Se $a = b + k$, para algum $k \in \mathbb{N}$, então

$$\begin{aligned} x &= \overline{(a,b)} \\ &= \overline{(b+k,b)} \\ &= \overline{(b+k,b)} + \overline{(1,1)} \\ &= \overline{(b+k+1,b+1)} \\ &= \overline{(b,b)} + \overline{(k+1,1)} \\ &= \overline{(k+1,1)} \in \mathbb{Z}_+. \end{aligned}$$

Reciprocamente, se $x \in \mathbb{Z}_+$, então $x = \overline{(k+1,1)}$, para algum $k \in \mathbb{N}$. Como $x = \overline{(a,b)}$ temos que

$$a + 1 = b + k + 1.$$

Assim, pelo Teorema 4.6, $a = b + k$.

Se $b = a + l$, para algum $l \in \mathbb{N}$, então

$$-x = -\overline{(a,b)} = \overline{(b,a)} = \overline{(a,a+l)} = \overline{(l+1,1)} \in \mathbb{Z}_+.$$

Reciprocamente, se $-x \in \mathbb{Z}_+$, então $-x = \overline{(l+1,1)}$, para algum $l \in \mathbb{N}$. Como $x = \overline{(a,b)}$ temos que $-x = \overline{(b,a)}$. Logo,

$$b + 1 = a + l + 1.$$

Assim, pelo Teorema 4.6, $b = a + l$. ■

Observação 4.16 *Note que o subconjunto $\mathbb{Z}_+$ de $\mathbb{Z}$ goza das seguintes propriedades*:

1. *$x + y \in \mathbb{Z}_+$, para todos $x, y \in \mathbb{Z}_+$.*
2. *$xy \in \mathbb{Z}_+$, para todos $x, y \in \mathbb{Z}_+$.*
3. *Se $x \in \mathbb{Z}$, então exatamente uma das seguintes condições é satisfeita*:
   - *(a) $x = 0$;*
   - *(b) $x \in \mathbb{Z}_+$;*
   - *(c) $-x \in \mathbb{Z}_+$.*

O conjunto $\mathbb{Z}_+$ é chamado o cone positivo *de $\mathbb{Z}$. Neste caso,*

$$\mathbb{Z} = \mathbb{Z}_- \dot{\cup} \{0\} \dot{\cup} \mathbb{Z}_+$$

Sejam $a, b \in \mathbb{Z}$. Dizemos que b é *maior do que* a, em símbolos $b > a$, se $b - a \in \mathbb{Z}_+$. Dizemos que b é *menor do que* a, em símbolos $b < a$, se $a - b \in \mathbb{Z}_+$. Note que, $a < b$ se, e somente se $b > a$. A notação $a \leq b$, significa que $a = b$ ou $a < b$.

Observação 4.17 *Sejam $a, b \in \mathbb{Z}$. Então exatamente uma das seguintes condições é satisfeita*:

1. *$a = b$;*
2. *$a > b$;*
3. *$a < b$.*

Teorema 4.18 *Sejam $a, b, c \in \mathbb{Z}$. Então*:

1. *Se $a < b$ e $b < c$, então $a < c$.*

2. Se $a < b$, então $a + c < b + c$.

3. Se $a < b$ e $0 < c$, então $ac < bc$.

4. Se $a < b$ e $0 > c$, então $ac > bc$.

Prova. Exercício. ■

No conjunto $\mathbb{Z}$ não temos problemas com a subtração, isto é, podemos subtrair um elemento qualquer de outro sem qualquer restrição, mas surge a impossibilidade de se efetuar a divisão de certos números inteiros ou de resolver equações do tipo $2x - 1 = 0$. Para contornarmos esse problema agiremos como acima.

Seja $J = \mathbb{Z} \times \mathbb{Z}$. Para $(a, b), (c, d) \in J$, definimos

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Agora surge um inconveniente, pois $\sim$ não é uma relação de equivalência em J, visto que

$$(2, 1) \sim (0, 0) \text{ e } (0, 0) \sim (3, 1) \text{ mas } (2, 1) \nsim (3, 1).$$

Para contornarmos essa situação consideremos o seguinte subconjunto de J

$$K = \{(a, b) \in J : b \neq 0\} = \mathbb{Z} \times \mathbb{Z}^*,$$

onde $\mathbb{Z}^* = \mathbb{Z} - \{0\}$ e, dizemos que

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Agora $\sim$ é uma relação de equivalência em C (prove isto!).

Vamos equipar $\frac{K}{\sim}$ com as seguintes operações binárias:

1. $\overline{(a, b)} + \overline{(c, d)} = \overline{(ad + bc, bd)}$;
2. $\overline{(a, b)} \bullet \overline{(c, d)} = \overline{(ac, bd)}$.

Provaremos apenas que a operação 1 está bem definida, ficando a outra como exercício.

Suponhamos que

$$\overline{(a, b)} = \overline{(x, y)} \text{ e } \overline{(c, d)} = \overline{(z, w)}.$$

Então devemos provar que

$$\overline{(ad + bc, bd)} = \overline{(xw + yz, yw)}.$$

De fato, como

$$\overline{(a, b)} = \overline{(x, y)} \Leftrightarrow ay = bx \text{ e } \overline{(c, d)} = \overline{(z, w)} \Leftrightarrow cw = dz$$

temos que

$$\begin{aligned}(ad+bc)yw - bd(xw+yz) &= \\ adyw + bcyw - bdxw - bdyz &= \\ bw(dx-cy) - bw(dx-cy) &= 0.\end{aligned}$$

Portanto,

$$(ad+bc)yw = bd(xw+yz),$$

isto é,

$$\overline{(ad+bc,bd)} = \overline{(xw+yz,yw)}.$$

Essas operações satisfazem as seguintes propriedades:

1. $[\overline{(a,b)} + \overline{(c,d)}] + \overline{(e,f)} = \overline{(a,b)} + [\overline{(c,d)} + \overline{(e,f)}]$ (prove isto!).
2. Existe único $\overline{(0,1)} \in \frac{K}{\sim}$ tal que $\overline{(a,b)} + \overline{(0,1)} = \overline{(a,b)}$, $\forall\ \overline{(a,b)} \in \frac{K}{\sim}$ (prove isto!). Note que, $(a,b) \in \overline{(0,1)}$ se, e somente se, $a = 0$. Portanto, $\overline{(0,b)} = \overline{(0,1)}$, para todo $b \in \mathbb{Z}^*$.
3. Para cada $\overline{(a,b)} \in \frac{K}{\sim}$, existe único $\overline{(-a,b)} \in \frac{K}{\sim}$ tal que $\overline{(a,b)} + \overline{(-a,b)} = \overline{(0,1)}$ (prove isto!).
4. $\overline{(a,b)} + \overline{(c,d)} = \overline{(c,d)} + \overline{(a,b)}$ (prove isto!).
5. $[\overline{(a,b)} \cdot \overline{(c,d)}] \cdot \overline{(e,f)} = \overline{(a,b)} \cdot [\overline{(c,d)} \cdot \overline{(e,f)}]$ (prove isto!).
6. Existe único $\overline{(1,1)} \in \frac{K}{\sim}$ tal que $\overline{(a,b)} \cdot \overline{(1,1)} = \overline{(a,b)}$, $\forall\ \overline{(a,b)} \in \frac{K}{\sim}$ (prove isto!). Note que, $(a,b) \in \overline{(1,1)}$ se, e somente se, $a = b$. Portanto, $\overline{(a,a)} = \overline{(1,1)}$, para todo $a \in \mathbb{Z}^*$.
7. $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(c,d)} \cdot \overline{(a,b)}$ (prove isto!).
8. $\overline{(a,b)} \cdot [\overline{(c,d)} + \overline{(e,f)}] = \overline{(a,b)} \cdot \overline{(c,d)} + \overline{(a,b)} \cdot \overline{(e,f)}]$ (prove isto!).
9. Para cada $\overline{(a,b)} \in \frac{K}{\sim} - \{\overline{(0,1)}\}$, existe único $\overline{(b,a)} \in \frac{K}{\sim}$ tal que $\overline{(a,b)} \cdot \overline{(b,a)} = \overline{(1,1)}$, pois
$$\overline{(a,b)} \bullet \overline{(b,a)} = \overline{(ab,ba)} = \overline{(1,1)}.$$

Denotaremos o conjunto quociente $\frac{K}{\sim}$ por $\mathbb{Q}$, $\overline{(0,1)}$ por 0 e $\overline{(1,1)}$ por 1 Com o propósito de simplificar vamos denotar $\overline{(a,b)} \cdot \overline{(c,d)}$ por $\overline{(a,b)(c,d)}$.

Teorema 4.19 *Seja $f : \mathbb{Z} \to \mathbb{Q}$ uma função definida pela regra $f(a) = \overline{(a,1)}$. Então f é injetora e*

1. $f(a+b) = f(a) + f(b), \forall\ a,b \in \mathbb{Z}$;
2. $f(ab) = f(a)f(b), \forall\ a,b \in \mathbb{Z}$.

Prova. Dados $a, b \in \mathbb{Z}$,

$$\begin{aligned} f(a) = f(b) &\Rightarrow \overline{(a,1)} = \overline{(b,1)} \\ &\Rightarrow a = b. \end{aligned}$$

Portanto, f é injetora.

$$\begin{aligned} f(a+b) &= \overline{(a+b,1)} \\ &= \overline{(a,1)} + \overline{(b,1)} \\ &= f(a) + f(b). \end{aligned}$$

Finalmente,

$$\begin{aligned} f(ab) &= \overline{(ab,1)} \\ &= \overline{(a,1)(b,1)} \\ &= f(a)f(b). \end{aligned}$$

■

O Teorema acima permite-nos identificar cada $a \in \mathbb{Z}$ com sua imagem $\overline{(a,1)}$ em $\mathbb{Q}$. Portanto, denotaremos, com abuso de notação, $\overline{(a,1)}$ por a e $\overline{(1,a)}$ por a^{-1}. Além disso,

$$\begin{aligned} \overline{(a,b)} &= \overline{(a,1)} \cdot \overline{(1,b)} \\ &= a \cdot b^{-1}. \end{aligned}$$

Assim, denotaremos $\overline{(a,b)}$ por $ab^{-1} = \frac{a}{b}$. Também,

$$\mathbb{Q}_+ = \left\{ \frac{a}{b} \in \mathbb{Q} : ab \in \mathbb{Z}_+ \right\}.$$

Observação 4.20 *Note que o subconjunto $\mathbb{Q}_+$ de $\mathbb{Q}$ goza das seguintes propriedades*:

1. *$x + y \in \mathbb{Q}_+$, para todos $x, y \in \mathbb{Q}_+$.*
2. *$xy \in \mathbb{Q}_+$, para todos $x, y \in \mathbb{Q}_+$.*
3. *Se $x \in \mathbb{Q}$, então exatamente uma das seguintes condições é satisfeita*:
   - *(a) $x = 0$;*
   - *(b) $x \in \mathbb{Q}_+$;*
   - *(c) $-x \in \mathbb{Q}_+$.*

Neste caso,

$$\mathbb{Q} = \mathbb{Q}_- \dot{\cup} \{0\} \dot{\cup} \mathbb{Q}_+$$

Pela observação, $x < y$ se, e somente se, $y - x \in \mathbb{Q}_+$, para todos $x, y \in \mathbb{Q}$.

Teorema 4.21 *Sejam $x, y \in \mathbb{Q}$. Então exatamente uma das seguintes condições é satisfeita:*

1. $x = y$;
2. $x > y$;
3. $x < y$.

Prova. Exercício. ■

Teorema 4.22 *Sejam $x, y, z \in \mathbb{Q}$. Então:*

1. *Se $x < y$ e $y < z$, então $x < z$;*
2. *Se $x < y$, então $x + z < y + z$;*
3. *Se $x < y$ e $0 < z$, então $xz < yz$;*
4. *Se $x < y$ e $0 > z$, então $xz > yz$;*
5. *Se $x > 0$ e $y < 0$, então $xy < 0$;*
6. *Se $x > 0$, então $x^{-1} > 0$;*
7. *Se $0 < x < y$, então $0 < y^{-1} < x^{-1}$.*

Prova. Provaremos apenas os itens (1), (3) e (7). Se $x < y$ e $y < z$, então $y - x \in \mathbb{Q}_+$ e $z - y \in \mathbb{Q}_+$. Logo,

$$z - x = (z - y) + (y - x) \in \mathbb{Q}_+.$$

Portanto, $x < z$. Para mostrar *3*, se $x < y$ e $0 < z$, então $y - x \in \mathbb{Q}_+$ e $z \in \mathbb{Q}_+$. Logo,

$$yz - xz = (y - x)z \in \mathbb{Q}_+.$$

Portanto, $xz < yz$. Para mostrar *7*, basta notar que

$$x^{-1} - y^{-1} = \frac{1}{x} - \frac{1}{y} = \frac{y - x}{xy} \in \mathbb{Q}_+.$$

■

Parte II

Números e Criptografia

Capítulo 5

Teoria dos Números

A teoria dos números se dedica ao estudo das propriedades dos números inteiros $\mathbb{Z}$. Neste capítulo faremos a apresentação de algumas definições e resultados sobre a teoria dos números que serão necessários para cursos subsequentes. O leitor interessado em mais detalhes pode consultar [16].

5.1 Algoritmo da Divisão

Já sabemos, desde a escola primária, que o processo ordinário de dividir um inteiro positivo a por um inteiro positivo b fornece um quociente q e um resto r. Formalmente, isto corresponde a:

Teorema 5.1 *Sejam $a, b \in \mathbb{Z}$ com $b > 0$. Então existem únicos $q, r \in \mathbb{Z}$ tais que*

$$a = qb + r, \ \ onde \ 0 \leq r < b.$$

Prova. (Existência) Podemos supor, sem perda de generalidade, que $a \geq 0$, pois o caso $a < 0$, reduz-se a esse com a substituição de a por $-a > 0$.

Quando $a = 0$, basta tomar $q = r = 0$. Assim, podemos supor $a \geq 1$ e $a > b$, pois se $a \leq b$, então $a = b$ ou $a < b$, assim, $a = b$ basta tomar $q = 1$ e $r = 0$, e $a < b$ basta tomar $q = 0$ e $r = a$. Agora, seja

$$X = \{a \in \mathbb{N} : a = qb + r, \ \text{onde} \ 0 \leq r < b\}.$$

Então:

1. $1 \in X$, pois $1 = 1.1 + 0$.

2. Suponhamos, como hipótese de indução, que o resultado seja válido para todo k, com $1 \leq k \leq a - 1$, isto é, $\{1, 2, \ldots, a - 1\} \subseteq X$.

Como $a > b > 0$ temos que $0 < a - b < a$ e, assim, existem, pela hipótese de indução, $q_1, r \in \mathbb{Z}$ tais que

$$a - b = q_1 b + r, \text{ onde } 0 \leq r < b.$$

Fazendo, $q = q_1 + 1$, obtemos

$$a = qb + r, \text{ onde } 0 \leq r < b.$$

(Unicidade) Suponhamos que existam $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ tais que

$$a = q_1 b + r_1, \text{ onde } 0 \leq r_1 < b.$$

e

$$a = q_2 b + r_2, \text{ onde } 0 \leq r_2 < b.$$

Logo,

$$q_1 b + r_1 = q_2 b + r_2 \Leftrightarrow (q_1 - q_2)b = r_2 - r_1.$$

Note que

$$0 \leq r_2 < b \text{ e } -b < -r_1 \leq 0 \Rightarrow 0 \leq |r_2 - r_1| < b.$$

Assim,

$$|q_1 - q_2|\, b = |r_2 - r_1| < b \Rightarrow 0 \leq |q_1 - q_2| < 1.$$

Portanto, pelo Teorema 3.11, temos que $|q_1 - q_2| = 0$, isto é, $q_1 = q_2$ e, assim, $r_1 = r_2$. ■

Exemplo 5.2 *Sejam $a = -1.998$ e $b = 7$. Determinar a divisão de a por b.*

Solução.

$$1.998 = 285 \cdot 7 + 3 \Rightarrow -1.998 = (-285)7 + (-3) = (-286)7 + 4.$$

Logo, $q = -286$ e $r = 4$.

Corolário 5.3 (Algoritmo da Divisão) *Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$. Então existem únicos $q, r \in \mathbb{Z}$ tais que*

$$a = qb + r, \text{ onde } 0 \leq r < |b|\,.$$

Prova. É suficiente considerar o caso em que $b < 0$. Então $|b| > 0$ e, pelo Teorema 5.1, existem únicos $q_1, r \in \mathbb{Z}$ tais que

$$a = q_1 |b| + r, \text{ onde } 0 \leq r < |b|\,.$$

Como $|b| = -b$, fazendo, $q = -q_1$, obtemos

$$a = qb + r, \text{ onde } 0 \leq r < |b|\,.$$

■

Exemplo 5.4 *Sejam $a = 2.466$ e $b = -11$. Determinar a divisão de a por b.*

Solução. Como

$$2.466 = 224 \cdot 11 + 2 = (-224)(-11) + 2$$

temos que $q = -224$ e $r = 2$.

Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$, dizemos que b *divide* a ou b é um *divisor* de a ou que a é um *múltiplo* de b, em símbolos $b \mid a$, se existir $c \in \mathbb{Z}$ tal que

$$a = bc.$$

Caso contrário, dizemos que b *não divide* a, e denotaremos por $b \nmid a$. Dizemos que $a \in \mathbb{Z}$ é um número *par* se $2 \mid a$ e *ímpar* se $2 \nmid a$.

Exemplo 5.5 $2 \mid 4$, $-3 \mid 15$, $5 \nmid 12$ *e* $b \mid 0$ *para todo* $b \in \mathbb{Z}^*$, *pois* $0 = 0 \cdot b$.

Observação 5.6 *O inteiro c é único, pois se $c' \in \mathbb{Z}$ é tal que $a = bc'$, então*

$$0 = bc - bc' = b(c - c') \Rightarrow c - c' = 0 \Rightarrow c = c'.$$

Teorema 5.7 *Sejam $a, b, c \in \mathbb{Z}^*$. Então as seguintes condições são satisfeitas*:

1. $\pm 1 \mid a$, $\pm a \mid a$.
2. $b \mid 1 \Leftrightarrow b = \pm 1$.
3. $b \mid a$ *e* $a > 0 \Rightarrow b \leq a$.
4. $b \mid a \Leftrightarrow bc \mid ac$.
5. $b \mid a$ *e* $a \mid c \Rightarrow b \mid c$.
6. $b \mid a$ *e* $a \mid b \Rightarrow a = \pm b$.
7. $c \mid a$ *e* $c \mid b \Rightarrow c \mid (ax + by), \forall x, y \in \mathbb{Z}$.

Prova. Mostraremos apenas os itens (2) e (6). $b \mid 1$ se, e somente se, existe $d \in \mathbb{Z}$ tal que $bd = 1$ se,e somente se, $|bd| = |b|\,|d| = 1$. Como $b, d \in \mathbb{Z}^*$ temos, pelo Teorema 3.11, que $|b| \geq 1$ e $|d| \geq 1$. Assim, se $|b| > 1$, então

$$|bd| = |b|\,|d| > |d| \geq 1,$$

o que é impossível. Logo, $|b| = 1$. Portanto, $b = \pm 1$. Se $b \mid a$ e $a \mid b$, então existem $d, e \in \mathbb{Z}$ tais que $a = bd$ e $b = ae$. Logo,

$$b = ae = bde \Rightarrow de = 1.$$

Por *2*, temos que $d = e = 1$ ou $d = e = -1$. Portanto, $a = \pm b$. ■

Observação 5.8 *A propriedade* (1) *diz que todo* $a \in \mathbb{Z} - \{-1, 0, 1\}$ *possui pelo menos quatro divisores,* (2) *diz que os únicos elementos* invertíveis *de* $\mathbb{Z}$ *são* ± 1*,* (6) *diz que os elementos* a *e* b *são* associados *em* $\mathbb{Z}$*, enquanto* (1) *e* (5) *diz que a relação de divisibilidade em* $\mathbb{Z}$ *é reflexiva e transitiva, entretanto, não é uma relação de equivalência nem de ordem parcial.*

Teorema 5.9 *Seja* $b \in \mathbb{N}$ *com* $b > 1$*. Então para todo* $a \in \mathbb{N}$ *existem únicos* $n, r_i \in \mathbb{Z}$ *tais que*

$$a = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b^1 + r_0 b^0 = (r_n r_{n-1} \cdots r_1 r_0)_b,$$

onde $r_i \in \{0, 1, \ldots, b-1\}$*,* $\forall i = 0, 1, \ldots, n$ *e* $n = \lfloor \log_b a \rfloor$*.*

Prova. (Existência) Seja

$$X = \{a \in \mathbb{N} : a = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b^1 + r_0 b^0\}.$$

Então:

1. $1 \in X$, pois existem $n = 0$ e $r_0 = 1$ tais que $1 = r_0 b^0$.

2. Suponhamos, como hipótese de indução, que o resultado seja válido para todo k, com $1 \leq k \leq a$, isto é, $\{1, 2, \ldots a\} \subseteq X$. Pelo Teorema 5.1, existem $q, r_0 \in \mathbb{Z}$ tais que
$$a + 1 = qb + r_0, \text{ onde } 0 \leq r_0 < b.$$

Podemos supor que $q > 0$, pois quando $q = 0$ existem $n = 0$ e $r_0 = a + 1$ e, assim, $a + 1 \in X$. Como $a + 1 > 0$ e $r_0 \geq 0$, temos que $q \leq a$, pois se $a < q$, então

$$a < q \text{ e } 1 < b \Rightarrow a + 1 \leq q \text{ e } q < qb \Rightarrow a + 1 < qb \Rightarrow qb + r_0 < qb \Rightarrow r_0 < 0,$$

o que é impossível. Assim, pela hipótese de indução, existem $n, r_i \in \mathbb{Z}$ tais que

$$q = r_n b^{n-1} + r_{n-1} b^{n-2} + \cdots + r_2 b^1 + r_1 b^0,$$

onde $r_i \in \{0, 1, \ldots, b-1\}$, $\forall i = 1, 2, \ldots, n$. Logo,

$$a + 1 = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b^1 + r_0 b^0,$$

isto é, $a + 1 \in X$. Portanto, $X = \mathbb{N}$.

(Unicidade) Suponhamos que existam $m, n, r_i, s_j \in \mathbb{Z}$ tais que

$$a = r_m b^m + r_{m-1} b^{m-1} + \cdots + r_1 b^1 + r_0 b^0,$$

onde $0 \leq r_i < b$, $r_m \geq 1$ e

$$a = s_n b^n + s_{n-1} b^{n-1} + \cdots + s_1 b^1 + s_0 b^0$$

onde $0 \leq s_j < b$, $s_n \geq 1$.

Afirmação: $b^m \leq a < b^{m+1}$.

De fato,

$$r_m \geq 1 \Rightarrow b^m \leq r_m b^m \leq a.$$

Por outro lado, como $r_i < b$ temos, pelo Teorema 3.11, que $r_i \leq b-1$. Logo,

$$\begin{aligned} a &= r_m b^m + r_{m-1} b^{m-1} + \cdots + r_1 b^1 + r_0 b^0 \\ &\leq (b-1)b^m + (b-1)b^{m-1} + \cdots + (b-1)b^1 + (b-1)b^0 \\ &= b^{m+1} - 1 \\ &< b^{m+1}. \end{aligned}$$

Portanto, $m = n$, pois se $m < n$, então $m+1 \leq n$ e, assim,

$$b^{m+1} \leq b^n \leq a,$$

o que é impossível. Logo,

$$r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b^1 + r_0 b^0 = s_n b^n + s_{n-1} b^{n-1} + \cdots + s_1 b^1 + s_0 b^0.$$

Assim,

$$r_0 - s_0 = bc$$

para algum $c \in \mathbb{Z}$. Como $0 \leq r_0, s_0 < b$ temos que $0 \leq |r_0 - s_0| < b$, assim,

$$b\,|c| < b \Rightarrow 0 \leq |c| < 1 \Rightarrow |c| = 0 \Rightarrow c = 0.$$

Logo, $r_0 = s_0$. Agora suponhamos, como hipótese de indução, que $r_i = s_i$, para todo i com $1 \leq i \leq k$ e $k < n$. Então

$$r_n b^n + \cdots + r_{k+2} b^{k+2} + r_{k+1} b^{k+1} = s_n b^n + \cdots + s_{k+2} b^{k+2} + s_{k+1} b^{k+1}.$$

Dividindo ambos os membros por b^{k+1}, obtemos

$$r_n b^{n-k-1} + \cdots + r_{k+2} b + r_{k+1} = s_n b^{n-k-1} + \cdots + s_{k+2} b + s_{k+1}$$

e, pelo mesmo argumento acima, $r_{k+1} = s_{k+1}$. Portanto, $r_i = s_i$ para todo $i = 1, 2, \ldots, n$.

Finalmente, como log é uma função crescente temos que

$$n = \log_b b^n \leq \log_b a < \log_b b^{n+1} = n+1.$$

Portanto, $n = \lfloor \log_b a \rfloor$. ■

Observação 5.10 *Dizemos que $a = (r_n r_{n-1} \cdots r_1 r_0)_b$ é a representação de a na base b e que $n+1$ é o número de dígitos na base b, onde $r_n > 0$ é o primeiro dígito e r_0 é o último*

dígito. A prova do Teorema fornece um ***Algoritmo*** *prático para representar um inteiro a em uma base qualquer $b > 1$, através das seguintes relações*:

$$\begin{array}{rcll} a & = & q_0 b + r_0, & 0 \leq r_0 < b \\ q_0 & = & q_1 b + r_1, & 0 \leq r_1 < b \\ \vdots & \vdots & \vdots & \vdots \\ q_{n-2} & = & q_{n-1} b + r_{n-1}, & 0 \leq r_{n-1} < b \ \text{ e } \ q_{n-1} < b. \end{array}$$

Fazendo $r_n = q_{n-1}$, obtemos

$$a = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b^1 + r_0.$$

Além disso, a adição, a subtração e a multiplicação são efetuadas pelo mesmo processo usual.

Exemplo 5.11 *Escreva* 142 *e* 153 *na base* 4 *e forme sua soma.*

Solução.

$$\begin{array}{rcl} 142 & = & 35 \cdot 4 + 2 \\ 35 & = & 8 \cdot 4 + 3 \\ 8 & = & 2 \cdot 4 + 0 \end{array}$$

e $2 < 4$. Logo,

$$(142)_4 = 2 \cdot 4^3 + 0 \cdot 4^2 + 3 \cdot 4 + 2 \cdot 4^0 = 2032.$$

De modo análogo, temos que

$$(153)_4 = 2 \cdot 4^3 + 1 \cdot 4^2 + 2 \cdot 4 + 1 \cdot 4^0 = 2121.$$

Soma

$$\begin{array}{cccccc} & 2 & 0 & 3 & 2 \\ + & 2 & 1 & 2 & 1 \\ \hline 1 & 0 & 2 & 1 & 3 \end{array}$$

$2 + 1 = 3$, $3 + 2 = 11$, escrevemos 1 e transportamos 1, $1 + 0 + 1 = 2$, etc.

EXERCÍCIOS

1. Sejam $a, b \in \mathbb{Z}$ tais que $a = qb + r$, onde $0 \leq r < b$. Se $a \geq 0$, mostrar que $q \geq 0$.

2. Sejam $a, b \in \mathbb{Z}$ tais que $a = qb + r$, onde $0 \leq r < b$. Se $a \geq b$, mostrar que $r \leq \frac{a}{2}$.

3. Sejam $a, b \in \mathbb{Z}$ tais que $a = qb + r$, onde $0 \leq r < b$. Mostrar que $q = \lfloor \frac{a}{b} \rfloor$.

4. Dado $c \in \mathbb{Q}$. Mostrar que existe $a \in \mathbb{Z}$ tal que $a \in \ ]c, c + 1]$.

5. Seja $b \in \mathbb{Z}$ com $b > 1$. Mostrar que a equação $xb = 1$ não tem solução em $\mathbb{Z}$.

6. Sejam $a, b \in \mathbb{Z}$ com $b > 0$. Mostrar que existem únicos $q, r \in \mathbb{Z}$ tais que $a = qb + r$, onde $2b \leq r < 3b$.

7. Exprima 212 usando as bases 2, 3, 4, 5, 7, 9 e 13.

8. Com quantos dígitos se escreve o número $2^{1.000}$ no sistema de representação decimal.

9. Sejam $a, b \in \mathbb{Z}$. Mostrar que, se 3 divide $a^2 + ab + b^2$, então a e b têm o mesmo resto quando divididos por 3.

10. Para todo $n \in \mathbb{N}$, mostrar que:

    (a) $5^{6n} - 3^{6n}$ é divisível por 152.

    (b) $a^n - b^n$ é divisível por $a - b$.

    (c) $a^n + b^n$ é divisível por $a + b$ se n é ímpar.

    (d) $(n+1)^n - 1$ é divisível por n^2.

    (e) $5^n + 2.3^{n-1} + 1$ é divisível por 8.

    (f) $10^n + 3.4^{n+2} + 5$ é divisível por 9.

    (g) $(3 + \sqrt{5})^n + (3 - \sqrt{5})^n$ é divisível por 2^n.

    (h) $3(1^5 + 2^5 + \cdots + n^5)$ é divisível por $1^3 + 2^3 + \cdots + n^3$.

11. Se $n \in \mathbb{N}$, com $n > 1$ e ímpar, então $1^n + 2^n + \cdots + (n-1)^n$ é divisível por n.

12. Mostrar que $1^{97} + 2^{97} + 3^{97} + 4^{97} + 5^{97}$ é divisível por 5.

13. Mostrar que não existe $n \in \mathbb{N}$ tal que $n^2 + 2n + 12$ seja divisível por 121.

14. Mostrar que a soma dos cubos de três inteiros consecutivos e positivos é divisível por 9.

15. Determinar todos os $a \in \mathbb{N}$ tais que $a^2 + 1$ seja divisível por $a + 1$.

16. Determinar todos os $a \in \mathbb{Z} - \{3\}$ tais que $a^3 - 3$ seja divisível por $a - 3$.

17. Seja $n \in \mathbb{N}$ com $n > 1$. Mostrar que k divide $(n+1)! + k$, onde $2 \leq k \leq n + 1$.

18. Seja $n \in \mathbb{N}$. Mostrar que existem $r, s \in \mathbb{N}$ tais que

$$n = \frac{(r+s)^2 + 3r + s}{2}.$$

19. Mostrar que se um número inteiro é simultaneamente um quadrado e um cubo $(64 = 8^2 = 4^3)$, então ele é da forma $7k$ ou $7k + 1$, para algum $k \in \mathbb{N}$.

20. Mostrar que nenhum termo da seqüência 11, 111, 1111, ... é um quadrado perfeito. (Sugestão: $111 \cdots 111 = 111 \cdots 108 + 3 = 4k + 3$.)

21. Mostrar que o número

$$\overbrace{11\cdots1}^{n-1}\underbrace{22\cdots2}_{n}5, \forall n \in \mathbb{N},$$

é um quadrado perfeito.

22. Sejam $a = xyz$ e $b = zyx$ dois inteiros positivos no sistema de representação decimal. Mostrar que $a - b$ é divisível por 99.

23. Sejam $n = xyzuv$ e $m = xyuv$ dois inteiros positivos no sistema de representação decimal. Determinar todos os n tais que

$$\frac{n}{m} \in \mathbb{N}.$$

(Sugestão: Mostre que $9m < n < 11m$.)

24. Determinar todos os inteiros positivos que começam com dígito 6 e diminui 25 vezes quando esse é descartado. (Sugestão: Seja $a \in \mathbb{N}$. Então $a = 6 \cdot 10^n + b$ e $a = 25b$, onde $0 \leq b \leq 10^n - 1$.)

25. Mostrar que não existe um número inteiro positivo que diminua 35 vezes quando seu primeiro dígito é descartado.

26. Determinar o menor inteiro positivo que começa com dígito 1 e aumenta 3 vezes quando esse dígito é passado para o final. (Sugestão: Seja $a \in \mathbb{N}$. Então $a = 10^n + b$ e $3a = 10b + 1$, onde $0 \leq b \leq 10^n - 1$, continue)

27. Determinar o menor inteiro positivo cujo último dígito é 6, sabendo-se que esse número aumenta 4 vezes quando esse último dígito é levado para o início do número.

28. Cada um dos números $1 = 1$, $3 = 1 + 2$, $6 = 1 + 2 + 3, \ldots$ representa o número de pontos que pode ser arranjado igualmente em um triângulo equilátero, por exemplo, o número 6 é representado como 3 na base 2 no meio e 1 no topo. Um número $t \in \mathbb{N}$ é chamado um *número triangular* se existir $n \in \mathbb{N}$ tal que $t = 1 + 2 + \cdots + n$. Mostrar que:

    (a) t é um número triangular se, e somente se, $t = \frac{n(n+1)}{2}$ para algum $n \in \mathbb{N}$.

    (b) Se t é um número triangular, então $8t + 1$ é um quadrado perfeito.

    (c) A soma de quaisquer dois números triangulares consecutivos é um quadrado perfeito.

    (d) Se t é um número triangular, então $9t + 1$, $25t + 3$ e $49t + 6$ também o são.

    (e) Se t é um número triangular, então $4t + 1$ é uma soma de dois quadrados.

29. Seja T_n o n-ésimo número triangular. Mostrar que:

(a) $T_n = \binom{n+1}{2}$.

(b) $T_1 + T_2 + \cdots + T_n = \frac{n(n+1)(n+2)}{6}$. (Sugestão: $T_{k-1} + T_k = k^2$.)

(c) $T_{9n+4} - T_{3n+1} = 9(2n+1)^2$.

30. Seja $n \in \mathbb{N}$. Mostrar que 2^n pode ser escrito como uma soma de dois quadrados.

5.2 MDC e MMC

Nesta seção estudaremos formalmente os conceitos de máximo divisor comum e de mínimo múltiplo comum de quaisquer dois inteiros não ambos nulos, os quais podem, indutivamente, ser estendidos para quaisquer número finito de inteiros não nulos.

Definição 5.12 *Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$ ou $b \neq 0$. O* máximo divisor comum *de a e b, em símbolos $mdc(a, b)$, é um inteiro positivo d tal que*:

1. *$d \mid a$ e $d \mid b$.*

2. *Se $c \mid a$ e $c \mid b$, então $c \mid d$.*

Observação 5.13 *A condição* (1) *diz que d é um divisor comum de a e b,* (2) *diz que d é o "maior" divisor comum de a e b. Se $a, b \in \mathbb{Z}^*$ e $mdc(a, b)$ existe, então ele é único.* (*Prove isto!*)

Exemplo 5.14 *Os divisores positivos de -12 são $1, 2, 3, 4, 6, 12$, enquanto os divisores positivos de 30 são $1, 2, 3, 5, 6, 10, 15, 30$. Logo, os divisores comuns são $1, 2, 3, 6$. Como 6 é o maior desses divisores comuns temos que $mdc(-12, 30) = 6$.*

Teorema 5.15 *Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$ ou $b \neq 0$. Então $d = mdc(a, b)$ existe. Além disso, existem $x, y \in \mathbb{Z}$ tais que $d = ax + by$.*

Prova. Seja

$$X = \{ar + bs : r, s \in \mathbb{Z} \text{ e } ar + bs > 0\}.$$

Então $X \neq \emptyset$, pois se $a \neq 0$, então $|a| = a.1 + b.0$ ou $|a| = a(-1) + b.0$ mostrando, assim, que $|a| \in X$, e $X \subseteq \mathbb{N}$. Logo, pelo Axioma 3.9, X contém um menor elemento $d > 0$, isto é, existem $x, y \in \mathbb{Z}$ tais que $d = ax + by$.

Agora, vamos provar que $d = \text{mdc}(a, b)$. De fato, pelo Teorema 5.1, existem $q, r \in \mathbb{Z}$ tais que

$$a = qd + r, \text{ onde } 0 \leq r < d.$$

Então

$$r = a - qd = a(1 - qx) + b(-qy) \Rightarrow r = 0,$$

pois se $r > 0$, então $r \in X$, o que contradiz a escolha de d. Assim, $a = qd$ ou $d \mid a$. De modo análogo, mostra-se que $d \mid b$. Finalmente, se $c \mid a$ e $c \mid b$, temos, pelo item (7) do Teorema 5.7, que $c \mid (ax + by)$, isto é, $c \mid d$. ■

Sejam $a, b \in \mathbb{Z}^*$, dizemos que a e b são *relativamente primos* ou *primos entre si* quando $\text{mdc}(a, b) = 1$.

Teorema 5.16 *Sejam $a, b \in \mathbb{Z}^*$. Então a e b são relativamente primos se, e somente se, existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$.*

Prova. Suponhamos que existam $x, y \in \mathbb{Z}$ tais que $ax + by = 1$ e seja $d = \text{mdc}(a, b)$. Então temos, pelo item 7 do Teorema 5.7, que $d \mid 1$ e, portanto, $d = 1$. A recíproca é imediata. ■

Lema 5.17 *Sejam $a, b, c \in \mathbb{Z}^*$. Então $mdc(ac, bc) = |c|\, mdc(a, b)$.*

Prova. Seja $d = \text{mdc}(a, b)$. Então $d \mid a$ e $d \mid b$. Logo, pelo item (4) do Teorema 5.7, $cd \mid ca$ e $cd \mid cb$ e, assim, $cd \mid \text{mdc}(ca, bc)$, isto é, existe $x \in \mathbb{Z}$ tal que $\text{mdc}(ca, bc) = xcd$. Logo, $xcd \mid ca$ e $xcd \mid cb$ e, pelo item (4) do Teorema 5.7, $xd \mid a$ e $xd \mid b$. Logo, por hipótese, $xd \mid d$, ou seja, $x \mid 1$ e, pelo item (2) do Teorema 5.7, $x = \pm 1$. Portanto, $\text{mdc}(ca, bc) = \pm cd = |c|\, \text{mdc}(a, b)$. ■

Exemplo 5.18 *Sejam $a, b \in \mathbb{Z}^*$. Se $mdc(a, b) = 1$ mostrar que*

$$mdc(a + b, a - b) = 1 \text{ ou } 2.$$

Solução. Seja $d = \text{mdc}(a + b, a - b)$. Então $d \mid (a + b)$ e $d \mid (a - b)$. Logo, pelo item (7) do Teorema 5.7, $d \mid 2a$ e $d \mid 2b$. Logo, $d \leq \text{mdc}(2a, 2b) = 2\text{mdc}(a, b) = 2$. Portanto, $d = 1$ ou 2.

Se $c \mid ab$ não vale, em geral, que $c \mid a$ ou $c \mid b$. Por exemplo,

$$6 \mid 3 \cdot 4 \text{ mas } 6 \nmid 3 \text{ e } 6 \nmid 4.$$

Mas temos o seguinte:

Lema 5.19 (Euclides) *Sejam $a, b, c \in \mathbb{Z}^*$. Se $c \mid ab$ e $mdc(a, c) = 1$, então $c \mid b$.*

Prova. Como $\text{mdc}(a, c) = 1$ temos que existem $x, y \in \mathbb{Z}$ tais que $ax + cy = 1$. Logo, $abx + bcy = b$. Pela hipótese, $c \mid ab$ e $c \mid c$, assim, pelo item (7) do Teorema 5.7, $c \mid (abx + bcy)$, isto é, $c \mid b$. ■

Lema 5.20 *Sejam $a, b \in \mathbb{Z}^*$. Se $a = qb + r$, onde $0 \leq r < b$, então $mdc(a, b) = mdc(b, r)$.*

Prova. Suponhamos que $\text{mdc}(a,b) = d$. Então

$$d \mid a \text{ e } d \mid b \Rightarrow d \mid r.$$

Logo, $d \mid b$ e $d \mid r$. Por outro lado, se $c \mid b$ e $c \mid r$, então $c \mid a$. Logo, $c \mid a$ e $c \mid b$, assim, pela hipótese, $c \mid d$. Portanto, $d = \text{mdc}(b,r)$. ■

Embora o Teorema 5.15 assegure a existência do $\text{mdc}(a,b)$, a sua demonstração não diz como achar o seu valor. Agora, apresentaremos um processo, conhecido como **Algoritmo Euclidiano**, para determinar o máximo divisor comum de dois inteiros não nulos a e b.

Podemos supor, sem perda de generalidade, que $a \geq b > 0$, pois

$$\text{mdc}(a,b) = \text{mdc}(|a|, |b|).$$

Pelo Teorema 5.1 existem $q_1, r_1 \in \mathbb{Z}$ tais que

$$a = q_1 b + r_1, \text{ onde } 0 \leq r_1 < b.$$

Se $r_1 = 0$, então $b \mid a$ e $\text{mdc}(a,b) = b$. Se, ao contrário, $r_1 \neq 0$, então existem $q_2, r_2 \in \mathbb{Z}$ tais que

$$b = q_2 r_1 + r_2, \text{ onde } 0 \leq r_2 < r_1.$$

Se $r_2 = 0$, então $r_1 \mid b$ e $\text{mdc}(a,b) = \text{mdc}(b,r_1) = r_1$. Caso contrário, procedendo como antes, obtemos

$$r_1 = q_3 r_2 + r_3, \text{ onde } 0 \leq r_3 < r_2,$$

e assim por diante até que algum dos restos seja igual a zero, digamos $r_{n+1} = 0$, pois uma seqüência

$$r_1 > r_2 > \cdots > r_n > 0$$

decrescente de inteiros positivos não pode ser infinita pelo Axioma 3.9. Obtemos as seguintes relações:

$$\begin{array}{lcll}
a & = & q_1 b + r_1 & \text{onde } 0 < r_1 < b \\
b & = & q_2 r_1 + r_2 & \text{onde } 0 < r_2 < r_1 \\
r_1 & = & q_3 r_2 + r_3 & \text{onde } 0 < r_3 < r_2 \\
\vdots & \vdots & \vdots & \vdots \\
r_{n-2} & = & q_n r_{n-1} + r_n & \text{onde } 0 < r_n < r_{n-1} \\
r_{n-1} & = & q_{n+1} r_n. &
\end{array}$$

Portanto, $\text{mdc}(a,b) = \text{mdc}(b,r_1) = \cdots = \text{mdc}(r_{n-1}, r_n) = r_n$. Podemos representar estas relações pela Tabela abaixo

	q_1	q_2	q_3	$\cdots$	q_n	q_{n+1}
a	b	r_1	r_2	$\cdots$	r_{n-1}	r_n
r_1	r_2	r_3	r_4	$\cdots$	r_n	0

Note que o Algoritmo Euclidiando para determinar o máximo divisor comum de $a, b \in \mathbb{Z}_+$ pode ser implementado iterativamente nos os seguintes passos:

1.^{o} Passo. Se $b = 0$, então retorne a, e vá para o Passo 4.

2.^{o} Passo. Calcule q_1e r_1 de modo que $a = q_1 b + r_1$ e $0 \leq r_1 < b$.

3.^{o} Passo. Faça $b = r_1$ e $a = b$, e volte para 1.

4.^{o} Passo. Fim.

O número de iterações deste Algoritmo é finito (no máximo $a + b$), pois a seqüência decrescente

$$r_1 > r_2 > \cdots > r_n \geq 0$$

de inteiros positivos não pode ser infinita.

Exemplo 5.21 *Determinar o mdc*$(21, 35)$.

Solução. Pela tabela

$$\begin{array}{cccc} a & b & q & r \\ 35 & 21 & 1 & 14 \\ 21 & 14 & 1 & 7 \\ 14 & 7 & 2 & 0 \\ 7 & 0 & & \end{array},$$

obtemos que o mdc$(21, 35) = 7$.

Observação 5.22 *O Algoritmo Euclidiano pode também ser usado para representar o mdc*(a, b) *na forma* $ax + by$*, pois da penúltima equação, obtemos*:

$$r_n = r_{n-2} + (-q_n) r_{n-1}.$$

Agora, substituindo o resto r_{n-1} *da equação anterior, obtemos*:

$$r_n = (-q_n) r_{n-3} + (1 + q_n q_{n-1}) r_{n-2}.$$

Prosseguindo assim, podemos eliminar sucessivamente os restos

$$r_{n-1}, r_{n-2}, \ldots, r_2, r_1$$

e expressar r_n *em termos de* a *e* b*, isto é, podemos encontrar* $x, y \in \mathbb{Z}$ *tais que*

$$mdc(a, b) = ax + by.$$

Exemplo 5.23 *Encontrar* $x, y \in \mathbb{Z}$ *tais que*

$$mdc(21, 35) = 21x + 35y.$$

Solução. De

$$\begin{aligned} 35 &= 1 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 + 0 \end{aligned}$$

obtemos que

$$7 = 2.21 + (-1)35.$$

Portanto, $\text{mdc}(21, 35) = 7$. Além disso, $x = 2$ e $y = -1$ são tais que $7 = 21x + 35y$. Como $z = 2 - 35n$ e $w = -1 + 21n$, para todo $n \in \mathbb{Z}$, também satisfazem, temos que x e y não são únicos.

Uma equação algébrica com coeficientes inteiros chama-se uma *equação Diofantina* se suas soluções são números inteiros ou racionais.

Exemplo 5.24 *Determinar todas as soluções positivas da equação Diofantina*

$$39x + 54y = 6.000. \tag{5.1}$$

Solução. De

$$\begin{aligned} 54 &= 1 \cdot 39 + 15 \\ 39 &= 2 \cdot 15 + 9 \\ 15 &= 1 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

obtemos que

$$7 \cdot 39 + (-5) \cdot 54 = 3.$$

Portanto,

$$14.000 \cdot 39 + (-10.000) \cdot 54 = 6.000.$$

Assim, $x = 14.000 - 18t$ e $y = -10.000 + 13t$, para todo $t \in \mathbb{Z}$ é a solução geral da equação 5.1. Podemos também resolver a equação 5.1 usando operações elementares sobre as duas primeiras colunas do seguinte arranjo:

$$\begin{array}{rrr} 39 & 54 & 6.000 \\ 1 & 0 & \\ 0 & 1 & \end{array} \quad \begin{array}{c} \\ c_2 \to c_2 - c_1 \\ \\ \end{array} \quad \begin{array}{rrr} 39 & 15 & 6.000 \\ 1 & -1 & \\ 0 & 1 & \end{array} \quad \begin{array}{c} \\ c_1 \to c_1 - 2c_2 \\ \\ \end{array}$$

$$\begin{array}{rrr} 9 & 15 & 6.000 \\ 3 & -1 & \\ -2 & 1 & \end{array} \quad \begin{array}{c} \\ c_2 \to c_2 - c_1 \\ \\ \end{array} \quad \begin{array}{rrr} 9 & 6 & 6.000 \\ 3 & -4 & \\ -2 & 3 & \end{array} \quad \begin{array}{c} \\ c_1 \to c_1 - c_2 \\ \\ \end{array}$$

$$\begin{array}{rrr} 3 & 6 & 6.000 \\ 7 & -4 & \\ -5 & 3 & \end{array} \quad \begin{array}{c} \\ c_2 \to c_2 - 2c_1 \\ \\ \end{array} \quad \begin{array}{rrr} 3 & 0 & 6.000 \\ 7 & -18 & \\ -5 & 13 & \end{array} \quad ,$$

onde $c_i \rightarrow c_i + mc_j$, $\forall m \in \mathbb{Z}$, significa a substituição da coluna c_i pela coluna $c_i + mc_j$. Sejam $z, w \in \mathbb{Z}$ as variáveis que estão implicitamente no último arranjo. Então $3z = 6.000$ ou $z = 2.000$. Assim,

$$x = 7z - 18w = 14.000 - 18w \text{ e } y = -5z + 13w = -10.000 + 13w$$

é a solução geral da equação 5.1. Note que o termo constante da solução geral pode ser reduzido, por exemplo, fazendo $w = k + 777$, obtemos

$$x = 14 - 18k \text{ e } y = 101 + 13k$$

Como queremos as soluções positivas, temos que resolver as inequações

$$14 - 18k \geq 0 \text{ e } 101 + 13k \geq 0.$$

Logo,

$$-\frac{101}{13} \leq k \leq \frac{14}{18},$$

isto é, $-7 \leq k \leq 0$. Portanto, as soluções positivas são:

$$x = 14 - 18k \text{ e } y = 101 + 13k$$

com $k \in \{-7, -6, -5, -4, -3, -2, -1, 0\}$.

Observação 5.25 *O método de operações elementares visto acima pode ser usado para resolver sistemas de equações Diofantinas com duas ou mais variáveis.*

Definição 5.26 *Sejam $a, b \in \mathbb{Z}^*$. O* mínimo múltiplo comum *de a e b, em símbolos $mmc(a, b)$, é um inteiro positivo m tal que*:

1. *$a \mid m$ e $b \mid m$.*
2. *Se $a \mid c$ e $b \mid c$, então $m \mid c$.*

Observação 5.27 *A condição 1 diz que m é um múltiplo comum de a e b, 2 diz que m é o menor múltiplo comum de a e b. Se $a, b \in \mathbb{Z}^*$ e $mmc(a, b)$ existe, então ele é único. (Prove isto!)*

Teorema 5.28 *Sejam $a, b \in \mathbb{Z}^*$. Então*

$$mmc(a, b) = \frac{|ab|}{mdc(a, b)}.$$

Prova. Basta verificarmos o caso em que $a, b > 0$. Seja $d = \text{mdc}(a, b)$. Então existem $u, v \in \mathbb{Z}$ tais que

$$a = ud \text{ e } b = vd.$$

Se $md = ab$, então $m = ub$ e $m = va$. Logo, $a \mid m$ e $b \mid m$. Por outro lado, se $a \mid c$ e $b \mid c$, então existem $r, s \in \mathbb{Z}$ tais que

$$c = ra \text{ e } c = sb.$$

Como existem $x, y \in \mathbb{Z}$ tais que

$$d = ax + by,$$

temos que

$$\frac{c}{m} = \frac{cd}{md} = \frac{cax + cby}{ab} = \frac{absx + abry}{ab} = sx + ry \in \mathbb{Z}.$$

Logo, $m \mid c$. ■

Corolário 5.29 *Sejam $a, b \in \mathbb{Z}^*$. Então $mmc(a, b) = |ab|$ se, e somente se, $mdc(a, b) = 1$.* ■

Exemplo 5.30 *Calcule o mínimo múltiplo comum de 21 e 35.*

Solução. Temos que

$$\text{mmc}(21, 35) = \frac{21 \cdot 35}{\text{mdc}(21, 35)} = \frac{21 \cdot 35}{7} = 105.$$

Podemos, também, determinar o mínimo múltiplo comum de 21 e 35 usando a seguinte tabela:

$$\begin{array}{cc|c} 21 & 35 & 3 \\ 7 & 35 & 5 \\ 7 & 7 & 7 \\ 1 & 1 & \end{array} .$$

Portanto, $\text{mmc}(21, 35) = 3 \cdot 5 \cdot 7 = 105$.

Exemplo 5.31 *Sejam $a, b \in \mathbb{N}$. Dados $d = mdc(a, b)$ e $m = mmc(a, b)$, determinar a e b.*

Solução. Como $d = \text{mdc}(a, b)$ temos que existem $x, y \in \mathbb{Z}$ tais que

$$a = dx \text{ e } b = dy,$$

onde $\text{mdc}(x, y) = 1$. Temos, pelo Teorema 5.28, que $md = d^2xy$, ou ainda, $m = dxy$. Assim, como d e m são dados, podemos da equação $m = dxy$ determinar todas as possibilidades para x e y tais que $\text{mdc}(x, y) = 1$.

EXERCÍCIOS

1. Calcular $x, y \in \mathbb{Z}$ tais que $\text{mdc}(a, b) = ax + by$, nos seguintes casos:

   (a) $a = 11$ e $b = 15$.

   (b) $a = 167$ e $b = 389$.

(c) $a = 180$ e $b = 252$.

(d) $a = 2.464$ e $b = 7.469$.

2. Sejam $a_1, \ldots, a_n \in \mathbb{Z}^*$. Mostrar que se

$$\text{mdc}(a_1, a_2) = d_2, \text{mdc}(d_2, a_3) = d_3, \ldots, \text{mdc}(d_{n-1}, a_n) = d_n,$$

então

$$\text{mdc}(a_1, a_2, \ldots, a_n) = d_n$$

3. Encontrar o $\text{mmc}(a, b)$ no exercício 1.

4. Sejam $a_1, \ldots, a_n \in \mathbb{Z}^*$. Mostrar que se

$$\text{mmc}(a_1, a_2) = m_2, \text{mmc}(m_2, a_3) = m_3, \ldots, \text{mmc}(m_{n-1}, a_n) = m_n,$$

então

$$\text{mmc}(a_1, a_2, \ldots, a_n) = m_n$$

5. Mostrar que existem infinitos $a, b \in \mathbb{Z}$ tais que $a + b = 100$ e $\text{mdc}(a, b) = 5$.

6. Sejam $a, b, c \in \mathbb{Z}^*$ e $\text{mdc}(a, b) = d$. Mostrar que:

(a) A equação $ax + by = c$ tem solução em $\mathbb{Z}$ se, e somente se, d divide c.

(b) Se $x_0, y_0 \in \mathbb{Z}$ é uma solução particular da equação $ax + by = c$, então

$$x = x_0 + k\frac{b}{d} \text{ e } y = y_0 - k\frac{a}{d}, \forall k \in \mathbb{Z}$$

também o é.

(c) Se $d = 1$ e $c \geq ab$, então existem $x, y \in \mathbb{Z}_+$ tais que $ax + by = c$.

7. Determinar, se existir, a solução geral das seguintes equações:

(a) $15x + 51y = 41$.

(b) $17x + 19y = 23$.

(c) $10x - 8y = 12$.

8. Em uma loja dois produtos custam $R\$71,00$ e $R\$83,00$, respectivamente. Que quantidade inteiras de ambos podem ser compradas com $R\$1.670,00$?

9. Um terreno retângular, com dimensões $7.200m$ por $2.700m$, respectivamente, foi dividido em lotes quadrados. Determinar a maior área possível para esses lotes.

10. Sejam $a, b \in \mathbb{Z}$. Mostrar que $\text{mdc}(a, b) = 1$ se, e somente se, existem $u, v \in \mathbb{Z}$ tais que
$$\det(\begin{bmatrix} a & b \\ u & v \end{bmatrix}) = \pm 1.$$

11. Sejam $a, b, c \in \mathbb{Z}^*$. Mostrar as seguintes afirmações:

    (a) $\text{mdc}(a, b) = \text{mdc}(a, -b) = \text{mdc}(-a, b) = \text{mdc}(-a, -b)$.

    (b) $\text{mdc}(a, b) = \text{mdc}(a, ar + b), \forall r \in \mathbb{Z}$.

    (c) $\text{mdc}(a, b) = \text{mdc}(a, b, ar + bs), \forall r, s \in \mathbb{Z}$.

    (d) Se $\text{mdc}(a, b) = \text{mdc}(a, c) = 1$, então $\text{mdc}(a, bc) = 1$.

    (e) Se $\text{mdc}(a, b) = 1$ e c divide $a + b$, então $\text{mdc}(a, c) = \text{mdc}(b, c) = 1$. (Sugestão: Seja $d = \text{mdc}(a, c)$. Então $d \mid a$ e $d \mid c$, assim d divide $(a + b) - a$, isto é, $d \mid b$.)

    (f) Se $\text{mdc}(a, b) = 1$, então $\text{mdc}(a^n, b^n) = 1, \forall n \in \mathbb{N}$.

12. Sejam $a_1, \ldots, a_n \in \mathbb{N}$ e $m = \text{mmc}(a_1, \ldots, a_n)$. Mostrar que o resto da divisão de $km - 1$ por a_i é $a_i - 1$ para todo $i = 1, \ldots, n$ e $k \in \mathbb{N}$.

13. Determinar o menor inteiro positivo que tem para restos 2, 3 e 4 quando dividido, respectivamente, por 3, 4 e 5. (Sugestão: Seja $n \in \mathbb{N}$. Então $n = 3r + 2$, $n = 4s + 3$ e $n = 5t + 4$. Logo, $n + 1 = 3(r + 1)$, $n + 1 = 4(s + 1)$ e $n + 1 = 5(t + 1)$, continue.)

14. Determinar o menor inteiro positivo que tem para restos 1, 2, 3, 4 e 5 quando dividido, respectivamente, por 2, 3, 4, 5 e 6.

15. Sejam $a, b \in \mathbb{Z}^*$ e $n \in \mathbb{N}$. Mostrar que:

    (a) Se a^n divide b^n, então a divide b. (Sugestão: Seja $d = \text{mdc}(a, b)$. Então existem $x, y \in \mathbb{Z}$ tais que $a = dx$ e $b = dy$, onde $\text{mdc}(x, y) = 1$. Pelo item (f) do exercício 10 temos que $\text{mdc}(x^n, y^n) = 1$. Agora mostre que $x = 1$, de modo que $a = d$.)

    (b) Se a^n divide $2b^n$, então a divide b.

16. Sejam $a, b \in \mathbb{Z}^*$. Mostrar que as seguintes condições são equivalentes:

    (a) a divide b.

    (b) $\text{mdc}(a, b) = |a|$.

    (c) $\text{mmc}(a, b) = |b|$.

17. Sejam $a, b \in \mathbb{Z}^*$. Mostrar que se $\text{mdc}(a, b) = \text{mmc}(a, b)$, então $|a| = |b|$.

18. Sejam $a, b \in \mathbb{Z}^*$. Mostrar que $\text{mdc}(a, a + b)$ divide b.

19. Mostrar que $\text{mdc}(a, a+2) = 1$ ou 2 para todo $a \in \mathbb{Z}$.

20. Mostrar que $\text{mdc}(4a+3, 5a+4) = 1$ para todo $a \in \mathbb{Z}$.

21. Sejam $a, b, c \in \mathbb{Z}^*$ e $\text{mdc}(a, b) = d$. Mostrar que $a \mid bc$ se, e somente se, $\frac{a}{d} \mid c$.

22. Sejam $a, b, c \in \mathbb{Z}^*$. Se $\text{mdc}(a, b) = 1$, $a \mid c$ e $b \mid c$, então $ab \mid c$.

23. Mostrar que 10 divide $1^n + 8^n - 3^n - 6^n, \forall n \in \mathbb{N}$.

24. Mostrar que:

    (a) Dois inteiros consecutivos são sempre primos entre si.

    (b) $\text{mdc}(2a+1, 9a+4) = 1, \forall a \in \mathbb{Z}$.

25. Sejam $a, b \in \mathbb{Z}^*$ tais que $\text{mdc}(a, b) = 1$. Mostrar que $\text{mdc}(a+b, a^2 - ab + b^2) = 1$ ou 3. (Sugestão: Note que $a^2 - ab + b^2 = (a+b)^2 - 3ab$.)

26. Determinar todos os possíveis $a, b \in \mathbb{N}$ tais que $\text{mdc}(a, b) = 10$ e $\text{mmc}(a, b) = 100$.

27. Sejam $d, m \in \mathbb{N}$. Mostrar que existem $a, b \in \mathbb{Z}$ tais que $\text{mdc}(a, b) = d$ e $\text{mmc}(a, b) = m$ se, e somente se, $d \mid m$.

28. Sejam $d, m \in \mathbb{Z}$ com $d > 0$. Mostrar que existem $a, b \in \mathbb{Z}$ tais que $\text{mdc}(a, b) = d$ e $ab = m$ se, e somente se, $d^2 \mid m$.

29. Seja $x_1 = 2$, $x_2 = x_1 + 1$, $x_3 = x_1 x_2 + 1, \ldots$, $x_n = x_1 x_2 \cdots x_{n-1} + 1, \ldots$ uma seqüência. Mostrar que se $k \neq n$, então $\text{mdc}(x_k, x_n) = 1$.

30. Seja $x_1, x_2, \ldots, x_n, \ldots$ uma seqüência definida recursivamente por $x_1 = 1$, $x_2 = 1$ e $x_{n+2} = x_{n+1} + x_n$. Mostrar que:

    (a) $\text{mdc}(x_n, x_{n+1}) = 1$, para todo $n \in \mathbb{N}$.

    (b) $x_{m+n} = x_{m-1} x_n + x_m x_{n+1}$, para todos $m, n \in \mathbb{N}$. (Sugestão: Fixe m e use indução sobre n.)

    (c) x_{mn} divide x_m, para todos $m, n \in \mathbb{N}$.

    (d) $x_{n+2}^2 = x_{n+3} x_{n+1} + (-1)^{n+1}$, para todo $n \in \mathbb{N}$. (Sugestão:

$$\begin{aligned} x_{n+2}^2 - x_{n+3} x_{n+1} &= x_{n+2}(x_{n+1} + x_n) - x_{n+3} x_{n+1} \\ &= (x_{n+2} - x_{n+3}) x_{n+1} + x_{n+2} x_n \\ &= -1(x_{n+1}^2 - x_{n+2} x_n). \end{aligned}$$

    Agora, repete o argumento com $(x_{n+1}^2 - x_{n+2} x_n)$.)

31. Sejam $a, x_1, x_2, \ldots, x_n \in \mathbb{Z}^*$ tais que

$$\text{mdc}(a, x_1) = \cdots = \text{mdc}(a, x_n) = 1.$$

Mostrar que $\text{mdc}(a, x_1 x_2 \cdots x_n) = 1$.

32. Seja $x_1, x_2, \ldots, x_n, \ldots$ uma seqüência definida recursivamente por $x_1 = 2$ e $x_{n+1} = x_n^2 - x_n + 1$. Mostrar que $\text{mdc}(x_n, x_{n+1}) = 1$, para todo $n \in \mathbb{N}$. (Sugestão: Mostre que $x_{n+1} = x_n x_{n-1} \cdots x_2 x_1 + 1$.)

33. Escreva o número 300 como soma de dois inteiros positivos de tal forma que um é múltiplo de 7 e o outro seja múltiplo de 17.

34. Mostrar que não existem $a, b \in \mathbb{N}$ tais que $a^3 + 11^3 = b^3$.

35. Determinar todos os pares de inteiros a e b tais que $a^3 + b = b^3 + a$.

36. Determinar todos os pares de números inteiros cuja soma seja igual a seu produto.

37. Determinar todos os ternos de inteiros positivos a, b e c tais que

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 1.$$

(Sugestão: Primeiro mostre que pelo menos um dos inteiros a, b ou c é menor do que 4. Assim, se $a \leq b \leq c$, então $a = 2$ e $a = 3$, pois $a > 1$.)

38. Determinar todos os ternos de inteiros a, b e c tais que a soma de um deles com o produto dos outros dois seja igual a 2.

39. Determinar todos os ternos de inteiros a, b e c, dois a dois primos entre si, tais que

$$\frac{a}{b} + \frac{b}{c} + \frac{c}{a} \in \mathbb{Z}.$$

40. Mostrar que a soma dos quadrados de cinco números inteiros consecutivos não é um quadrado perfeito de um número inteiro.

41. Sejam $a, b, c \in \mathbb{Z}$ tais que $a^2 + b^2 = c^2$. Mostrar que:

    (a) a ou b é par.

    (b) a ou b é divisível por 3.

    (c) a ou b é divisível por 4.

42. Mostrar que se os comprimentos dos lados e da diagonal de um retângulo são números inteiros, então a área do retângulo é divisível por 12. (Sugestão: Use o exercício precedente.)

43. Mostrar que somando-se 1 ao produto de quatro números inteiros consecutivos obtém-se um quadrado perfeito.

44. Ache um número com quatro dígitos que é um quadrado perfeito tal que os dois primeiros dígitos são iguais e dois últimos dígitos são iguais.

45. A soma de um número de dois dígitos e um número obtido com os mesmos dígitos na ordem inversa é um quadrado perfeito. Ache todos esses números.

46. Mostrar que não existe polinômio com coeficientes inteiros tais que $f(1) = 2$ e $f(3) = 5$.

47. Seja $f(x)$ um polinômio com coeficientes inteiros. Se existem inteiros distintos a, b, c e d tais que
$$f(a) = f(b) = f(c) = f(d) = 5,$$
então mostre que não existe inteiro n tal que $f(n) = 8$. (Sugestão: Considere o polinômio $g(x) = f(x) - 5$.)

48. Se os coeficientes da equação
$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$$
são inteiros, então toda raiz racional desta equação é um inteiro.

49. Se $n > 1$ é um inteiro ímpar, então três termos consecutivos x, y e z de uma P.A. nunca satisfaz
$$x^n + y^n = z^n.$$
(Sugestão: Seja $x = y - r$ e $z = y + r$, onde $0 < r < y$. Assim,
$$(y-r)^n + y^n = (y+r)^n \Leftrightarrow (\frac{y}{r} - 1)^n + (\frac{y}{r})^n = (\frac{y}{r} + 1)^n.$$
Agora, fazendo $t = \frac{y}{r}$, obtemos a equação
$$(t-1)^n + t^n = (t+1)^n$$
e, use o exercício precedente.)

50. Para que valores de n o número $x = 2^8 + 2^{11} + 2^n$ é um quadrado perfeito.

51. Se $m, n, k \in \mathbb{N}$ e
$$1 + m + n\sqrt{3} = (2 + \sqrt{3})^{2k-1},$$
então m é um quadrado perfeito. (Sugestão: Como
$$1 + m - n\sqrt{3} = (2 - \sqrt{3})^{2k-1} \Rightarrow 1 + m = \frac{(2+\sqrt{3})^{2k-1} + (2-\sqrt{3})^{2k-1}}{2}.$$
Seja
$$f(k) = \frac{(2+\sqrt{3})^k}{1+\sqrt{3}} + \frac{(2-\sqrt{3})^k}{1-\sqrt{3}},$$
então $f(k+2) = 4f(k+1) - f(k)$. Agora mostre que $f(k) \in \mathbb{Z}$ e $(f(k))^2 = m$.)

52. Mostrar que o cubo de todo inteiro é a diferença de dois quadrados.

53. Mostrar que todo inteiro n pode ser escrito com uma soma de cinco cubos. (Sugestão: Note que
$$6q = (q+1)^3 + (q-1)^3 + (-q)^3 + (-q)^3, \forall q \in \mathbb{Z},$$
$6q + r - (6s + r)^3$ é divisível por 6 e $n = 6q + r$, onde $0 \leq r < 6$.)

54. Sejam $a_1, \ldots, a_n \in \mathbb{Z}$ com $a_i \neq 0$ para algum $i = 1, \ldots, n$. O máximo divisor comum de $a_1, \ldots, a_n$, em símbolos $\text{mdc}(a_1, \ldots, a_n)$, é um inteiro positivo d tal que

    (a) $d \mid a_i$ para $i = 1, \ldots, n$.

    (b) Se $c \mid a_i$ para $i = 1, \ldots, n$, então $c \mid d$.

    Mostrar que $d = \text{mdc}(a_1, \ldots, a_n)$ se, e somente se, d é o menor inteiro positivo tal que
    $$d = x_1 a_1 + \cdots + x_n a_n$$
    para alguns $x_i \in \mathbb{Z}$, com $i = 1, \ldots, n$.

55. Sejam $a, b, c \in \mathbb{Z}$. Mostrar que $\text{mdc}(a, b, c) = 1$ se, e somente se, existem $u_2, v_2, u_3, v_3, w_3 \in \mathbb{Z}$ tais que
$$\det\left(\begin{bmatrix} a & b & c \\ u_2 & v_2 & 0 \\ u_3 & v_3 & w_3 \end{bmatrix}\right) = \pm 1.$$

5.3 Teorema Fundamental da Aritmética

Um elemento $p \in \mathbb{Z}$ é chamado um *número primo* ou *primo* se as seguintes condições são satisfeitas:

1. p é não invertível ($p \neq \pm 1$).
2. Se $p = ab$ com $a, b \in \mathbb{Z}^*$, então $a = \pm 1$ ou $b = \pm 1$.

Um elemento $n \in \mathbb{Z}$ é chamado um *número composto* ou *composto* se as seguintes condições são satisfeitas:

1. n é não invertível ($n \neq \pm 1$).
2. $n = ab$ com $a, b \in \mathbb{Z}$ e $1 < |a| < |n|$, $1 < |b| < |n|$.

Como $-p$ é primo se, e somente se, p é primo, nos restringiremos apenas aos primos positivos. Por exemplo, 2, 3, 5, 7, 11 e 13 são números primos, enquanto 4, 6, 8, 9, 10, 12 e 14 são números compostos.

Teorema 5.32 *Se $a \in \mathbb{Z}$, com $|a| > 1$, então existe um número primo p que divide a.*

Prova. Podemos supor que $a > 1$, pois se $a < -1$, então $-a > 1$. Seja

$$X = \{a \in \mathbb{N} : a > 1 \text{ e } q \nmid a, \forall q \text{ primo}\}.$$

Então $X = \emptyset$, ao contrário, pelo Axioma 3.9, X contém um menor elemento $d > 0$. Como $d \mid d$ temos que d não pode ser um número primo. Logo, $d = bc$ com $1 < b, c < d$. Consequentemente, $b \notin X$ e, assim, existe um número primo p tal que $p \mid b$. Portanto, $p \mid d$ e $d \notin X$, o que é impossível. Assim, existe um número primo p que divide a. ■

Teorema 5.33 *Seja $a \in \mathbb{Z}$, com $|a| > 1$ um número composto. Então a contém um divisor primo p tal que $p \leq \sqrt{|a|}$.*

Prova. Podemos supor que $a > 1$, pois se $a < -1$, então $-a > 1$. Seja

$$X = \{a \in \mathbb{N} : a > 1 \text{ e } q \mid a \text{ para algum primo } q\}.$$

Então, pelo Teorema 5.32, $X \neq \emptyset$. Assim, pelo Axioma 3.9, X contém um menor divisor primo p. Logo, existe $b \in \mathbb{N}$ tal que $a = pb$. É claro que $p \leq b$ e, assim,

$$p^2 \leq pb = a,$$

isto é, $p \leq \sqrt{a}$. ■

Exemplo 5.34 *Seja $a = 1.998$. Então $\lfloor \sqrt{1.998} \rfloor = 44$. Assim, para encontrar um divisor primo de a é preciso experimentar com os primos menores do que ou iguais a 44. Não é difícil verificar que*

$$1.998 = 2.3^3.37.$$

Lema 5.35 *Sejam $a, b \in \mathbb{Z}^*$. Se p é um número primo e $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Prova. Suponhamos que $p \nmid a$. Então $\text{mdc}(p, a) = 1$, pois se $d = \text{mdc}(p, a)$, então $d \mid p$ e $d \mid a$. Como p é primo e $d \mid p$ temos que $d = p$ ou $d = 1$. A possibilidade $d = p$ não pode ocorrer. Logo, $d = 1$. Assim, pelo Lema 5.19, $p \mid b$. ■

Corolário 5.36 *Se p é um número primo e $p \mid p_1 p_2 \cdots p_n$, onde $p_1, p_2, \ldots, p_n$ são números primos, então $p = p_i$ para algum $i = 1, 2, \ldots, n$.* ■

Exemplo 5.37 *Sejam $a, b \in \mathbb{Z}^*$ tais que $mdc(a, b) = 1$. Determinar todos os possíveis valores de*

$$d = mdc(3a - b, 2a + b).$$

Solução. Suponhamos que $d > 1$ e seja p um número primo tal que $p \mid d$. Então existem $x, y \in \mathbb{Z}$ tais que

$$3a - b = px \text{ e } 2a + b = py$$

ou, equivalentemente,

$$5a = p(x + y) \text{ e } 5b = p(3y - 2x).$$

Logo,

$$p \mid 5 \text{ ou } p \mid a \text{ e } p \mid 5 \text{ ou } p \mid b$$

ou, equivalentemente,

$$p \mid 5 \text{ ou } (p \mid a \text{ e } p \mid b).$$

Como $\text{mdc}(a, b) = 1$ temos que $p \mid 5$, isto é, $p = 5$. Assim, 5 é o único número primo que divide d e a maior potência de 5 que o divide é $5^0 = 1$. Portanto,

$$\text{mdc}(3a - b, 2a + b) = 1 \text{ ou } 5.$$

Teorema 5.38 (Fundamental da Aritmética) *Todo $a \in \mathbb{Z} - \{-1, 0, 1\}$ pode ser escrito de modo único, a menos da ordem dos fatores, na forma*

$$a = up_1p_2 \cdots p_n,$$

onde $u = \pm 1$ e $p_1, p_2 \ldots, p_n$ são números primos.

Prova. (Existência) Basta mostrarmos o caso em que $a > 1$, pois se $a < -1$, então $-a > 1$. Seja

$$X = \{a \in \mathbb{N} : a > 1 \text{ e } a \neq p_1p_2 \cdots p_n\}.$$

Então $X = \emptyset$. Caso contrário, pelo Axioma 3.9, X contém um menor elemento $b > 1$ e b não é um produto de números primos. Pelo Teorema 5.32, $b = pc$ para algum número primo p. Como $c < b$ temos que $c \notin X$, logo,

$$c = p_1p_2 \cdots p_n \text{ ou } c = 1.$$

Assim,

$$b = pp_1p_2 \cdots p_n \text{ ou } b = p.$$

Portanto, b é um produto de primos, o que é impossível.

(Unicidade) Suponhamos que exista $a > 1$ tal que

$$a = p_1p_2 \cdots p_m \text{ e } a = q_1q_2 \cdots q_n.$$

Então

$$p_1 \mid q_1q_2 \cdots q_n$$

e, pelo Corolário 5.36, temos que $p_1 = q_i$ para algum $i = 1, 2, \ldots, n$. Reindexando, se necessário, de modo que $p_1 \mid q_1$. Como q_1 é um número primo temos que $p_1 = q_1$. Logo, pela lei do cancelamento,

$$p_2p_3 \cdots p_m = q_2q_3 \cdots q_n$$

Agora, vamos usar indução sobre o $\max\{m, n\}$.

Se $m > n$, então

$$p_{n+1}p_{n+2}\cdots p_m = 1,$$

o que é impossível. Se $m < n$, então

$$1 = q_{m+1}q_{m+2}\cdots q_n,$$

o que é impossível. Portanto, $m = n$ e a seqüência $p_2, p_3, \ldots, p_n$ é no máximo uma re-ordenação da seqüência $q_2, q_3, \ldots, q_n$. ■

Corolário 5.39 *Todo $a \in \mathbb{Z} - \{-1, 0, 1\}$ pode ser escrito de modo único na forma*

$$a = up_1^{r_1}p_2^{r_2}\cdots p_n^{r_n},$$

onde $u = \pm 1$, $p_1 < p_2 < \cdots < p_n$ são números primos e $r_i \in \mathbb{N} \cup \{0\}$. ■

Embora o Teorema Fundamental da Aritmética assegure a existência da fatoração de um número inteiro $a \in \mathbb{Z} - \{-1, 0, 1\}$, a sua demonstração não diz como achar a sua fatoração. Agora, apresentaremos um **Algoritmo** (fatoração de Fermat), para determinar a fatoração de um número composto $a \in \mathbb{N}$.

Dado $a \in \mathbb{N}$ composto, então podemos sempre escrevê-lo na forma

$$a = 2^r b,$$

onde b é um número ímpar e $r \in \mathbb{N} \cup \{0\}$. Se b é um número primo, então nada há para fazer. Se b é um número composto, então faça iterativamente os seguintes passos:

1.^{o} Passo. Faça $m = \lfloor \sqrt{b} \rfloor$.

2.^{o} Passo. Se $m^2 - b = n^2$, então $b = (m - n)(m + n)$.

3.^{o} Passo. Se $m^2 - b \neq n^2$, então soma 1 a m e volte para 2.

O número de iterações deste Algoritmo é finito, pois se $b = rs$, então

$$b = \left(\frac{r+s}{2}\right)^2 - \left(\frac{r-s}{2}\right)^2.$$

Exemplo 5.40 *Obtenha a fatoração do número* 8.415.

Solução. É claro que 8.415 é um número ímpar, assim, seja $m = \lfloor \sqrt{8.415} \rfloor = 91$. Então

$$m^2 - 8.415 = -134 \Rightarrow m^2 - 8.415 \neq n^2.$$

Assim,

$$(m+1)^2 - 8.415 = 49 = 7^2.$$

Logo,

$$8.415 = 92^2 - 7^2 = (92 - 7)(92 + 7) = 85 \cdot 99.$$

Agora, repete o Algoritmo com 85 e 99, para obter a fatoração

$$8.415 = 3^2 \cdot 5 \cdot 11 \cdot 17$$

Note que, se $a \in \mathbb{N}$ e $a = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$ é sua fatoração em fatores primos distintos com $r_i > 0$, então todo divisor b de a é da forma $b = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$, onde $0 \leq s_i \leq r_i$.

De fato, suponhamos que b divide a. Então existe $c \in \mathbb{Z}$ tal que $a = bc$ e, portanto, todos os divisores primos de b aparecem na decomposição de a com expoentes não menores que os expoentes com que eles mesmos aparecem na decomposição de b. Logo, b é da forma acima.

Assim, para cada i, os possíveis valores de s_i são $0, 1, \ldots, r_i$, isto é, existem $r_i + 1$ possibilidades para s_i. Portanto, a possui

$$(r_1 + 1) \cdots (r_n + 1)$$

divisores.

Lema 5.41 *Sejam $a, b \in \mathbb{N}$ tais que $mdc(a, b) = 1$. Se ab é um quadrado perfeito, então a e b também o são.*

Prova. Seja $p \in \mathbb{N}$ qualquer número primo tal que $p \mid a$. Então existe $r \in \mathbb{N}$ tal que $p^r \mid a$ e $p^{r+1} \nmid a$. Como $\text{mdc}(a, b) = 1$ temos que $p^r \nmid b$ e, assim, $p^r \mid ab$ e $p^{r+1} \nmid ab$. Logo, pela hipótese, r é um número par. Portanto, a é um quadrado perfeito. De modo análogo, mostra-se que b é um quadrado perfeito. ■

Lema 5.42 *Seja $q \in \mathbb{Q}^*$. Então $q = \frac{a}{b}$, onde $mdc(a, b) = 1$.*

Prova. Suponhamos que $q = \frac{a}{b}$ e $\text{mdc}(a, b) = d$. Se $d = 1$ nada há para provar. Se $d > 1$, então existem $r, s \in \mathbb{Z}$ tais que $a = dr$ e $b = ds$. Como existem $x, y \in \mathbb{Z}$ tais que

$$ax + by = d$$

temos que

$$ax + by = d \Rightarrow drx + dsy = d \Rightarrow rx + sy = 1.$$

Logo, $\text{mdc}(r, s) = 1$. Portanto,

$$q = \frac{r}{s},$$

onde $\text{mdc}(r, s) = 1$. ■

Exemplo 5.43 *Mostrar que $\sqrt{p}$ é um número irracional para todo número primo p.*

Solução. Suponhamos, por absurdo, que $\sqrt{p}$ seja um número racional. Então

$$\sqrt{p} = \frac{a}{b},$$

onde $\text{mdc}(a,b) = 1$. Logo, $a^2 = pb^2$ e, assim, $b \mid a^2$. Se $b > 1$, então, pelo Teorema 5.32, existe um número primo q tal que $q \mid b$. Logo, $q \mid a^2$ e, portanto, $q \mid a$, o que é impossível, pois $\text{mdc}(a,b) = 1$. Portanto, $b = 1$ e $a^2 = p$, o que é uma contradição, pois se $a = p_1 p_2 \cdots p_m$, então

$$p = p_1^2 p_2^2 \cdots p_m^2$$

o que implica que no membro da direita cada fator primo aparece um número par de vezes, no entanto o da esquerda o fator primo p somente aparece um número ímpar de vezes.

Teorema 5.44 *Se $a \in \mathbb{N}$ com $a > 2$, então entre a e $a!$ existe pelo menos um número primo p.*

Prova. Seja $b = a! - 1$. Então $b > 1$, pelo Teorema 5.32, existe um número primo p tal que $p \mid b$. Claramente, $p \leq b < a!$. Suponhamos que $p \leq a$. Então p é um dos fatores do produto $1 \cdot 2 \cdot 3 \cdots a = a!$ e, assim, $p \mid a!$. Logo, $p \mid (a! - b)$, isto é, $p \mid 1$, o que é impossível. Portanto, $a < p < a!$. ■

Corolário 5.45 (Euclides) *O conjunto dos números primos é infinito.*

Prova. Suponhamos, por absurdo, que exista um número finito de primos, digamos

$$p_1, p_2, \ldots, p_m.$$

Seja $a = p_1 p_2 \cdots p_m + 1$. Então $a > 2$ e, pelo Teorema 5.44, existe um número primo p tal que $p > a$. Portanto,

$$p \neq p_i, \forall i = 1, 2, \ldots, m,$$

o que é uma contradição. ■

Exemplo 5.46 *Seja $n \in \mathbb{N}$. Mostrar que o conjunto dos números primos da forma $4n+3$ é infinito.*

Solução. Suponhamos, por absurdo, que exista um número finito de primos, digamos

$$7, 11, \ldots, p_m.$$

Seja $a = 4(7 \cdot 11 \cdots p_m) + 3$. Como todo número primo ímpar é da forma $4r + 1$ ou $4r + 3$ e

$$(4r + 1)(4r + 1) = 4(4r^2 + 2r) + 1 = 4s + 1$$

temos que existe um número primo p da forma $4n + 3$ tal que $p \mid a$. É fácil verificar que $p \neq 7, 11$ e p_i, o que é uma contradição.

EXERCÍCIOS

1. Verificar se 38.567 é um número primo.

2. Sejam $n \in \mathbb{N}$ e p um número primo. Mostrar que se p divide a^n, então p^n divide a^n.

3. Mostrar que se $n \in \mathbb{N}$ e $n > 1$, então existem n números compostos consecutivos.(Sugestão: Veja o exercício 17 da Seção 5.1)

4. Seja $n \in \mathbb{N}$. Mostrar que $n = ab^2$, onde a não é um quadrado (livre de quadrados), isto é, não existe $x \in \mathbb{N}$ tal que $x^2 = a$.

5. Mostrar que:

   (a) Se r é raiz da equação $10^r = 2$, então r é irracional.

   (b) Se $n \in \mathbb{N}$ não é um quadrado, então $\sqrt{n}$ é irracional.

   (c) Se $\sqrt{n}$ é racional, então $\sqrt{n}$ é inteiro.

6. Mostrar que p é um número primo se, e somente se, p possui exatamente dois divisores.

7. Mostrar que $n^4 + 4$ é um número composto para todo $n \in \mathbb{N}$, com $n > 1$.

8. Mostrar que $n^4 + n^2 + 1$ é um número composto para todo $n \in \mathbb{N}$, com $n > 1$.

9. Seja $a \in \mathbb{N}$, com $a > 1$. Mostrar que $a^{4n} + a^{2n} + 1$ é um número composto para todo $n \in \mathbb{N}$.

10. Sejam $a, b \in \mathbb{Z}$. Mostrar que se $\text{mdc}(a, b) = 1$, então $\text{mdc}(a^2, ab, b^2) = 1$.

11. Mostrar que:

    (a) $\text{mdc}(a + 2b, 4a + 9b) = \text{mdc}(a, b - a), \forall a, b \in \mathbb{Z}^*$.

    (b) $\text{mdc}(a, b) = 1 \Leftrightarrow \text{mdc}(a^2 + ab + b^2, a^2 - ab + b^2) = 1, \forall a, b \in \mathbb{Z}^*$.

12. Mostrar que $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por

$$f((m, n)) = 2^{m-1}(2n - 1)$$

    é uma correspondência biunívoca.

13. Seja $p_0, p_1, \ldots$ uma enumeração de todos os números primos. Mostrar que

$$f : \mathbb{Z}[x] \to \mathbb{Q}_+^* \text{ dada por } f(a_0 + a_1x + \cdots + a_nx^n) = p_0^{a_0}p_1^{a_1} \cdots p_n^{a_n}$$

    é bijetora.

14. Defina uma função sobrejetora $f : \mathbb{N} \to \mathbb{N}$ tal que, para cada $k \in \mathbb{N}$, o conjunto $f^{-1}(k)$ seja infinito. (Sugestão: Seja $n \in \mathbb{N}$. Então n pode ser escrito de modo único sob a forma $n = 2^{k-1}m$, onde $k, m \in \mathbb{N}$ com m um número ímpar. Defina $f : \mathbb{N} \to \mathbb{N}$ por $f(n) = k$. Agora mostre que f tem as propriedades desejadas.)

15. Obtenha uma decomposição
$$\mathbb{N} = \bigcup_{n=1}^{\infty} A_n$$
tal que os conjuntos A_n sejam infinitos e $A_m \cap A_n = \emptyset$ para $m \neq n$.

16. Se $2^n - 1$ é um número primo, então n também o é.

17. Seja p é um número primo. Então $p = x^3 - y^3$ se, e somente se, $p = 3n(n-1) + 1$.

18. Seja $n \in \mathbb{N}$. Mostrar que o conjunto dos números primos da forma $6n + 5$ é infinito.

19. Mostrar que:

    (a) Se p e $8p - 1$ são ambos números primos, então $8p + 1$ é um número composto. (Sugestão: Se $p = 3$, então $8p - 1 = 23$ é primo e $8p + 1 = 25$ é composto. Se $p > 3$, então o resto da divisão de p por 3 é igual a 1 ou 2. Agora, mostre que o resto não pode ser igual a 2, continue.)

    (b) Se p e $8p^2 + 1$ são ambos números primos, então $8p^2 - 1$ é um número primo.

20. Determinar todos os pares $a, b \in \mathbb{N}$ tais que
$$\frac{ab}{a+b} = p,$$
onde p é um número primo. (Sugestão: Note que
$$ab - pa - pb = 0 \Rightarrow ab - pa - pb + p^2 = p^2 \Rightarrow (a-p)(b-p) = p^2.)$$

21. Seja $n \in \mathbb{N}$, com $n > 1$ e ímpar. Então n é um número primo se, e somente se, n pode ser escrito de modo único como a diferença de dois quadrados.

22. Sejam $a, b \in \mathbb{N}$ tais que $\text{mdc}(a, b) = 1$ e $n = ab$. Mostrar que existem $r, s \in \mathbb{N}$ tais que
$$\frac{m}{n} = \frac{r}{a} + \frac{s}{b}.$$

23. Sejam $a, b \in \mathbb{N}$ e $a = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$ sua fatoração em fatores primos distintos e $r_i > 0$ para todo i. Mostrar que existem $b_1, b_2, \ldots, b_n \in \mathbb{N}$ tais que
$$\frac{b}{a} = \frac{b_1}{p_1^{r_1}} + \frac{b_2}{p_2^{r_2}} + \cdots + \frac{b_n}{p_n^{r_n}}.$$

24. Mostrar que se $a^n - 1$, com $a, n \in \mathbb{N}$ e $a > 1$, é um número primo, então $a = 2$ e n é um número primo.

25. Mostrar que se $a^n + 1$, com $n \in \mathbb{N}$ e $a > 1$, é um número primo, então a é par e n é uma potência de 2.

26. Sejam $m, n \in \mathbb{N}$, com $m > 1$ e $n > 1$. Mostrar que se $m^4 + 4^n$ é primo, então m é par e n é ímpar.

27. Mostrar que não existem $m, n \in \mathbb{N}$ tais que $n^2 + (n+1)^2 = m^3$.

28. Mostrar que quaisquer dois números da seqüência $x_1, \ldots, x_n, \ldots$, onde

$$x_n = 2^{2^{n-1}} + 1,$$

são primos entre si. Conclua que existem infinitos primos. (Sugestão: Mostre que

$$2^{2^{n-1}} - 1 = (2^{2^{n-1}} + 1) - 2$$

é divisível por $x_1, \ldots, x_{n-1}$, isto implica que $\text{mdc}(2, x_i) = 1$, para cada $i = 1, \ldots, n$).

29. Seja $n \in \mathbb{N}$. Mostrar que $2^{2^n} + 1$ pode ser escrito como uma soma de dois quadrados.

30. Existem números inteiros m e n tais que $m^2 = n^2 + 1.998$?

31. Mostrar que não existem números inteiros a, b e c tais que

$$a^2 + b^2 - 8c = 6.$$

32. Mostrar que não existe um número primo p tal que

$$p^m = 2^n - 1,$$

onde $m, n \in \mathbb{N}$.

33. Mostrar que existe um número infinito de polinômios mônicos irredutíveis em $F[x]$, onde F é um corpo qualquer. (Um polinômio f chama-se irredutível se as seguintes condições são satisfeitas:

    (a) $f \notin F$ $(\partial(f) \geq 1)$.

    (b) Se $f = g \cdot h$, então $g \in F$ ou $h \in F$.)

34. Determinar o máximo divisor comum de cada um dos seguintes pares de polinômios sobre o corpo $\mathbb{Q}$

    (a) $x + 2$ e $x^2 + 8x + 16$.

    (b) $2x^5 - x^3 - 3x^2 - 6x + 4$ e $x^4 + x^3 - x^2 - 2x - 2$.

(c) $3x^4 + 8x^2 - 3$ e $x^3 + 2x^2 + 3x + 6$.

(d) $x^4 - 2x^3 - 2x^2 - 2x - 3$ e $x^3 + 6x^2 + 7x + 1$.

35. Sejam $f = 2x + 1, g = x^2 + x + 1 \in \mathbb{Z}[x]$. Mostrar que existem $r, s \in \mathbb{Z}[x]$ tais que

$$rf + sg = 1$$

mas $\text{mdc}(f, g)$ não existe.

36. Sejam F é um corpo qualquer, $a_1, a_2, \ldots, a_n$ elementos distintos de F e $b_1, b_2, \ldots, b_n$ elementos de F. Sejam

$$f = \prod_{i=1}^{n}(x - a_i), \;\; \widehat{f_i} = \frac{f}{f_i}, \;\; i = 1, \ldots, n, \;\; \text{e} \;\; g = \sum_{i=1}^{n} \frac{\widehat{f_i}}{\widehat{f_i}(a_i)} b_i.$$

Mostrar que:

(a) $g(a_i) = b_i$, $i = 1, \ldots, n$. O polinômio g é chamado de *fórmula de interpolação de Lagrange*.

(b) O $\text{mdc}(f_i, \widehat{f_i}) = 1$.

37. Mostrar que não existe polinômio com coeficientes inteiros tais que $f(1) = 2$, $f(2) = 3$ e $f(3) = 5$.

38. Sejam $a, b \in \mathbb{N}$ e $a = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$ sua fatoração em fatores primos distintos e $r_i > 0$ para todo i. Mostrar que:

(a) Se $d(a)$ denota o número de divisores distintos de a, então

$$d(a) = (r_1 + 1)(r_2 + 1) \cdots (r_n + 1).$$

(b) Se $\text{mdc}(a, b) = 1$, então $d(ab) = d(a)d(b)$.

(c) Mostrar que a é um quadrado perfeito se, e somente se, $d(a)$ é ímpar.

(d) Se $s(a)$ denota a soma dos divisores distintos de a, então

$$s(a) = \left(\frac{p_1^{r_1+1} - 1}{p_1 - 1}\right)\left(\frac{p_2^{r_2+1} - 1}{p_2 - 1}\right) \cdots \left(\frac{p_n^{r_n+1} - 1}{p_n - 1}\right).$$

(Sugestão: Note que

$$s(p^n) = 1 + p + p^2 + \cdots + p^n = \frac{p^{n+1} - 1}{p - 1}.)$$

39. Sejam $a, b \in \mathbb{N}$ e $d = \text{mdc}(a, b)$. Mostrar que se ab é um quadrado perfeito, então existem $r, s \in \mathbb{N}$ tais que

$$a = dr^2 \;\; \text{e} \;\; b = ds^2.$$

40. Seja $n \in \mathbb{N}$. Mostrar que se n não é um quadrado perfeito, então não existem $a, b \in \mathbb{N}$ tais que
$$a = b\sqrt{n}$$

41. Um número $n \in \mathbb{N}$, com $n > 1$, é *perfeito* se a soma de seus divisores é igual a $2n$. Mostrar que se o número $2^n - 1$ é primo, então o número $2^{n-1}(2^n - 1)$ é perfeito.

42. Sejam $p_1, p_2, \ldots, p_n$ os n primeiros números primos. Determinar o menor n tal que $a = p_1 p_2 \cdots p_n + 1$ é um número composto.

43. Determinar o menor n tal que n, $n+1$, $n+2$, $n+3$, $n+4$, $n+5$ são todos números compostos.

44. Se p_n denota o n-ésimo número primo, isto é, $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$, então $p_{n+1} \leq p_n^n + 1$. (Sugestão: Mostre que $p_1 p_2 \cdots p_n + 1 \leq p_n^n + 1$.)

45. Se p_n denota o n-ésimo número primo, então
$$p_n \leq 2^{2^{n-1}}.$$
(Sugestão: Mostre que $p_{n+1} \leq p_1 p_2 \cdots p_n + 1$.)

46. Sejam $a, b \in \mathbb{N}$, $a = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$ e $b = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$ suas fatorizações em fatores primos distintos, com $r_i \geq 0, s_i \geq 0$ para todo i. Mostrar que:

    (a) $\text{mdc}(a, b) = p_1^{u_1} p_2^{u_2} \cdots p_n^{u_n}$, onde $u_i = \min\{r_i, s_i\}$.

    (b) $\text{mmc}(a, b) = p_1^{v_1} p_2^{v_2} \cdots p_n^{v_n}$, onde $v_i = \max\{r_i, s_i\}$.

    Conclua que $\text{mdc}(a, b) = 1$ se, e somente se, $r_i s_i = 0$ para todo i.

Capítulo 6

Aritmética Modular

Neste capítulo apresentaremos a definição de congruência módulo $n \in \mathbb{N}$ e os Teoremas Chinês dos Restos, de Fermat e de Euler. O leitor interessado em mais detalhes pode consultar [**?**].

6.1 Congruências

Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Dizemos que a e b são *congruentes módulo* n, em símbolos $a \equiv b \,(\mathrm{mod}\, n)$, quando $a - b$ é divisível por n. Caso contrário, dizemos que a *não é congruente a* b *módulo* n e denotaremos por $a \not\equiv b \,(\mathrm{mod}\, n)$.

Exemplo 6.1 $9^4 \equiv 1 \,(\mathrm{mod}\, 5)$*, pois*

$$9^4 - 1 = (9^2 - 1)(9^2 + 1) = 5 \cdot 1.312.$$

Teorema 6.2 *Sejam* $a, b \in \mathbb{Z}$ *e* $n \in \mathbb{N}$*. Então* $a \equiv b \,(\mathrm{mod}\, n)$ *se, e somente se,* a *e* b *possuem o mesmo resto quando divididos por* n*.*

Prova. Suponhamos que $a \equiv b \,(\mathrm{mod}\, n)$. Então existe $k \in \mathbb{Z}$ tal que

$$a - b = kn.$$

Agora, pelo Teorema 5.1, podemos encontrar $q, r \in \mathbb{Z}$ tais que

$$b = qn + r, \text{ onde } 0 \leq r < n.$$

Logo,

$$a = b + kn = (q + k)n + r, \text{ onde } 0 \leq r < n.$$

Portanto, a e b possuem o mesmo resto quando divididos por n.

Reciprocamente, suponhamos que

$$a = q_1 n + r \text{ e } b = q_2 n + r, \text{ onde } 0 \leq r < n.$$

Então

$$a - b = (q_1 - q_2)n,$$

isto é, n divide $a - b$. Portanto, $a \equiv b \pmod{n}$. ■

Teorema 6.3 *Sejam $a, b, c, d, x \in \mathbb{Z}$ e $n \in \mathbb{N}$. Então as seguintes condições são satisfeitas*:

1. $a \equiv a \pmod{n}$.
2. *Se* $a \equiv b \pmod{n}$, *então* $b \equiv a \pmod{n}$.
3. *Se* $a \equiv b \pmod{n}$ *e* $b \equiv c \pmod{n}$, *então* $a \equiv c \pmod{n}$.
4. *Se* $a \equiv b \pmod{n}$ *e* $c \equiv d \pmod{n}$, *então*

$$a + c \equiv b + d \pmod{n} \ \text{ e } \ ac \equiv bd \pmod{n}.$$

5. *Se* $a \equiv b \pmod{n}$, *então* $ax \equiv bx \pmod{n}$.
6. *Se* $a \equiv b \pmod{n}$ *e* $c \equiv d \pmod{n}$, *então*

$$ax \equiv c \pmod{n} \Leftrightarrow bx \equiv d \pmod{n}.$$

7. *Se* $a \equiv b \pmod{n}$, *então* $a^k \equiv b^k \pmod{n}$, $\forall\ k \in \mathbb{N}$.

Prova. Provaremos apenas os itens (4) e (7). Suponhamos que $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$. Então existem $x, y \in \mathbb{Z}$ tais que

$$a - b = xn \ \text{ e } \ c - d = yn.$$

Logo,

$$(a + c) - (b + d) = (a - b) + (c - d) = (x + y)n,$$

isto é, $a + c \equiv b + d \pmod{n}$.

$$ac - bd = (b + xn)(d + yn) - bd = (by + dx + xyn)n,$$

isto é, $ac \equiv bd \pmod{n}$. Agora, vamos provar (7), suponhamos que $a \equiv b \pmod{n}$ e seja

$$X = \{k \in \mathbb{N} : a^k \equiv b^k \pmod{n}\}.$$

Então:

1. $1 \in X$.
2. Suponhamos, como hipótese de indução, que o resultado seja válido para algum $k > 1$, isto é, $k \in X$.

Como $a \equiv b \,(\mathrm{mod}\, n)$ e $a^k \equiv b^k \,(\mathrm{mod}\, n)$ temos, pelo item 4, que $a^{k+1} \equiv b^{k+1} \,(\mathrm{mod}\, n)$. Logo, $k+1 \in X$. Portanto, $X = \mathbb{N}$. ■

Exemplo 6.4 *Mostrar que é divisível* $2.222^{5.555} + 5.555^{2.222}$ *por* 3.

Solução. Como $2.222 = 740 \cdot 3 + 2$ e $5.555 = 1.851 \cdot 3 + 2$ temos que

$$2.222 \equiv 2 \,(\mathrm{mod}\, 3) \text{ e } 5.555 \equiv 2 \,(\mathrm{mod}\, 3).$$

Sendo $2 \equiv -1 \,(\mathrm{mod}\, 3)$ temos, pelo item (3) do Teorema 6.3, que

$$2.222 \equiv -1 \,(\mathrm{mod}\, 3) \text{ e } 5.555 \equiv -1 \,(\mathrm{mod}\, 3).$$

Assim, pelo item (7) do Teorema 6.3,

$$2.222^{5.555} \equiv -1 \,(\mathrm{mod}\, 3) \text{ e } 5.555^{2.222} \equiv 1 \,(\mathrm{mod}\, 3).$$

Portanto, pelo item (4) do Teorema 6.3,

$$2.222^{5.555} + 5.555^{2.222} \equiv 0 \,(\mathrm{mod}\, 3).$$

As condições (1), (2) e (3) do Teorema 6.3 mostram que a relação de congruência é uma relação de equivalência, sendo a classe de equivalência de $a \in \mathbb{Z}$ módulo n dada por

$$\begin{aligned} \overline{a} &= \{b \in \mathbb{Z} : b \equiv a \,(\mathrm{mod}\, n)\} \\ &= \{a + kn : k \in \mathbb{Z}\} \\ &= a + \mathbb{Z}n. \end{aligned}$$

Agora, para todo $a \in \mathbb{Z}$ temos, pelo Teorema 5.1, que existem $q, r \in \mathbb{Z}$ tais que

$$a = qn + r \text{ onde } 0 \leq r < n.$$

Então qualquer $a \in \mathbb{Z}$ é congruente módulo n a um dos elementos

$$\overline{0}, \overline{1}, \ldots, \overline{n-1}.$$

Além disso, esses elementos são todos distintos. De fato: se $\overline{i} = \overline{j}$, com $0 \leq i \leq j < n$, então

$$j \equiv i \,(\mathrm{mod}\, n) \Leftrightarrow n \mid j - i \Rightarrow j - i = 0 \Rightarrow j = i,$$

pois, $0 \leq j - i < n$. Portanto, o conjunto quociente

$$\mathbb{Z}_n = \frac{\mathbb{Z}}{\equiv} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Note que a função $f : \mathbb{Z} \to \mathbb{Z}_n$ definida por $f(a) = \overline{a}$ é sempre sobrejetora.

Agora vamos considerar as operações de adição e multiplicação no conjunto quociente $\mathbb{Z}_n$. Uma *operação binária* sobre $\mathbb{Z}_n$ é qualquer função de $\mathbb{Z}_n \times \mathbb{Z}_n$ em $\mathbb{Z}_n$. Dados $\overline{a}, \overline{b} \in \mathbb{Z}_n$, vamos definir em $\mathbb{Z}_n$ as seguintes operações binárias:

$$\overline{a} \oplus \overline{b} = \overline{a+b} \text{ e } \overline{a} \odot \overline{b} = \overline{ab}.$$

Assim, pelo item (4) do Teorema 6.3, essas operações estão bem definidas, isto é,

$$\overline{a} = \overline{c} \text{ e } \overline{b} = \overline{d} \Rightarrow \overline{a+b} = \overline{c+d} \text{ e } \overline{ab} = \overline{cd}.$$

Essas operações satisfazem quase todas as propriedades das operações usuais de adição e multiplicação em $\mathbb{Z}$.

1. $(\overline{a} \oplus \overline{b}) \oplus \overline{c} = \overline{a} \oplus (\overline{b} \oplus \overline{c})$, $\forall\ \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$, pois

$$\begin{aligned}(\overline{a} \oplus \overline{b}) \oplus \overline{c} &= \overline{(a+b)} \oplus \overline{c} = \overline{(a+b)+c} \\ &= \overline{a+(b+c)} = \overline{a} \oplus \overline{(b+c)} = \overline{a} \oplus (\overline{b} \oplus \overline{c}).\end{aligned}$$

2. Existe $\overline{0} \in \mathbb{Z}_n$ tal que $\overline{a} \oplus \overline{0} = \overline{0} \oplus \overline{a} = \overline{a}$, $\forall\ \overline{a} \in \mathbb{Z}_n$, pois

$$\overline{a} \oplus \overline{0} = \overline{a+0} = \overline{a}.$$

3. Para cada $\overline{a} \in \mathbb{Z}_n$ existe $\overline{(-a)} \in \mathbb{Z}_n$ tal que $\overline{a} \oplus \overline{(-a)} = \overline{(-a)} \oplus \overline{a} = \overline{0}$, pois

$$\overline{a} \oplus \overline{(-a)} = \overline{a+(-a)} = \overline{0}.$$

4. $\overline{a} \oplus \overline{b} = \overline{b} \oplus \overline{a}$, $\forall\ \overline{a}, \overline{b} \in \mathbb{Z}_n$, pois

$$\overline{a} \oplus \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} \oplus \overline{a}.$$

5. $(\overline{a} \odot \overline{b}) \odot \overline{c} = \overline{a} \odot (\overline{b} \odot \overline{c})$, $\forall\ \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$, pois

$$\begin{aligned}(\overline{a} \odot \overline{b}) \odot \overline{c} &= \overline{(ab)} \odot \overline{c} = \overline{(ab)c} \\ &= \overline{a(bc)} = \overline{a} \odot \overline{(bc)} = \overline{a} \odot (\overline{b} \odot \overline{c}).\end{aligned}$$

6. Existe $\overline{1} \in \mathbb{Z}_n$ tal que $\overline{a} \odot \overline{1} = \overline{1} \odot \overline{a} = \overline{a}$, $\forall\ \overline{a} \in \mathbb{Z}_n$, pois

$$\overline{a} \odot \overline{1} = \overline{a1} = \overline{a}.$$

7. $\overline{a} \odot \overline{b} = \overline{b} \odot \overline{a}$, $\forall\ \overline{a}, \overline{b} \in \mathbb{Z}_n$, pois

$$\overline{a} \odot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \odot \overline{a}.$$

8. $(\overline{a} \oplus \overline{b}) \odot \overline{c} = \overline{a} \odot \overline{c} \oplus \overline{b} \odot \overline{c}$, $\forall\ \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$, pois

$$\begin{aligned}(\overline{a} \oplus \overline{b}) \odot \overline{c} &= \overline{(a+b)} \odot \overline{c} = \overline{(a+b)c} \\ &= \overline{ac+bc} = \overline{ac} \oplus \overline{bc} = \overline{a} \odot \overline{c} \oplus \overline{b} \odot \overline{c}.\end{aligned}$$

A lei do cancelamento não vale, em geral, em $\mathbb{Z}_n$. Por exemplo,

$$14 \equiv 8 \,(\mathrm{mod}\, 6) \text{ mas } 7 \not\equiv 4 \,(\mathrm{mod}\, 6).$$

Mas temos o seguinte:

Teorema 6.5 *Sejam $a, b, c \in \mathbb{Z}$. Se $ac \equiv bc \,(\mathrm{mod}\, n)$ e $mdc(c, n) = 1$, então $a \equiv b \,(\mathrm{mod}\, n)$.*

Prova. Se $ac \equiv bc \,(\mathrm{mod}\, n)$, então $n \mid (a-b)c$. Como $\mathrm{mdc}(c, n) = 1$ temos, pelo Lema 5.19, que $n \mid (a-b)$. Portanto, $a \equiv b \,(\mathrm{mod}\, n)$. ■

Teorema 6.6 *Seja $f(x)$ um polinômio com coeficientes inteiros. Se $a \equiv b \,(\mathrm{mod}\, n)$, então $f(a) \equiv f(b) \,(\mathrm{mod}\, n)$.*

Prova. Seja

$$f(x) = r_m x^m + r_{m-1} x^{m-1} + \cdots + r_1 x + r_0,$$

com $r_i \in \mathbb{Z}$. Pelos itens (5) e (7) do Teorema 6.3, temos que

$$r_{m-i} a^{m-i} \equiv r_{m-i} b^{m-i} \,(\mathrm{mod}\, n), \forall \; i = 0, 1, \ldots, m.$$

Assim, somando membro a membro, obtemos $f(a) \equiv f(b) \,(\mathrm{mod}\, n)$. ■

Dizemos que a é *solução* ou *raiz* da congruência $f(x) \equiv 0 \,(\mathrm{mod}\, n)$ se $f(a) \equiv 0 \,(\mathrm{mod}\, n)$. Assim, se $a \equiv b \,(\mathrm{mod}\, n)$ e a é solução da congruência $f(x) \equiv 0 \,(\mathrm{mod}\, n)$, então b também o é, pois

$$f(b) \equiv f(a) \equiv 0 \,(\mathrm{mod}\, n).$$

A teoria das congruências é uma ferramenta poderosa para evidenciar certas regras práticas, tais como "critérios de divisibilidades." É bem conhecido que quando a soma dos dígitos da representação decimal de um número r é um múltiplo de 3, então r também é um múltiplo de 3. Formalmente temos:

Exemplo 6.7 *Sejam*

$$r = r_m 10^m + r_{m-1} 10^{m-1} + \cdots + r_1 10 + r_0$$

a representação decimal de $r > 1$, onde $0 \leq r_i < 10$, e

$$s = r_m + r_{m-1} + \cdots + r_1 + r_0.$$

Então $3 \mid r$ se, e somente se, $3 \mid s$.

Solução. Seja

$$f(x) = r_m x^m + r_{m-1} x^{m-1} + \cdots + r_1 x + r_0.$$

Então $r = f(10)$ e $s = f(1)$. Como $10 \equiv 1 \,(\mathrm{mod}\, 3)$ temos que $f(10) \equiv f(1) \,(\mathrm{mod}\, 3)$. Portanto, $f(10) \equiv 0 \,(\mathrm{mod}\, 3)$ se, e somente se, $f(1) \equiv 0 \,(\mathrm{mod}\, 3)$, isto é, $3 \mid r$ se, e somente se, $3 \mid s$.

EXERCÍCIOS

1. Mostrar que, para todo $a \in \mathbb{Z}$, $a^2 \equiv 0 \pmod 4$ ou $a^2 \equiv 1 \pmod 4$.
2. Mostrar que, para todo $a \in \mathbb{Z}$, $a^2 \equiv 0 \pmod 8$, $a^2 \equiv 1 \pmod 8$ ou $a^2 \equiv 4 \pmod 8$.
3. Mostrar que $a \equiv 1 \pmod 4$ ou $a \equiv -1 \pmod 4$, para todo $a \in \mathbb{Z}$ ímpar.
4. Mostrar que $2^{70} + 3^{70} \equiv 0 \pmod{13}$.
5. Determinar o dígito das unidades de 3^{98}.
6. Determinar o último dígito de cada um dos seguintes números 7^{7^7} e 9^{9^9}.
7. Determinar o resto da divisão de $7.812^{384} + 5.770^{23} + 3.572^8$ por 9.
8. Determinar o resto da divisão de $10^{10} + 10^{10^2} + \cdots + 10^{10^{10}}$ por 7.
9. Determinar o resto da divisão de $1! + 2! + \cdots + 100!$ por 12. (Sugestão: Se $n \geq 4$, então

$$n! = n \cdot (n-1) \cdots 6 \cdot 5 \cdot 4! \equiv n \cdot (n-1) \cdots 6 \cdot 5 \cdot 0 \equiv 0 \pmod{12},$$

pois $4! = 24 \equiv 0 \pmod{12}$.)

10. Mostrar que:
    (a) $3^{1.000} - 4$ é divisível por 7.
    (b) $2.222^{5.555} + 5.555^{2.222}$ é divisível por 7.
    (c) $2.222^{5.555} + 5.555^{2.222}$ é divisível por 11.
    (d) $2.222^{5.555} + 5.555^{2.222}$ é divisível por 231.
    (e) $\sqrt{327^{328} + 329^{330}}$ é irracional.
11. Mostrar que se $a \equiv -1 \pmod 4$ e $b \equiv 1 \pmod 4$, então $\sqrt{a^{2k} + b^m}$ é irracional, $\forall\ k, m \in \mathbb{N}$.
12. Seja

$$r = r_m 10^m + r_{m-1} 10^{m-1} + \cdots + r_1 10 + r_0$$

a representação decimal de $r > 1$, onde $0 \leq r_i < 10$. Mostrar que:
    (a) $2 \mid r$ se, e somente se, r_0 é par.
    (b) $4 \mid r$ se, e somente se, $4 \mid (2r_1 + r_0)$.
    (c) $5 \mid r$ se, e somente se, $r_0 = 0$ ou $r_0 = 5$.
    (d) $7 \mid r$ se, e somente se, $r_0 + 3r_1 + \cdots + 3^m r_m$ é divisível por 7.

(e) $9 \mid r$ se, e somente se, $r_0 + r_1 + \cdots + r_m$ é divisível por 9.

(f) $11 \mid r$ se, e somente se, $(r_0 + r_2 + \cdots) - (r_1 + r_3 + \cdots)$ é divisível por 11.

13. Determinar os dígitos a, b e c dos números abaixo, representados no sistema decimal, tal que:

(a) $2a7b$ seja divisível por 4 e 11.

(b) $28a75b$ seja divisível por 3 e 11.

(c) $45ab$ seja divisível por 4 e 9.

(d) $13ab45c$ seja divisível por $8, 9$ e 11.

14. Mostrar que se $n > 4$ é número composto, então $(n-1)! \equiv 0 \pmod{n}$.

15. Sejam $a, b \in \mathbb{Z}$. Mostrar que se $a \equiv b \pmod{n}$, então $\text{mdc}(a, n) = \text{mdc}(b, n)$.

16. Sejam $a, b, c \in \mathbb{Z}$, $\text{mdc}(c, n) = d$ e $n = rd$. Mostrar que $ac \equiv bc \pmod{n}$ se, e somente se, $a \equiv b \pmod{r}$.

17. Sejam $a, b \in \mathbb{Z}$. Mostrar que $a \equiv b \pmod{n}$ e $a \equiv b \pmod{m}$ se, e somente se, $a \equiv b \pmod{\text{mmc}(m, n)}$.

18. Determinar o menor inteiro positivo que deixa restos $5, 4, 3$ e 2 quando dividido, respectivamente, por $6, 5, 4$ e 3. (Sugestão: Note que $5 \equiv -1 \pmod{6}$, $4 \equiv -1 \pmod{5}$, $3 \equiv -1 \pmod{4}$, $2 \equiv -1 \pmod{3}$ e use o exercício precedente.)

19. Seja $n \in \mathbb{N}$ com $n > 1$. Mostrar que $n = a^2 - b^2$ se, e somente se, $n \not\equiv 2 \pmod{4}$. (Sugestão: Use o exercício 1.)

20. Mostrar que $1^n + 2^n + 3^n + 4^n \equiv 0 \pmod{5}$ se, e somente se, $n \not\equiv 0 \pmod{4}$.

21. Mostrar que se um dos números $2^n - 1$ e $2^n + 1$, onde $n > 2$, é primo, então o outro é composto. (Sugestão: Considere o resto da divisão de 2^n por 3.)

22. Mostrar que

$$(a + b + c)^{333} - a^{333} - b^{333} - c^{333}$$

é divisível por

$$(a + b + c)^3 - a^3 - b^3 - c^3.$$

(Sugestão: Note que

$$(a + b + c)^3 - a^3 - b^3 - c^3 = 3(a + b)(a + c)(b + c)$$

e mostre que

$$f(a, b, c) = (a + b + c)^{333} - a^{333} - b^{333} - c^{333}$$

é divisível por $a + b$, $a + c$ e $b + c$.)

23. Mostrar que
$$a^{9.999} + a^{8.888} + \cdots + a^{1.111} + 1$$
é divisível por
$$a^9 + a^8 + \cdots + a + 1.$$
(Sugestão: Note que $a^{9.999} - a^9 = a^9[(a^{10})^{999} - 1], \ldots$)

24. Mostrar que o polinômio $f(x) = x^2 - 117x + 31$ não tem solução inteira.

25. Seja $f(x)$ um polinômio com coeficientes inteiros. Mostrar que se $f(0)$ e $f(1)$ são ímpares, então $f(x)$ não tem solução inteira.

26. A fórmula abaixo determina o dia da semana correspondente a uma data posterior a 1.582.
$$\begin{aligned} d \equiv\ & 1 - 2C + D + N + \lfloor \frac{C}{4} \rfloor + \lfloor \frac{D}{4} \rfloor \\ & + \lfloor 2,6M - 0,2 \rfloor - (1 + B)\lfloor \frac{M}{11} \rfloor \pmod 7, \end{aligned}$$
onde d é o dia da semana ($d = 0$ para o sábado,..., $d = 6$ para a sexta-feira), N é o dia do mês, M é o mês ($M = 1$ para o mês de março,..., $M = 12$ para o mês de fevereiro), $100C + D$ corresponde ao ano, $B = 1$ corresponde aos anos bissextos e $B = 0$ corresponde aos anos não bissextos. Determinar o dia da semana que morreu Tiradentes, sabendo que ele morreu no dia 21 de abril de 1.792.

6.2 Congruências Lineares

Nesta seção consideraremos o problema de encontrar todas as soluções inteiras $x_i, i = 1, \ldots, k$, para a equação Diofantina:
$$a_1x_1 + \cdots + a_kx_k = n, \tag{6.1}$$
onde $a_i \in \mathbb{Z}^*$. Primeiro vamos considerar a congruência linear
$$ax \equiv b \pmod n. \tag{6.2}$$
Note que a congruência linear 6.2 nem sempre tem solução em $\mathbb{Z}$, por exemplo, a congruência linear
$$3x \equiv 4 \pmod 3$$
não tem solução em $\mathbb{Z}$, pois
$$3x \equiv 4 \pmod 3 \Leftrightarrow \frac{3x - 4}{3} \in \mathbb{Z} \Leftrightarrow \frac{-1}{3} \in \mathbb{Z},$$
o que é um absurdo. A última implicação é uma aplicação do item (6) do Teorema 6.3. Além disso, se $x_0 \in \mathbb{Z}$ é uma solução da congruência linear 6.2, então $x = x_0 + kn$,

$\forall\ k \in \mathbb{Z}$, também o é. Portanto, se a congruência linear 6.2 tem uma solução em $\mathbb{Z}$, ela tem uma quantidade infinita de soluções em $\mathbb{Z}$.

Uma solução $x_0 \in \mathbb{Z}$ da congruência linear 6.2, com $0 \leq x_0 < n$, é chamada de *solução principal*. A *solução geral* da congruência linear 6.2 é $x = x_0 + kn$, com $k \in \mathbb{Z}$.

Exemplo 6.8 *Determinar as soluções, se existirem, da congruência linear*

$$3x \equiv 2 \,(\mathrm{mod}\, 5).$$

Solução. $3x \equiv 2 \,(\mathrm{mod}\, 5) \Leftrightarrow \exists t \in \mathbb{Z}$ tal que $3x - 2 = 5t$ ou $x = t + 2\left(\frac{t+1}{3}\right)$. Assim, $\frac{t+1}{3} \in \mathbb{Z}$ se, e somente se, $t + 1$ é um múltiplo de 3. Logo, $x_0 = 4$ é a solução principal da congruência linear. Portanto, $x = 4 + 5k$, $k \in \mathbb{Z}$ é a solução geral da congruência linear.

Teorema 6.9 *Sejam $a, b \in \mathbb{Z}$ e $mdc(a, n) = d$. Então a congruência linear $ax \equiv b \,(\mathrm{mod}\, n)$ tem solução em $\mathbb{Z}$ se, e somente se, d divide b.*

Prova. Seja $x_0 \in \mathbb{Z}$ uma solução da congruência linear $ax \equiv b \,(\mathrm{mod}\, n)$, isto é, existe $y \in \mathbb{Z}$ tal que $ax_0 + (-y)n = b$. Como $d \mid a$ e $d \mid n$ temos, pelo item (7) do Teorema 5.7, que d divide b.

Reciprocamente, Suponhamos que $d \mid b$ e que existam $r, s \in \mathbb{Z}$ tais que $ar + ns = d$. Como existe $t \in \mathbb{Z}$ tal que $b = td$ temos que

$$b = td = a(tr) + n(ts),$$

logo $(rt)a \equiv b \,(\mathrm{mod}\, n)$ e, assim, $x_0 = rt \in \mathbb{Z}$ é solução da congruência linear $ax \equiv b \,(\mathrm{mod}\, n)$. ■

Corolário 6.10 *Sejam $a, b \in \mathbb{Z}$ e $mdc(a, n) = 1$. Então a congruência linear $ax \equiv b \,(\mathrm{mod}\, n)$ tem solução $x_0 \in \mathbb{Z}$. Além disso,*

$$S = \{x_0 + kn : k \in \mathbb{Z}\}$$

é o conjunto de todas as soluções dessa congruência linear.

Prova. Seja $x_1 \in \mathbb{Z}$ outra solução da congruência linear $ax \equiv b \,(\mathrm{mod}\, n)$. Então $ax_1 \equiv ax_0 \,(\mathrm{mod}\, n)$. Logo, pelo Teorema 6.5, $x_1 \equiv x_0 \,(\mathrm{mod}\, n)$. Portanto, $x_1 \in S$. ■

Sejam $a, b \in \mathbb{Z}$ e $\mathrm{mdc}(a, n) = d$. Apresentaremos agora um **Algoritmo** para determinar, se existirem, as soluções da congruência linear

$$ax \equiv b \,(\mathrm{mod}\, n) :$$

1 - Use o Algoritmo Euclidiano para encontrar $r, s \in \mathbb{Z}$ tais que $ar + sn = d$.

2 - Se $d \nmid b$ vá para o Passo 5, caso contrário, multiplique $ar + sn = d$ por $\frac{b}{d}$, obtendo

$$ar\frac{b}{d} + sn\frac{b}{d} = b.$$

3 - $x_0 = r\frac{b}{d}$ é uma solução particular da congruência linear $ax \equiv b \pmod{n}$ e a solução geral da congruência linear é da forma

$$x = x_0 + k\frac{n}{d}, \ \ k \in \mathbb{Z}.$$

4 - Se x_0 é qualquer solução da congruência linear $ax \equiv b \pmod{n}$, então

$$x_0, x_0 + \frac{n}{d}, \ldots, x_0 + (d-1)\frac{n}{d}$$

são todas as soluções não congruentes (distintas) módulo n da congruência linear. Fim.

5 - A congruência linear $ax \equiv b \pmod{n}$ não tem solução. Fim.

Exemplo 6.11 *Determinar as soluções, se existirem, da congruência linear* $315x \equiv 12 \pmod{501}$.

Solução.

1 - De

$$\begin{aligned} 501 &= 1 \cdot 315 + 186 \\ 315 &= 1 \cdot 186 + 129 \\ 186 &= 1 \cdot 129 + 57 \\ 129 &= 2 \cdot 57 + 15 \\ 57 &= 3 \cdot 15 + 12 \\ 15 &= 1 \cdot 12 + 3 \\ 12 &= 4 \cdot 3 + 0 \end{aligned}$$

obtemos que $\text{mdc}(315, 501) = 3$ e $315 \cdot 35 + (-22) \cdot 501 = 3$.

2 - Como $3 \mid 12$, multiplicando $315 \cdot 35 + (-22) \cdot 501 = 3$ por $\frac{12}{3}$, obtemos

$$315 \cdot 140 + (-88) \cdot 501 = 12.$$

3 - $x_0 = 140$ é solução da congruência linear e

$$x = 140 + 167k, \ \ k \in \mathbb{Z}$$

é solução geral de $315x \equiv 12 \pmod{501}$.

4 - 140, 307 e 474 são as soluções não congruentes módulo 501 da congruência linear $315x \equiv 12 \pmod{501}$. Fim.

Note, pelo exemplo acima, que podem existir várias soluções principais.

Sejam $a, b \in \mathbb{Z}^*$ e $d = \text{mdc}(a, b)$. Temos, pelo Teorema 6.9, que a equação Diofantina

$$ax + ny = c \tag{6.3}$$

possui uma solução se, e somente se, d divide c. Podemos supor que $d = 1$, pois (x_0, y_0) é uma solução da equação 6.3 se, e somente se, (x_0, y_0) é solução da equação

$$\frac{a}{d}x + \frac{n}{d}y = \frac{c}{d}.$$

Como a equação 6.3 é equivalente a

$$ax \equiv c \,(\mathrm{mod}\, n),$$

cujas soluções são $x = x_0 + kn, \forall\ k \in \mathbb{Z}$, temos que

$$y = \frac{c - ax_0}{n} - ka,$$

isto é,

$$S = \{(x_0 + kn, y_0 - ka) : k \in \mathbb{Z}\},\ \ y_0 = \frac{c - ax_0}{n}$$

é o conjunto de todas as soluções dessa equação.

Observação 6.12 *Sejam $p, q, r, s \in \mathbb{Z}$ tais que $ps - qr = 1$. Então é fácil verificar que*

$$x = pu + qv,\ \ y = ru + sv \in \mathbb{Z} \Leftrightarrow u, v \in \mathbb{Z}.$$

Agora vamos resolver a equação

$$ax + by + cz = n, \tag{6.4}$$

onde $a, b, c \in \mathbb{Z}^*$. Seja $d = \mathrm{mdc}(a, b, c)$. Então é fácil verificar que a equação 6.4 possui uma solução se, e somente se, d divide n. Podemos supor que $d = 1$. Substituindo x e y da observação acima na equação 6.4, obtemos

$$(ap + br)u + (aq + bs)v + cz = n. \tag{6.5}$$

Assim, (u_0, v_0, z_0) é uma solução da equação 6.5 se, e somente se, (x_0, y_0, z_0) é uma solução da equação 6.4. Logo, escolhendo

$$p = \frac{b}{\mathrm{mdc}(a, b)}\ \text{ e }\ r = -\frac{a}{\mathrm{mdc}(a, b)}$$

temos que $\mathrm{mdc}(p, r) = 1$ e pelo Algoritmo Euclidiano obtemos os valores de q e s. Portanto, essa escolha transforma a equação 6.4 no seguinte sistema,

$$\begin{cases} x &= pu + qv \\ y &= ru + sv \\ \mathrm{mdc}(a, b)v + cz &= n, \end{cases}$$

onde $\mathrm{mdc}(\mathrm{mdc}(a, b), c) = 1$. A solução da última equação é

$$v = v_0 + ck\ \text{ e }\ z = z_0 - \mathrm{mdc}(a, b)k, \forall\ k \in \mathbb{Z}.$$

Assim, as soluções da equação são

$$\begin{cases} x &= pu + qck + qv_0 \\ y &= ru + sck + sv_0 \\ z &= 0u - \text{mdc}(a,b)k + z_0 \end{cases}$$

para quaisquer $u, k \in \mathbb{Z}$. Usando esse método de redução e indução finita podemos encontrar todas soluções da equação 6.1

Exemplo 6.13 *Determinar as soluções, se existirem, da equação*

$$2x + 3z + 4z = 7.$$

Solução. É fácil verificar que $\text{mdc}(2,3) = 1$. Assim, $p = 3$, $r = -2$ e

$$ps - qr = 3s + 2q = 1 \Rightarrow s = -1, q = 2.$$

Logo,

$$\begin{cases} x &= 3u + 2v \\ y &= -2u - 1v \\ v + 4z &= 7. \end{cases}$$

A solução da última equação é

$$v = 7 + 4k \text{ e } z = 0 - k, \forall\ k \in \mathbb{Z}.$$

Assim, as soluções da equação são

$$\begin{cases} x &= 3u + 8k + 14 \\ y &= -2u - 4k - 7 \\ z &= 0u - k + 0 \end{cases}$$

para quaisquer $u, k \in \mathbb{Z}$.

Exemplo 6.14 *A um feirante foi perguntado quantas laranjas ele possuia? Não sei, mas quando os separo de três em três sobra uma, de cinco em cinco sobra duas e de sete em sete sobra três. Qual é a quantidade mínima de laranjas que o feirante possuia*?

Solução. Seja x o número de laranjas do feirante. Então nosso problema é resolver o sistema de congruências

$$\begin{cases} x &\equiv 1 \,(\text{mod}\, 3) \\ x &\equiv 2 \,(\text{mod}\, 5) \\ x &\equiv 3 \,(\text{mod}\, 7). \end{cases}$$

Sabemos que a solução geral da premeira congruência é

$$x = 1 + 3y, \forall\ y \in \mathbb{Z}.$$

Substituindo na segunda congruência, obtemos

$$1 + 3y \equiv 2 \,(\mathrm{mod}\, 5) \Leftrightarrow 3y \equiv 1 \,(\mathrm{mod}\, 5),$$

cuja solução geral é

$$y = 2 + 5z, \forall\ z \in \mathbb{Z}.$$

Logo,

$$\begin{aligned} x &= 1 + 3y \\ &= 1 + 3(2 + 5z) \\ &= 7 + 15z, \forall\ z \in \mathbb{Z} \end{aligned}$$

é solução simultânea das duas congruências. Finalmente, substituindo na terceira congruência, obtemos

$$7 + 15z \equiv 3 \,(\mathrm{mod}\, 7) \Leftrightarrow 15z \equiv 3 \,(\mathrm{mod}\, 7),$$

cuja solução geral é

$$z = 3 + 7k, \forall\ k \in \mathbb{Z}.$$

Portanto,

$$\begin{aligned} x &= 7 + 15z \\ &= 7 + 15(3 + 7k) \\ &= 52 + 105k, \forall\ z \in \mathbb{Z} \end{aligned}$$

é solução geral do sistema de congruências e $x_0 = 52$ é quantidade mínima de laranjas que o feirante possuia. Mais geralmente, temos o seguinte teorema:

Teorema 6.15 (Teorema Chinês dos Restos) *Sejam $b_1, \ldots, b_k \in \mathbb{Z}$ e $n_1, \ldots, n_k \in \mathbb{N}$ tais que $mdc(n_i, n_j) = 1$ com $i \neq j$. Então o sistema de congruências*

$$\begin{cases} x \equiv b_1 \,(\mathrm{mod}\, n_1) \\ x \equiv b_2 \,(\mathrm{mod}\, n_2) \\ \quad \vdots \\ x \equiv b_k \,(\mathrm{mod}\, n_k) \end{cases}$$

tem uma única solução x_0 com $1 \leq x_0 < n$, onde $n = n_1 n_2 \cdots n_k$. Além disso,

$$S = \{x_0 + kn : k \in \mathbb{Z}\}$$

é o conjunto de todas as soluções deste sistema.

Prova. É claro que

$$\frac{n}{n_i} \in \mathbb{Z} \text{ e } \mathrm{mdc}(\frac{n}{n_i}, n_i) = 1,$$

para todo $i = 1, 2, \ldots, k$. Logo, pelo Corolário 6.10, para cada i existe $r_i \in \mathbb{Z}$ tal que

$$\frac{n}{n_i} r_i \equiv 1 \,(\mathrm{mod}\, n_i) \text{ e } \frac{n}{n_i} r_i b_i \equiv b_i \,(\mathrm{mod}\, n_i).$$

Se $j \neq i$, então é fácil verificar que

$$\frac{n}{n_i} r_i \equiv 0 \,(\mathrm{mod}\, n_j) \text{ e } \frac{n}{n_i} r_i b_i \equiv 0 \,(\mathrm{mod}\, n_j).$$

Assim, pondo

$$x_0 = \sum_{i=1}^{k} \frac{n}{n_i} r_i b_i$$

obtemos que

$$x_0 \equiv b_i \,(\mathrm{mod}\, n_i), \forall \; i = 1, 2, \ldots, k,$$

isto é, x_0 é uma solução do sistema de congruências.

Sejam $x_1, x_2 \in \mathbb{Z}$ duas soluções do sistema de congruências com

$$1 \leq x_1 \leq x_2 < n.$$

Então

$$x_1 \equiv x_2 \,(\mathrm{mod}\, n_i), \forall \; i = 1, 2, \ldots, k$$

e, portanto, $x_1 \equiv x_2 \,(\mathrm{mod}\, n)$, isto é, $n \mid (x_1 - x_2)$. Como $0 \leq x_1 - x_2 < n$ temos que $x_1 = x_2$. ■

Observação 6.16 *Como* $\mathrm{mdc}(\frac{n}{n_i}, n_i) = 1$*, para todo* $i = 1, 2, \ldots, k$*, temos, pelo Corolário* 6.10*, que existe um menor* $r_i \in \mathbb{Z}$*, com* $0 < r_i < n_i$*, tal que*

$$\frac{n}{n_i} r_i \equiv 1 \,(\mathrm{mod}\, n_i).$$

Para cada $i = 1, 2, \ldots, k$*, seja* $e_i = \frac{n}{n_i} r_i$*. Então*

1. $e_i^2 \equiv e_i \,(\mathrm{mod}\, n)$.
2. $e_i e_j \equiv 0 \,(\mathrm{mod}\, n)$ *se, e somente se,* $i \neq j$.
3. $\sum_{i=1}^{k} e_i \equiv 1 \,(\mathrm{mod}\, n)$.
4. $\sum_{i=1}^{k} a_i e_i \equiv \sum_{i=1}^{k} b_i e_i \,(\mathrm{mod}\, n)$ *se, e somente se,* $a_i \equiv b_i \,(\mathrm{mod}\, n_i)$.

Exemplo 6.17 *Determinar o menor inteiro positivo* x *tal que*

$$\begin{cases} x & \equiv & 5 \,(\mathrm{mod}\, 7) \\ x & \equiv & 7 \,(\mathrm{mod}\, 11) \\ x & \equiv & 3 \,(\mathrm{mod}\, 13). \end{cases}$$

Solução. Temos que $b_1 = 5$, $b_2 = 7$, $b_3 = 3$, $n_1 = 7$, $n_2 = 11$, $n_3 = 13$ e $n = 1.001$. Como

$$\text{mdc}(\frac{1.001}{7}, 7) = \text{mdc}(143, 7) = 1$$

temos, pelo Algoritmo Euclidiano, que $7 \cdot 21 + (-2) \cdot 143 = 1$, isto é,

$$(-2) \cdot 143 \equiv 1 \,(\text{mod}\, 7).$$

Assim, podemos escolher $r_1 = -2$. De modo análogo, podemos escolher $r_2 = 4$ e $r_3 = -1$. Logo,

$$x_0 = 11 \cdot 13 \cdot (-2) \cdot 5 + 7 \cdot 13 \cdot 4 \cdot 7 + 7 \cdot 11 \cdot (-1) \cdot 3 = 887$$

é a única solução. Portanto, $x_0 = 887$ é a menor solução positiva. Seja $e_1 = 715$, então

$$\begin{aligned} e_1^2 - e_1 &= 511\,225 - 715 \\ &= 510\,510 \\ &= 7293 \cdot 7. \end{aligned}$$

De modo análogo, podemos encontrar $e_2 = 364$ e $e_3 = 924$. Logo,

$$e_1 e_2 = e_1 e_3 = e_2 e_3 \equiv 0 \,(\text{mod}\, 1.001)$$

e

$$e_1 + e_2 + e_3 \equiv 1 \,(\text{mod}\, 1.001).$$

Exemplo 6.18 *Resolver o sistema de congruências*

$$\begin{cases} 5x &\equiv 1 \,(\text{mod}\, 6) \\ 3x &\equiv 5 \,(\text{mod}\, 8). \end{cases}$$

Solução. Como

$$\text{mdc}(5, 6) = 1 \mid 1 \text{ e } \text{mdc}(3, 8) = 1 \mid 5$$

temos que as congruências lineares admitem soluções particulares $x_1 = 5$ e $x_2 = 7$, respectivamente. Então nosso sistema de congruências é equivalente ao sistema de congruências

$$\begin{cases} x &\equiv 5 \,(\text{mod}\, 6) \\ x &\equiv 7 \,(\text{mod}\, 8). \end{cases}$$

Sendo $\text{mdc}(6, 8) = 2$, não podemos aplicar o Teorema Chinês dos Restos, mas o sistema de congruências tem solução, pois sabemos que a solução geral da primeira congruência é

$$x = 5 + 6y, \forall \; y \in \mathbb{Z}.$$

Logo, substituindo na segunda congruência, obtemos

$$5 + 6y \equiv 7 \,(\text{mod}\, 8) \Leftrightarrow 6y \equiv 2 \,(\text{mod}\, 8) \Leftrightarrow 3y \equiv 1 \,(\text{mod}\, 4).$$

e, assim, a solução geral da congruência é

$$y = 3 + 4z, \forall\ z \in \mathbb{Z}.$$

Portanto, a solução geral do sistema de congruências é

$$x = 5 + 6(3 + 4z) = 23 + 24z, \forall\ z \in \mathbb{Z},$$

confira exercício 12 abaixo.

EXERCÍCIOS

1. Sejam $a, b \in \mathbb{Z}$ e $\text{mdc}(a, n) = d$. Mostrar que se $x_0 \in \mathbb{Z}$ é solução da congruência linear $ax \equiv b \pmod{n}$, então também o é da congruência linear $ax \equiv b \pmod{\frac{n}{d}}$.

2. Resolver as seguintes congruências lineares:

   (a) $4x \equiv 3 \pmod{7}$.

   (b) $3x + 1 \equiv 4 \pmod{5}$.

   (c) $9x \equiv 11 \pmod{26}$.

   (d) $8x \equiv 6 \pmod{14}$.

   (e) $330x \equiv 42 \pmod{273}$.

   (f) $26x \equiv 1 \pmod{17}$.

3. Resolver os seguintes sistemas de congruências:

   (a) $x \equiv 3 \pmod{7}$ e $x \equiv 2 \pmod{5}$.

   (b) $x \equiv 1 \pmod{3}$, $x \equiv 1 \pmod{5}$ e $x \equiv 1 \pmod{7}$.

   (c) $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$ e $x \equiv 5 \pmod{2}$.

   (d) $x \equiv 1 \pmod{4}$, $x \equiv 0 \pmod{3}$ e $x \equiv 5 \pmod{7}$.

4. Determinar o menor inteiro positivo que tem para restos 2, 3 e 2 quando dividido, respectivamente, por 3, 5 e 7.

5. Determinar o menor inteiro positivo que tem para restos 1, 4, 2, 9 e 3 quando dividido, respectivamente, por 3, 5, 7, 11 e 13.

6. Determinar o menor inteiro positivo que tem para restos 5, 4, 3 e 2 quando dividido, respectivamente, por 6, 5, 4 e 3.

7. Determinar o menor múltiplo positivo de 7 que tem para resto 1 quando dividido por 2, 3, 4, 5 e 6. (Sugestão: Note que $7x \equiv 1 \pmod{2}, \ldots$ e use o exercício 17 da Seção 6.1.)

8. Um grupo de 13 piratas obteve um certo número de moedas de ouro que, distribuídas igualmente entre eles, sobravam 8 moedas. Imprevisivelmente, dois deles morreram. Eles voltaram a repartir e sobraram agora 3 moedas. Posteriormente, três deles se afogaram. Repartindo novamente as moedas, restaram 5 moedas. Quantas moedas havia em jogo?

9. Determinar quatro inteiros consecutivos divisíveis por 5, 7, 9 e 11, respectivamente.

10. Mostrar que, para todo $n \in \mathbb{N}$, com $n > 1$, existem n inteiros consecutivos que são divisíveis por quadrados maiores do que 1.(Sugestão: Sejam $p_1, \ldots, p_n$ números primos distintos. Considere o sistema de congruências

$$\begin{cases} x & \equiv & 0 \pmod{p_1^2} \\ x & \equiv & -1 \pmod{p_2^2} \\ & \vdots & \\ x & \equiv & -(n-1) \pmod{p_n^2} \end{cases}$$

e resolva.)

11. Sejam $a_1, \ldots, a_k, b_1, \ldots, b_k \in \mathbb{Z}$ e $n_1, \ldots, n_k \in \mathbb{N}$ tais que $\text{mdc}(n_i, n_j) = 1$ com $i \neq j$. Mostrar que o sistema de congruências

$$\begin{cases} a_1 x & \equiv & b_1 \pmod{n_1} \\ a_2 x & \equiv & b_2 \pmod{n_2} \\ & \vdots & \\ a_k x & \equiv & b_k \pmod{n_k} \end{cases}$$

tem uma solução se, e somente se, $\text{mdc}(a_i, n_i) \mid b_i$ para $i = 1, 2, \ldots, k$. Além disso,

$$S = \{x_0 + kn : k \in \mathbb{Z}\},$$

onde $n = n_1 \cdots n_k$, é o conjunto de todas as soluções deste sistema.

12. Sejam $b_1, \ldots, b_k \in \mathbb{Z}$ e $n_1, \ldots, n_k \in \mathbb{N}$. Mostrar que o sistema de congruências

$$\begin{cases} x & \equiv & b_1 \pmod{n_1} \\ x & \equiv & b_2 \pmod{n_2} \\ & \vdots & \\ x & \equiv & b_k \pmod{n_k} \end{cases}$$

tem uma solução se, e somente se, $\text{mdc}(n_i, n_j) \mid (b_i - b_j)$ para $i, j = 1, 2, \ldots, k$. Além disso,

$$S = \{x_0 + kn : k \in \mathbb{Z}\},$$

onde $n = \text{mmc}(n_1, \ldots, n_k)$, é o conjunto de todas as soluções deste sistema.

13. Resolver os seguintes sistemas de congruências:

(a) $x \equiv 2 \pmod 5$ e $3x \equiv 1 \pmod 8$.

(b) $3x \equiv 2 \pmod 5$ e $2x \equiv 1 \pmod 3$.

(c) $6x \equiv 5 \pmod{11}$, $5x \equiv 6 \pmod 7$ e $x \equiv 6 \pmod{13}$.

(d) $x \equiv 17 \pmod{504}$, $x \equiv 31 \pmod{35}$ e $x \equiv 33 \pmod{16}$.

14. Determinar o menor inteiro positivo que tem para restos 3, 9 e 17 quando dividido, respectivamente, por 10, 16 e 24.

6.3 Teorema de Euler

Definição 6.19 *Um subconjunto $\{r_1, \ldots, r_k\}$ de $\mathbb{Z}$ é um* sistema completo de resíduos módulo n *se as seguintes condições são satisfeitas*:

1. *Se $i \neq j$, então $r_i \not\equiv r_j \pmod n$, $\forall\ i, j \in \{1, 2, \ldots, k\}$.*

2. *Para todo $a \in \mathbb{Z}$ existe $i \in \{1, 2, \ldots, k\}$ tal que $a \equiv r_i \pmod n$.*

Exemplo 6.20 *O subconjunto $\{0, 1, \ldots, n-1\}$ de $\mathbb{Z}$ é um sistema completo de resíduos módulo n.*

Solução. Sejam $a, b \in \{0, 1, \ldots, n-1\}$, com $0 \leq a \leq b < n$. Então

$$b \equiv a \pmod n \Leftrightarrow n \mid (b-a) \Leftrightarrow b = a,$$

pois $0 \leq b - a < n$. Agora, para todo $a \in \mathbb{Z}$ temos, pelo Teorema 5.1, que existem $q, r \in \mathbb{Z}$ tais que

$$a = qn + r \ \text{ onde } \ 0 \leq r < n.$$

Portanto,

$$a \equiv r \pmod n \ \text{ onde } \ r \in \{0, 1, \ldots, n-1\}.$$

É fácil verificar, pelo lema abaixo, que $\{k, k+1, \ldots, k+(n-1)\}$ é um sistema completo de resíduos módulo n para todo $k \in \mathbb{Z}$. Assim, existe uma infinidade de sistemas completos de resíduos módulo n.

Lema 6.21 *Sejam $\{r_1, \ldots, r_k\}$ e $\{s_1, \ldots, s_l\}$ dois sistemas completos de resíduos módulo n. Então $k = l$ (e pelo exemplo acima, $k = n$).*

Prova. Suponhamos que $k > l$. Então, re-indexando se necessário, obtemos

$$r_1 \equiv s_1 \pmod n, \ldots, r_l \equiv s_l \pmod n.$$

Como $r_{l+1} \in \mathbb{Z}$ temos, pelo item *2* da definição, que existe $i \in \{1, 2, \ldots, l\}$ tal que $r_{l+1} \equiv s_i \pmod n$. Assim, $r_{l+1} \equiv r_i \pmod n$, o que é uma contradição, pois $l + 1 \neq i$. Portanto, $k \leq l$. De modo análogo, mostra-se que $l \leq k$. ■

Definição 6.22 *Um subconjunto* $\{r_1, \ldots, r_k\}$ *de* $\mathbb{Z}$ *é um* sistema reduzido de resíduos módulo n *se as seguintes condições são satisfeitas*:

1. $\text{mdc}(r_i, n) = 1$, $\forall\ i \in \{1, 2, \ldots, k\}$.
2. *Se* $i \neq j$, *então* $r_i \not\equiv r_j \pmod{n}$, $\forall\ i, j \in \{1, 2, \ldots, k\}$.
3. *Para todo* $a \in \mathbb{Z}$, *com* $\text{mdc}(a, n) = 1$, *existe* $i \in \{1, 2, \ldots, k\}$ *tal que* $a \equiv r_i \pmod{n}$.

Pelo exercício 16 da Secão 5.1 é fácil verificar que se

$$\{r_1, \ldots, r_n\}$$

é um sistema completo de resíduos módulo n e

$$\{s_1, \ldots, s_l\}$$

são todos os elementos de

$$\{r_1, \ldots, r_n\}$$

tais que $\text{mdc}(s_i, n) = 1$, então

$$\{s_1, \ldots, s_l\}$$

é um sistema reduzido de resíduos módulo n, isto é, um sistema reduzido de resíduos módulo n pode ser obtido eliminando de um sistema completo de resíduos módulo n aqueles números que não são relativamente primos de n. Por exemplo,

$$\{0, 1, 2, 3, 4, 5\}$$

é um sistema completo de resíduos módulo 6. Assim,

$$\{1, 5\}$$

é um sistema reduzido de resíduos módulo 6. Além disso, pelo Lema 6.21, todos os sistemas reduzidos de resíduos módulo n têm a mesma cardinalidade, que denotaremos por $\phi(n)$. Essa função é chamada de *função* ϕ *de Euler*. Por exemplo,

$$\phi(6) = 2.$$

Teorema 6.23 *Seja* $P_n = \{k \in \mathbb{N} : mdc(k, n) = 1\ \ e\ \ k < n\}$. *Então*

$$\phi(n) = \#(P_n).$$

Prova. Como

$$\{0, 1, \ldots, n-1\}$$

é um sistema completo de resíduos módulo n, temos que P_n é um sistema reduzido de resíduos módulo n. Portanto, $\#(P_n) = \phi(n)$. ■

Um elemento $\overline{a} \in \mathbb{Z}_n$ é chamado *invertível* se existir $\overline{x} \in \mathbb{Z}_n$ tal que

$$\overline{a} \odot \overline{x} = \overline{x} \odot \overline{a} = \overline{1}$$

ou, equivalentemente,

$$ax \equiv 1 \,(\mathrm{mod}\, n).$$

Seja $\mathbb{Z}_n^\bullet$ o conjunto dos elementos invertíveis em $\mathbb{Z}_n$, isto é,

$$\mathbb{Z}_n^\bullet = \{\overline{a} \in \mathbb{Z}_n : \overline{a} \odot \overline{x} = \overline{x} \odot \overline{a} = \overline{1} \text{ para algum } \overline{x} \in \mathbb{Z}_n\}.$$

Note que se $a \in P_n$, então $\mathrm{mdc}(a, n) = 1$. Logo, existem $x, y \in \mathbb{Z}$ tais que

$$ax + ny = 1$$

e, consequentemente,

$$ax \equiv 1 \,(\mathrm{mod}\, n) \Leftrightarrow \overline{a} \odot \overline{x} = \overline{1}.$$

Portanto, $\overline{a} \in \mathbb{Z}_n^\bullet$.

Reciprocamente, se $\overline{a} \in \mathbb{Z}_n^\bullet$, então existe $\overline{x} \in \mathbb{Z}_n$ tal que

$$\overline{a} \odot \overline{x} = \overline{x} \odot \overline{a} = \overline{1}.$$

Logo, $ax \equiv 1 \,(\mathrm{mod}\, n)$, isto é, existe $y \in \mathbb{Z}$ tal que

$$ax + n(-y) = 1.$$

Assim, $\mathrm{mdc}(a, n) = 1$. Portanto, $a \in P_n$. Assim, a função

$$f : P_n \to \mathbb{Z}_n^\bullet \text{ dada por } f(a) = \overline{a}$$

é uma correspondência biunívoca. Neste caso,

$$\phi(n) = \#(\mathbb{Z}_n^\bullet),$$

isto é,

$$\mathbb{Z}_n^\bullet = \{\overline{r}_1, \ldots, \overline{r}_{\phi(n)}\},$$

onde

$$\{r_1, \ldots, r_{\phi(n)}\}$$

é um sistema reduzido de resíduos módulo n.

Exemplo 6.24 *Seja p um número primo. Então*

$$\mathbb{Z}_p^\bullet = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}.$$

Solução. Sabemos que

$$\{0, 1, 2, \ldots, p-1\}$$

é um sistema completo de resíduos módulo p e que 0 é o único elemento deste conjunto que não é relativamente primo com p. Logo,

$$P_p = \{1, 2, \ldots, p-1\}$$

é um sistema reduzido de resíduos módulo p. Portanto,

$$\mathbb{Z}_p^\bullet = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\} \text{ e } \phi(p) = p-1.$$

Teorema 6.25 *Se $p \in \mathbb{N}$ é um número primo, então $\phi(p^k) = p^k(1 - \frac{1}{p})$, para todo $k \in \mathbb{N}$.*

Prova. Note que, se

$$a \in \{1, 2, \ldots, p^k\} \text{ e } \text{mdc}(a, p^k) \neq 1,$$

então $a = pb$ com

$$b \in \{1, 2, \ldots, p^{k-1}\}.$$

Assim,

$$\text{mdc}(a, p^k) \neq 1 \Leftrightarrow a \in \{p, 2p, \ldots, pp^{k-1} = p^k\},$$

isto é, existem p^{k-1} números entre 1 e p^k que são divisíveis por p. Portanto,

$$\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p}).$$

■

Lema 6.26 *Sejam $a, b, n \in \mathbb{Z}$. Se $mdc(a, n) = mdc(b, n) = 1$, então*

$$mdc(ab, n) = 1.$$

Prova. Se $\text{mdc}(a, n) = \text{mdc}(b, n) = 1$, então existem $r, s, x, y \in \mathbb{Z}$ tais que

$$ar + ns = 1 \text{ e } bx + ny = 1.$$

Logo,

$$1 = 1 \cdot 1 = (ar + ns)(bx + ny) = ab(rs) + n(ary + bsx + nsy) = abu + nv,$$

onde $u = rs$, $v = ary + bsx + nsy \in \mathbb{Z}$, isto é, $\text{mdc}(ab, n) = 1$. ■

Lema 6.27 *Seja $a \in \mathbb{Z}$, com $mdc(a, n) = 1$. Se*

$$\{r_1, \ldots, r_n\}$$

é um sistema completo (reduzido) de resíduos módulo n, então

$$\{ar_1, \ldots, ar_n\}$$

é um sistema completo (reduzido) de resíduos módulo n.

Prova. Sabemos, pelo Lema 6.26, que

$$\text{mdc}(a,n) = \text{mdc}(r_i,n) = 1 \Rightarrow \text{mdc}(ar_i,n) = 1.$$

Além disso,

$$\#(\{r_1,\ldots,r_n\}) = \#(\{ar_1,\ldots,ar_n\}).$$

Assim, basta mostrar que se $i \neq j$, então $ar_i \not\equiv ar_j (\text{mod}\, n)$. Temos, pelo Teorema 6.5, que

$$ar_i \equiv ar_j \,(\text{mod}\, n) \Rightarrow r_i \equiv r_j \,(\text{mod}\, n) \Rightarrow i = j.$$

Portanto,

$$\{ar_1,\ldots,ar_n\}$$

é um sistema completo (reduzido) de resíduos módulo n. ■

Lema 6.28 *Seja $a \in \mathbb{Z}$, com $mdc(a,n) = 1$. Então*

$$\{r, r+a, r+2a, \ldots, r+(n-1)a\}$$

é um sistema completo de resíduos módulo n para todo $r \in \mathbb{Z}$.

Prova. Temos, pelo Lema 6.27, que

$$\{0, a, 2a, \ldots, (n-1)a\},$$

é um sistema completo de resíduos módulo n. Como

$$\#(\{0,a,2a,\ldots,(n-1)a\}) = \#(\{r, r+a, r+2a, \ldots, r+(n-1)a\})$$

temos que

$$\{r, r+a, r+2a, \ldots, r+(n-1)a\}$$

é um sistema completo de resíduos módulo n para todo $r \in \mathbb{Z}$. ■

Teorema 6.29 *Sejam $m,n \in \mathbb{N}$. Se $mdc(m,n) = 1$, então*

$$\phi(mn) = \phi(m)\phi(n).$$

Prova. Consideremos o conjunto

$$X = \{qm + r : 0 \leq r < m \text{ e } 0 \leq q < n\}.$$

É fácil verificar que $\#(X) = mn$ e $a < mn$ para todo $a \in X$. Logo,

$$X = \{a \in \mathbb{Z} : 0 \leq a < mn\}.$$

Pelo Lema 6.26 e $\text{mdc}(m,n) = 1$ temos que

$$\text{mdc}(a,mn) = 1 \Leftrightarrow \text{mdc}(a,m) = \text{mdc}(a,n) = 1.$$

Logo, podemos analizar os elementos de X que são relativamente primos com m e n separadamente. Note que

$$\text{mdc}(r, m) = 1 \Rightarrow \text{mdc}(r, r + im) = 1, \forall\ i \in \{1, \ldots, n-1\}.$$

Assim, se

$$\{r_1, \ldots, r_{\phi(m)}\}$$

é um sistema reduzido de resíduos módulo m, então, pelo Lema 6.28,

$$\{r_j, r_j + m, r_j + 2m, \ldots, r_j + (n-1)m\}, \forall\ j \in \{1, \ldots, \phi(m)\}$$

é um sistema completo de resíduos módulo n e contém um sistema reduzido de resíduos módulo n. Logo, existem $\phi(m)\phi(n)$ números da forma $qm + r$, que são relativamente primos com m e n, isto é, com mn. Portanto,

$$\phi(mn) = \phi(m)\phi(n).$$

■

Corolário 6.30 *Seja $n \in \mathbb{N}$, com $n > 1$. Então*

$$\phi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right),$$

onde $p_1, \ldots, p_r$ são os primos distintos que dividem n. ■

Teorema 6.31 (Euler) *Sejam $m, n \in \mathbb{N}$ com $mdc(m, n) = 1$. Então*

$$n^{\phi(m)} \equiv 1 \,(\text{mod}\, m).$$

Prova. Seja

$$\{r_1, \ldots, r_{\phi(m)}\}$$

um sistema reduzido de resíduos módulo m, então, pelo Lema 6.27,

$$\{nr_1, \ldots, nr_{\phi(m)}\}$$

é um sistema reduzido de resíduos módulo m. Portanto, para cada $i \in \{1, \ldots, \phi(m)\}$, existe $j \in \{1, \ldots, \phi(m)\}$ tal que

$$nr_i \equiv r_j \,(\text{mod}\, m).$$

Assim, pelo item *4* do Teorema 6.3,

$$\prod_{i=1}^{\phi(m)} nr_i \equiv \prod_{j=1}^{\phi(m)} r_j \,(\text{mod}\, m) \Rightarrow n^{\phi(m)} \prod_{i=1}^{\phi(m)} r_i \equiv \prod_{i=1}^{\phi(m)} r_i \,(\text{mod}\, m).$$

Como $\text{mdc}(r_i, m) = 1$ para $i = 1, \ldots, \phi(m)$ temos, pelo Teorema 6.5, que

$$n^{\phi(m)} \equiv 1 \,(\text{mod}\, m).$$

■

Corolário 6.32 (Fermat) *Seja $p \in \mathbb{N}$ um número primo. Então*

$$a^p \equiv a \,(\mathrm{mod}\, p), \forall\ a \in \mathbb{Z}.$$

Prova. Se $a = 0$ não há nada para provar. Podemos supor, sem perda de generalidade, que $a > 0$, pois o caso $a < 0$, reduz-se a esse com a substituição de a por $b = -a > 0$. Assim, há dois casos a ser considerado:

1º **Caso**. Se $p \mid a$, então

$$a \equiv 0 \,(\mathrm{mod}\, p)\ \text{ e }\ a^p \equiv 0 \,(\mathrm{mod}\, p) \Rightarrow a^p \equiv a \,(\mathrm{mod}\, p).$$

2º **Caso**. Se $p \nmid a$, então $\mathrm{mdc}(a, p) = 1$. Logo, pelo Teorema de Euler,

$$a^{\phi(p)} \equiv 1 \,(\mathrm{mod}\, p)\ \text{ ou }\ a^{p-1} \equiv 1 \,(\mathrm{mod}\, p).$$

Como $a \equiv a \,(\mathrm{mod}\, p)$ temos, pelo item *4* do Teorema 6.3, que

$$a^p \equiv a \,(\mathrm{mod}\, p).$$

Portanto, em qualquer caso, $a^p \equiv a \,(\mathrm{mod}\, p)$. ■

Observação 6.33 *O Teorema de Euler pode ser usado para determinar o inverso de todo elemento $\overline{a} \in \mathbb{Z}_n^{\bullet}$, pois*

$$a^{\phi(n)} \equiv 1 \,(\mathrm{mod}\, n) \Leftrightarrow a^{-1} = a^{\phi(n)-1} \,(\mathrm{mod}\, n).$$

Exemplo 6.34 *Determinar os últimos três dígitos do número $7^{9.999}$ no sistema de representação decimal.*

Solução. Basta encontrar o resto da divisão de $7^{9.999}$ por 1.000, isto é,

$$7^{9.999} \equiv r \,(\mathrm{mod}\, 1.000),\ \text{ onde }\ 0 \leq r < 1.000.$$

Como $\mathrm{mdc}(7, 1.000) = 1$ temos, pelo Teorema de Euler, que

$$7^{\phi(1.000)} \equiv 1 \,(\mathrm{mod}\, 1.000) \Rightarrow 7^{400} \equiv 1 \,(\mathrm{mod}\, 1.000),$$

pois

$$\phi(1.000) = \phi(2^3 5^3) = \phi(2^3)\phi(5^3) = 2^3 \left(1 - \frac{1}{2}\right) 5^3 \left(1 - \frac{1}{5}\right) = 400.$$

Sendo $9.999 = 24 \cdot 400 + 399$ segue-se que

$$7^{9.999} \equiv 7^{399} \,(\mathrm{mod}\, 1.000).$$

Assim,

$$7^{400} \equiv 1 \,(\mathrm{mod}\, 1.000) \Rightarrow 7^{399} \cdot 7 \equiv 1 \,(\mathrm{mod}\, 1.000).$$

Logo, devemos resolver a congruência linear

$$7x \equiv 1 \,(\mathrm{mod}\, 1.000).$$

É fácil verificar que $x_0 = 143$ é a solução principal dessa congruência linear. Portanto, a representação decimal de $7^{9.999}$ termina em 143.

Exemplo 6.35 *Mostrar que*

$$a^{561} \equiv a \,(\mathrm{mod}\, 561), \forall\ a \in \mathbb{Z}.$$

Solução. Note que $561 = 3 \cdot 11 \cdot 17$. Assim, basta mostrar que

$$a^{561} \equiv a \,(\mathrm{mod}\, 3), a^{561} \equiv a \,(\mathrm{mod}\, 11) \text{ e } a^{561} \equiv a \,(\mathrm{mod}\, 17).$$

Se $561 \mid a$ não há nada para fazer. Assim, suponhamos que $\mathrm{mdc}(561, a) = 1$. Pelo Teorema de Euler,

$$\begin{aligned} a^2 &\equiv 1 \,(\mathrm{mod}\, 3) \Rightarrow a^{560} \equiv 1 \,(\mathrm{mod}\, 3) \Rightarrow a^{561} \equiv a \,(\mathrm{mod}\, 3). \\ a^{10} &\equiv 1 \,(\mathrm{mod}\, 11) \Rightarrow a^{560} \equiv 1 \,(\mathrm{mod}\, 11) \Rightarrow a^{561} \equiv a \,(\mathrm{mod}\, 11). \\ a^{16} &\equiv 1 \,(\mathrm{mod}\, 17) \Rightarrow a^{560} \equiv 1 \,(\mathrm{mod}\, 17) \Rightarrow a^{561} \equiv a \,(\mathrm{mod}\, 17). \end{aligned}$$

Portanto, a recíproca do Teorema de Fermat é falsa, isto é,

$$a^{561} \equiv a \,(\mathrm{mod}\, 561), \forall\ a \in \mathbb{Z},$$

mas 561 não é um número primo.

Denotaremos por $M_2(\mathbb{Z}_n)$ o conjunto das matrizes 2×2 com entradas sobre $\mathbb{Z}_n$.

Teorema 6.36 *Sejam*

$$A = \begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix} \in M_2(\mathbb{Z}_n) \ \ e \ \ D = ad - bc \in \mathbb{Z}.$$

Então as seguintes condições são equivalentes:

1. $mdc(n, D) = 1$.

2. *A tem uma matriz inversa.*

3. *A função*

$$T : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \times \mathbb{Z}_n \ \ dada\ por\ T\left(\begin{bmatrix} \overline{x} \\ \overline{y} \end{bmatrix}\right) = A \begin{bmatrix} \overline{x} \\ \overline{y} \end{bmatrix}$$

   é uma correspondência biunívoca.

4. *Se* $\overline{x}$ *ou* $\overline{y} \in \mathbb{Z}_n^*$, *então*

$$T\left(\begin{bmatrix} \overline{x} \\ \overline{y} \end{bmatrix}\right) \neq \begin{bmatrix} \overline{0} \\ \overline{0} \end{bmatrix}.$$

Prova. (*1.* $\Rightarrow$ *2.*) Suponhamos que $\mathrm{mdc}(n, D) = 1$. Então existe $\overline{D}^{-1} \in \mathbb{Z}_n$ tal que

$$\overline{D} \odot \overline{D}^{-1} = \overline{1}.$$

Portanto,

$$A^{-1} = \begin{bmatrix} \overline{D}^{-1}\overline{d} & -\overline{D}^{-1}\overline{b} \\ -\overline{D}^{-1}\overline{c} & \overline{D}^{-1}\overline{a} \end{bmatrix}$$

é a matriz inversa de A. É fácil verificar que (*2.* $\Rightarrow$ *3.*) e (*3.* $\Rightarrow$ *4.*). Assim, resta mostrar que (*4.* $\Rightarrow$ *1.*), Suponhamos que $\mathrm{mdc}(n, D) = k > 1$ e seja $m = \frac{n}{k}$. Então há três casos a ser considerado:

1º **Caso**. Se todas as entradas de A são divisíveis por k, então pondo

$$\begin{bmatrix} \overline{x} \\ \overline{y} \end{bmatrix} = \begin{bmatrix} \overline{m} \\ \overline{m} \end{bmatrix}, \text{ obtemos que } T\left(\begin{bmatrix} \overline{x} \\ \overline{y} \end{bmatrix}\right) = \begin{bmatrix} \overline{0} \\ \overline{0} \end{bmatrix}.$$

2º **Caso**. Se a e b não são ambos divisíveis por k, então pondo

$$\begin{bmatrix} \overline{x} \\ \overline{y} \end{bmatrix} = \begin{bmatrix} -\overline{bm} \\ \overline{am} \end{bmatrix}, \text{ obtemos que } T\left(\begin{bmatrix} \overline{x} \\ \overline{y} \end{bmatrix}\right) = \begin{bmatrix} \overline{0} \\ \overline{0} \end{bmatrix},$$

pois n divide Dm.

3º **Caso**. Se c e d não são divisíveis por k, então pondo

$$\begin{bmatrix} \overline{x} \\ \overline{y} \end{bmatrix} = \begin{bmatrix} \overline{dm} \\ -\overline{cm} \end{bmatrix}, \text{ obtemos que } T\left(\begin{bmatrix} \overline{x} \\ \overline{y} \end{bmatrix}\right) = \begin{bmatrix} \overline{0} \\ \overline{0} \end{bmatrix},$$

pois n divide Dm. ■

Lema 6.37 *Sejam* $a, n \in \mathbb{N}$, *com* $mdc(a, n) = 1$. *Se* $r, t \in \mathbb{N}$ *são tais que* $rt \equiv 1 \pmod{\phi(n)}$, *então*

$$a^{rt} \equiv a \pmod{n}.$$

Prova. Como $rt \equiv 1 \pmod{\phi(n)}$ temos que existe $s \in \mathbb{N}$ tal que

$$rt = 1 + s\phi(n).$$

Logo,

$$a^{rt} = a^{1+s\phi(n)} = a \cdot a^{s\phi(n)} = a\left(a^{\phi(n)}\right)^s \equiv a \cdot 1^s \equiv a \pmod{n}.$$

■

Corolário 6.38 *Sejam* $n, r, t \in \mathbb{N}$. *Se* $mdc(t, \phi(n)) = 1$, *então a função*

$$f : \mathbb{Z}_n \to \mathbb{Z}_n \text{ dada por } f(\overline{x}) = \overline{x}^t$$

é uma correspondência biunívoca com $f^{-1}(\overline{x}) = \overline{x}^r$, *onde*

$$rt \equiv 1 \pmod{\phi(n)}.$$

■

6.4 Triângulos Pitagorianos

Nesta seção consideraremos o problema de encontrar todas as soluções inteiras positivas x, y e z para a equação Diofantina:

$$x^2 + y^2 = z^2. \tag{6.6}$$

Suponhamos que $x, y, z \in \mathbb{N}$ seja uma solução da equação 6.6. Seja $d = \text{mdc}(x, y)$. Então $d^2 \mid x^2$ e $d^2 \mid y^2$ e, assim, $d^2 \mid x^2 + y^2$, isto é, $d^2 \mid z^2$. Temos, pela unicidade do Teorema Fundamental da Aritmética, que $d \mid z$. Portanto,

$$\text{mdc}(x, y) = \text{mdc}(x, z) = \text{mdc}(y, z) = \text{mdc}(x, y, z).$$

Assim, se $x, y, z \in \mathbb{N}$ é uma solução da equação 6.6 e $d = \text{mdc}(x, y)$, então

$$a = \frac{x}{d}, b = \frac{y}{d} \text{ e } c = \frac{z}{d}$$

é uma solução da equação 6.6 com $\text{mdc}(a, b) = 1$, chamamos (a, b, c) uma solução *primitiva*, por exemplo, 3, 4 e 5 e 5, 12 e 13 são soluções primitivas da equação 6.6. Assim, todo triângulo Pitagoriano é similar a um triângulo Pitagoriano primitivo. Portanto, basta considerar o problema de encontrar todas as soluções primitivas da equação 6.6.

Seja x, y e z uma solução primitiva da equação 6.6. Então x e y não podem ser ambos pares e também não podem ser ambos ímpares, pois

$$x^2 \equiv 1 \,(\text{mod}\, 4) \text{ e } y^2 \equiv 1 \,(\text{mod}\, 4) \Rightarrow z^2 \equiv 2 \,(\text{mod}\, 4),$$

o que é impossível. Como x e y aparecem simetricamente na equação 6.6, podemos supor, sem perda de generalidade, que x é par e y e z são ímpares. Note que

$$x^2 + y^2 = z^2 \Leftrightarrow x^2 = (z + y)(z - y) \Leftrightarrow (\frac{x}{2})^2 = (\frac{z + y}{2})(\frac{z - y}{2})$$

e a última equação tem sentido, pois x, $z + y$ e $z - y$ são pares. Afirmação:

$$\text{mdc}(\frac{z + y}{2}, \frac{z - y}{2}) = 1.$$

De fato, seja $d = \text{mdc}(\frac{z+y}{2}, \frac{z-y}{2})$. Então $d \mid y$ e $d \mid z$. Logo, por hipótese, $d = 1$. Assim, pelo Lema 5.41, existem $r, s \in \mathbb{N}$ tais que

$$\frac{z + y}{2} = r^2, \frac{z - y}{2} = s^2 \text{ e } \frac{x}{2} = rs.$$

É fácil verificar que r e s têm paridades distintas com $\text{mdc}(r, s) = 1$ e $r > s > 0$ (prove isto!). Finalmente, das equações acima, temos que

$$x = 2rs, \;\; y = r^2 - s^2 \text{ e } z = r^2 + s^2, \forall \;\; r, s \in \mathbb{N},$$

onde r e s têm paridades distintas com $\text{mdc}(r, s) = 1$ e $r > s > 0$, são todas as soluções primitivas da equação 6.6.

EXERCÍCIOS

1. Determine os últimos dois dígitos do número 3^{400} no sistema de representação decimal.

2. Mostrar que
$$\{2, 2^2, \ldots, 2^{18}\}$$
forma um sistema reduzido de resíduos módulo 27.

3. Seja $p \in \mathbb{N}$ um número primo. Mostrar que
$$\{ap + 1, ap + 2, \ldots, ap + (p - 1)\}$$
é um sistema reduzido de resíduos módulo p para todo $a \in \mathbb{Z}$. (Sugestão: Se $b \in \mathbb{Z}$ é tal que $\text{mdc}(b, p) = 1$, então existe $k \in P_p$ tal que $b \equiv k \,(\text{mod}\, p)$. Como $ap \equiv 0 \,(\text{mod}\, p)$ temos que $b \equiv ap + k \,(\text{mod}\, p)$.)

4. Seja $m \in \mathbb{N}$ um número ímpar. Mostrar que
$$\{2, 4, \ldots, 2m\}$$
é um sistema completo de resíduos módulo m.

5. Seja $m \in \mathbb{N}$, com $m > 2$. Mostrar que
$$\{1^2, 2^2, \ldots, m^2\}$$
não é um sistema completo de resíduos módulo m.

6. Seja $p \in \mathbb{N}$ um número primo. Mostrar que se
$$\{r_1, r_2, \ldots, r_{p-1}\}$$
é um sistema reduzido de resíduos módulo p, então
$$\prod_{i=1}^{p-1} r_i \equiv -1 \,(\text{mod}\, p).$$

7. Sejam $p \in \mathbb{N}$ um número primo ímpar,
$$\{r_1, r_2, \ldots, r_p\} \text{ e } \{s_1, s_2, \ldots, s_p\}$$
dois sistemas completos de resíduos módulo p. Mostrar, com um exemplo,
$$\{r_1 s_1, r_2 s_2, \ldots, r_p s_p\}$$
pode não ser um sistema completo de resíduos módulo m.

8. Sejam $k, p \in \mathbb{N}$, com p um número primo. Mostrar que

$$\{1^k, 2^k, \ldots, (p-1)^k\}$$

é um sistema reduzido de resíduos módulo p se, e somente se, $\text{mdc}(k, p-1) = 1$.

9. Sejam $k, n \in \mathbb{N}$ e

$$\{r_1, r_2, \ldots, r_m\}$$

é um sistema reduzido de resíduos módulo n, onde $m = \phi(n)$. Mostrar que

$$\{r_1^k, r_2^k, \ldots, r_m^k\}$$

é um sistema reduzido de resíduos módulo n se, e somente se, $\text{mdc}(k, m) = 1$.

10. Determinar os elementos invertíveis de $\mathbb{Z}_6$, $\mathbb{Z}_7$, $\mathbb{Z}_{10}$, $\mathbb{Z}_{13}$ e $\mathbb{Z}_{24}$.

11. Seja $p \in \mathbb{N}$ um número primo. Mostrar que $\text{mdc}(k!, p) = 1$, para todo k com $1 < k < p$.

12. Seja $p \in \mathbb{N}$ um número primo. Mostrar que

$$\binom{p}{k} \equiv 0 \pmod{p}$$

para todo k com $1 \leq k < p$. (Sugestão: Se $1 \leq j \leq \max\{k, p-k\}$, então $j < p$. Logo, $\text{mdc}(k!, p) = \text{mdc}((p-k)!, p) = 1$, continue). Mostrar que isto é falso se p não é um número primo.

13. Sejam $m, n, p \in \mathbb{N}$, com p um número primo. Mostrar que $p^n \equiv 1 \pmod{(p^m - 1)}$ se, e somente se, m divide n.

14. Sejam $a, b \in \mathbb{Z}$ e $p \in \mathbb{N}$ um número primo. Mostrar que

$$a^p \equiv b^p \pmod{p} \Rightarrow a^p \equiv b^p \pmod{p^2}.$$

15. Sejam $a, b \in \mathbb{Z}$ e $p \in \mathbb{N}$ um número primo. Mostrar que

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

16. Sejam $p \in \mathbb{N}$ um número primo e $n = p^k m$. Mostrar que

$$\binom{n}{p^k} \equiv m \pmod{p}.$$

(Sugestão: Note que $(x+1)^n = (x^{p^k} + 1)^m \pmod{p}$.)

17. Seja $p \in \mathbb{N}$ um número primo. Mostrar que a função

$$f : \mathbb{Z}_p \to \mathbb{Z}_p \text{ dada por } f(\overline{x}) = \overline{x}^p$$

satisfaz as seguintes condições:

(a) $f(\overline{x} + \overline{y}) = \overline{x}^p + \overline{y}^p$.

(b) $f(\overline{x} \odot \overline{y}) = \overline{x}^p \odot \overline{y}^p$.

18. Sejam $p \in \mathbb{N}$ um número primo e $a \in \mathbb{Z}$. Mostrar que se $\text{mdc}(a, p) = 1$ e $n \equiv m \,(\text{mod}(p-1))$, então

$$a^n \equiv a^m \,(\text{mod}\, p).$$

19. Determine o último dígito do número $2^{1.000.000}$ no sistema de representação de base 7.

20. Sejam $n \in \mathbb{N}$ e $a \in \mathbb{Z}$. Mostrar que se $\text{mdc}(a, n) = 1$ e k o menor inteiro positivo tal que $m \equiv k \,(\text{mod}\, \phi(n))$, então

$$a^m \equiv a^k \,(\text{mod}\, n).$$

21. Seja $n \in \mathbb{N}$ um produto de dois números primos distintos p e q. Mostrar que podemos calcular $\phi(n)$ de p e q, e reciprocamente, calcular p e q de n e $\phi(n)$.

22. Mostrar que:

(a) $2^{11} - 1$ é um número composto.

(b) $2^{23} - 1$ é um número composto.

(c) $2^{911} - 1$ é um número composto.

23. Seja $a \in \mathbb{Z}$. Mostrar que se $\text{mdc}(a, 7) = 1$, então $a^{6k} \equiv 1 \,(\text{mod}\, 7)$.

24. Sejam $a \in \mathbb{Z}$ e $n \in \mathbb{N}$. Mostrar que se $\text{mdc}(a, n) = 1$ e $a^{n-1} \not\equiv 1 \,(\text{mod}\, n)$, então n não é um número primo.

25. Mostrar que $2^{32} + 1$ é um número composto. (Sugestão: Note que

$$5 \cdot 2^7 \equiv -1 \,(\text{mod}\, 641) \text{ e } 5^4 \equiv -2^4 \,(\text{mod}\, 641).)$$

26. Sejam $p, q \in \mathbb{N}$ dois números primos distintos. Mostrar que

$$p^{q-1} + q^{p-1} \equiv 1 \,(\text{mod}\, pq).$$

27. Sejam $m, n \in \mathbb{N}$ com $\text{mdc}(m, n) = 1$. Mostrar que

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \,(\text{mod}\, mn).$$

28. Resolver o sistema de congruências

$$\begin{cases} 2x + 3y & \equiv & 1 \pmod{26} \\ 7x + 8y & \equiv & 2 \pmod{26}. \end{cases}$$

29. Resolver o sistema de congruências

$$\begin{cases} x + 4y & \equiv & 29 \pmod{143} \\ 2x - 9y & \equiv & -84 \pmod{143}. \end{cases}$$

30. Seja $n \in \mathbb{N}$. Mostrar que

$$n = \sum_{d|n} \phi(d).$$

(Sugestão: Seja

$$X = \{1, 2, \ldots, n\}$$

e para cada divisor d de n seja

$$X_d = \{k \in X : \text{mdc}(k, n) = d\}.$$

Então

$$X = \bigcup_{d|n} X_d \text{ e } X_d \cap X_e = \emptyset \text{ se } d \neq e.$$

Portanto,

$$n = \sum_{d|n} \#(X_d).$$

Agora mostre que a função

$$f : X_d \to \mathbb{Z}_{\frac{n}{d}}^{\bullet} \text{ dada por } f(k) = \frac{k}{d}$$

é uma correspondência biunívoca.)

31. Seja $\mu : \mathbb{N} \to \{-1, 0, 1\}$ a função (de Möbius) definida por

$$\mu(n) = \begin{cases} 1, & \text{se } n = 1 \\ 0, & \text{se } p^2 \mid n \text{ para algum primo } p \\ (-1)^k, & \text{se } n \text{ é um produto de } k \text{ primos distintos.} \end{cases}$$

Mostrar que:

(a) Se $\text{mdc}(m, n) = 1$, então $\mu(mn) = \mu(m)\mu(n)$.

(b) $\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$.

32. Seja $n \in \mathbb{N}$. Mostrar que se $\phi(n) \equiv 0 \pmod{(n-1)}$, então não existe nenhum número primo p tal que $p^2 \equiv 0 \pmod{n}$. (Sugestão: Suponha que exista um número primo p tal que $p^2 \equiv 0 \pmod{n}$. Então

$$n = p^k p_1^{k_1} \cdots p_r^{k_r},$$

onde $k \geq 2$, $k_i \in \mathbb{N}$ e $p_1, \ldots, p_r$ são primos distintos.)

33. Seja $n \in \mathbb{N}$. Mostrar que se n não é um quadrado perfeito e

$$n - n^{\frac{2}{3}} < \phi(n) < n - 1,$$

então n é um produto de dois números primos distintos. (Sugestão: Primeiro mostre que n não é um número primo, depois suponha, por absurdo, que n não é um produto de dois números primos distintos, então n é um produto de três ou mais números primos, não necessariamente distintos. Seja p o menor dos números primos. Então $p \leq n^{\frac{1}{3}}$ e $\phi(n) \leq n(1 - \frac{1}{p})$.)

34. Seja $n \in \mathbb{N}$. Mostrar que

$$a^n \equiv a^{n-\phi(n)} \pmod{n}, \forall\ a \in \mathbb{Z}.$$

35. Seja $p \in \mathbb{N}$ um número primo. Mostrar que:

    (a) $k^2 \equiv 1 \pmod{p} \Leftrightarrow k \equiv \pm 1 \pmod{p}$.

    (b) Se $1 \leq k, l < p$ e $k \not\equiv \pm 1 \pmod{p}$, então $k \cdot l \equiv 1 \pmod{p} \Rightarrow k \neq l$.

36. Seja $m \in \mathbb{N}$ com $m > 1$. Mostrar que m é um número primo se, e somente se, $(m-1)! \equiv -1 \pmod{m}$. (Sugestão: Use o exercício precedente.)

37. Sejam $k, m, n \in \mathbb{N}$. Mostrar que:

    (a) Se $m > 2$, então $\phi(m)$ é par.

    (b) Se m é ímpar, então $\phi(2m) = \phi(m)$.

    (c) Se m é par, então $\phi(2m) = 2\phi(m)$.

    (d) Se $m \equiv 0 \pmod{3}$, então $\phi(3m) = 3\phi(m)$.

    (e) Se $m \not\equiv 0 \pmod{3}$, então $\phi(3m) = 2\phi(m)$.

    (f) $\phi(m) = \frac{m}{2}$ se, e somente se, $m = 2^k$.

    (g) Se $n \mid m$, então $\phi(n) \mid \phi(m)$.

    (h) $\phi(\text{mdc}(m,n))\phi(mn) = \text{mdc}(m,n)\phi(m)\phi(n)$.

    (i) $\phi(m)\phi(n) = \phi(\text{mdc}(m,n))\phi(\text{mmc}(m,n))$.

38. Mostrar que se $n \in \mathbb{N}$ tem k fatores primos ímpares distintos, então 2^k divide $\phi(n)$.

39. Seja $n \in \mathbb{N}$, com $n > 1$. Mostrar que

$$\sum_{0<k<n} k = \frac{n\phi(n)}{2},$$

onde $\text{mdc}(n, k) = 1$. (Sugestão: Note que

$$\text{mdc}(n, k) = 1 \Leftrightarrow \text{mdc}(n, n - k) = 1.)$$

40. Determinar todas as soluções inteiras da equação $\phi(n) = 12$.

41. Mostrar que a equação $\phi(n) = 14$ não tem solução inteira.

Capítulo 7

Criptografia

Neste capítulo aplicaremos nossos conhecimento de Aritmética Modular para apresentar uma introdução aos sistemas clássicos de criptografia (modelos simétricos), bem como o sistema de criptografia com chave pública RSA (modelo assimétrico). Não trataremos aqui dos problemas de segurança, complexidade, etc. o leitor interessado em mais detalhes pode consultar [10, 11].

7.1 Cripto-sistemas

Nesta seção apresentaremos alguns resultados básicos sobre sistemas clássicos de criptografia.

Criptografia é a arte ou ciência de escrever mensagens em cifra ou em código, de modo que somente a pessoa autorizada possa decifrar e ler as mensagens.

A criptografia é tão antiga quanta a própria escrita, já estava presente no sistema de escrita hieroglífica dos egípcios. Os romanos utilizavam códigos secretos para comunicar planos de batalhas. O mais interessante é que a tecnologia de criptografia não mudou muito até meados do século vinte. Depois da Segunda Guerra Mundial, com a invensão do computador, a área realmente floresceu incorporando complexos algoritmos matemáticos. Durante a guerra, os ingleses ficaram conhecidos por seus esforços para decifração de mensagens. Na verdade, esse trabalho criptográfico formou a base para a ciência da computação moderna.

A mensagem para ser enviada é chamada de *texto-original* (plaintext) e a mensagem codificada é chamada de *texto-cifrado* (ciphertext). O texto-original e o texto-cifrado são escritos em algum alfabeto $\mathbb{F}$ consistindo de um certo número n de símbolos; isto é,

$$\#(\mathbb{F}) = n.$$

O processo de converter um texto-original para um texto-cifrado é chamado de *codificação* ou *cifragem*, e o processo de reverter é chamado de *decodificação* ou *decifragem*.

O texto-original e texto-cifrado são divididos em mensagens unitárias. Uma mensagen unitária poder ser um bloco de k símbolos do alfabeto $\mathbb{F}$. O *processo de codificação* é

uma função que associa cada mensagem unitária $\mathbf{u}$ do texto-original a uma mensagem unitária $\mathbf{c}$ do texto-cifrado. Mais precisamente, sejam $\mathcal{P}$ o conjunto de todas as possíveis mensagens unitárias $\mathbf{u}$ do texto-original e $\mathcal{C}$ o conjunto de todas as possíveis mensagens unitárias $\mathbf{c}$ do texto-cifrado. Então a correspondência biunívoca

$$f : \mathcal{P} \to \mathcal{C} \text{ tal que } f(\mathbf{u}) = \mathbf{c}$$

é o processo de codificação. A correspondência biunívoca

$$f^{-1} : \mathcal{C} \to \mathcal{P} \text{ tal que } f^{-1}(\mathbf{c}) = \mathbf{u}$$

é o processo de decodificação. Assim, temos o seguinte diagrama

$$\mathcal{P} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{P}$$

Cripto-sistema

Um *Cripo-sistema* é qualquer bijeção de $\mathcal{P}$ sobre $\mathcal{C}$.

É útil substituir os símbolos de um alfabeto $\mathbb{F}$ por números inteiros $0, 1, 2, \ldots$, para tornar mais fácil a construção do cripto-sistema f. Uma correspondência natural entre o alfabeto

$$\mathbb{F} = \{A, B, C, \ldots, K, \ldots, X, Y, Z, \text{ espaço} = \sqcup\}$$

e o conjunto de números inteiros

$$\mathbb{Z}_{27} = \{0, 1, 2, \ldots, 10, \ldots, 23, 24, 25, 26\}$$

é dada pela tabela:

$$\begin{array}{cccccccccc} A & B & C & \cdots & K & \cdots & X & Y & Z & \sqcup \\ \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow & \cdots & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 0 & 1 & 2 & \cdots & 10 & \cdots & 23 & 24 & 25 & 26. \end{array} \tag{7.1}$$

Em geral, podemos rotular mensagens unitárias, com blocos de k símbolos, de um alfabeto $\mathbb{F}$ de n símbolos, por inteiros do conjunto

$$\mathbb{Z}_{n^k} = \{0, 1, \ldots, n^k - 1\}$$

do seguinte modo:

$$(x_{k-1}, \ldots, x_1, x_0) \in \mathbb{Z}_n^k \leftrightarrow x_{k-1}n^{k-1} + \cdots + x_1 n + x_0 n^0 \in \mathbb{Z}_{n^k},$$

onde cada x_i corresponde a um símbolo do alfabeto $\mathbb{F}$. Por exemplo, a mensagem unitária com bloco de quatro símbolos

$$AQUI$$

corresponde ao inteiro

$$0 \cdot 27^3 + 16 \cdot 27^2 + 20 \cdot 27 + 8 \cdot 27^0 = 12212 \in \mathbb{Z}_{27^4}.$$

Teorema 7.1 *Sejam $n \in \mathbb{N}$ e $a, b \in \mathbb{Z}_n$ fixados. Se $mdc(a, n) = 1$, então a função*

$$f : \mathbb{Z}_n \to \mathbb{Z}_n \text{ dada por } f(x) = ax + b$$

é um cripto-sistema.

Prova. Como $\text{mdc}(a, n) = 1$ temos que existe $a' = a^{-1} \in \mathbb{Z}_n^{\bullet}$ tal que $a \cdot a' = 1$. Assim,

$$f^{-1}(x) = a'x + b',$$

onde $b' = -a'b$, é tal que

$$f \circ f^{-1} = f^{-1} \circ f = I_{\mathbb{Z}_n};$$

isto é, f^{-1} é a função inversa de f. ■

Observação 7.2 *O cripto-sistema*

$$f(x) = ax + b$$

é chamado de transformação afim. *O par (a, b) é chamado de* chave de codificação *ou* chave secreta. *Quando $n = 27$, $a = 1$ e $b \in \mathbb{Z}_{27}$ o cripto-sistema*

$$f(x) = x + b$$

é chamado de Cifra de César*, pois Júlio César a utilizava. Quando $b = 0$ o cripto-sistema*

$$f(x) = ax$$

é uma transformação linear.

Exemplo 7.3 *A correspondência biunívoca entre o alfabeto $\mathbb{F}$ e números inteiros é dada pela Tabela* 7.1. *Seja o símbolo $x \in \mathbb{Z}_{27}$ correspondendo uma mensagem unitária, com blocos de um símbolo, do texto-original. Assim, com $a = 13$ e $b = 9$, temos que a função*

$$f : \mathbb{Z}_{27} \to \mathbb{Z}_{27} \text{ dada por } f(x) = 13x + 9$$

é um cripo-sistema. Portanto, para codificar o texto-original

$$A\ MATEMÁTICA\ É\ LINDA,$$

primeiro calculamos

$$f(0) = 9, f(26) = 23, \ldots, f(3) = 21, f(0) = 9,$$

logo a mensagem cifrada é

$$JXDJNHDJNFIJXHXRFQVJ.$$

Para decodificar a mensagem cifrada, primeiro calculamos

$$f^{-1}(x) = 25x + 18$$

e depois

$$f^{-1}(9) = 0, f^{-1}(23) = 26, \ldots, f^{-1}(21) = 3, f^{-1}(9) = 0.$$

Logo a mensagem decifrada é

$$A\ MATEMÁTICA\ É\ LINDA.$$

Agora suponhamos que nossos texto-original e texto-cifrado são divididos em mensagens unitárias, com blocos de dois símbolos. Isto significa que o texto-original é dividido em segmentos de dois símbolos. Se o texto-original tem um número ímpar de símbolos, então para obter um número inteiro de blocos com dois símbolos adicionamos um símbolo extra no final; escolhemos um símbolo que não é provável para causar confusão, digamos espaço.

Exemplo 7.4 *Vamos primeiro estabelecer uma correspondência biunívoca entre o alfabeto* $\mathbb{F}$ *e números inteiros, pela tabela:*

$$\begin{array}{cccccccccc} A & B & C & \cdots & K & \cdots & X & Y & Z & \\ \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow & \cdots & \updownarrow & \updownarrow & \updownarrow & \\ 0 & 1 & 2 & \cdots & 10 & \cdots & 23 & 24 & 25. & \end{array} \tag{7.2}$$

Seja o símbolo

$$x26 + y \in \mathbb{Z}_{676}$$

correspondendo uma mensagem unitária, com blocos de dois símbolos, do texto-original, onde $x \in \mathbb{Z}_{26}$ *corresponde ao primeiro símbolo da mensagem unitária e* $y \in \mathbb{Z}_{26}$ *corresponde ao segundo símbolo da mensagem unitária. Assim, com* $a = 159$ *e* $b = 580$*, temos que a função*

$$f : \mathbb{Z}_{676} \to \mathbb{Z}_{676} \ \textit{dada por}\ f(z) = 159z + 580$$

é um cripo-sistema. Portanto, para codificar o texto-original

$$AMOR,$$

primeiro dividimos o texto-original em blocos de dois símbolos e fazemos a correspondência numérica

$$\begin{array}{cc} AM & OR \\ \updownarrow & \updownarrow \\ 12 & 381. \end{array}$$

Agora, calculamos

$$f(12) = 460 = 17 \cdot 26 + 18 \ \ e \ \ f(381) = 319 = 12 \cdot 26 + 7,$$

logo a mensagem cifrada é

$$RSMH.$$

Um modo alternativo de transmitir mensagens unitárias, com blocos de dois símbolos, é fazer cada bloco de dois símbolos corresponder a um vetor

$$\mathbf{x} = \begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{Z}_n^2.$$

Teorema 7.5 *Sejam* $n \in \mathbb{N}$,

$$A = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \in M_2(\mathbb{Z}_n), B = \begin{bmatrix} a \\ b \end{bmatrix} \in \mathbb{Z}_n^2$$

e $D = \det(A)$. *Se* $mdc(n, D) = 1$, *então a função*

$$f : \mathbb{Z}_n^2 \to \mathbb{Z}_n^2 \text{ dada por } f(\mathbf{x}) = A\mathbf{x} + B,$$

é um cripto-sistema.

Prova. Temos, pelo Teorema 6.36, que a função

$$f : \mathbb{Z}_n^2 \to \mathbb{Z}_n^2 \text{ dada por } f(\mathbf{x}) = A\mathbf{x} + B,$$

é uma função invertível com inversa

$$f^{-1} : \mathbb{Z}_n^2 \to \mathbb{Z}_n^2 \text{ dada por } f^{-1}(\mathbf{x}) = A^{-1}\mathbf{x} - A^{-1}B.$$

■

Observação 7.6 *O Teorema acima pode ser generalizado para* $\mathbb{Z}_n^k$.

Exemplo 7.7 *A correspondência biunívoca entre o alfabeto* $\mathbb{F}$ *e números inteiros é dada pela Tabela* 7.2. *Seja o vetor*

$$\mathbf{x} = \begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{Z}_{26}^2$$

correspondendo uma mensagem unitária, com blocos de dois símbolos, do texto-original, onde $x \in \mathbb{Z}_{26}$ *corresponde ao primeiro símbolo da mensagem unitária e* $y \in \mathbb{Z}_{26}$ *corresponde ao segundo símbolo da mensagem unitária. Assim, com*

$$A = \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix} \in M_2(\mathbb{Z}_{26}) \text{ e } B = \begin{bmatrix} 7 \\ 11 \end{bmatrix} \in \mathbb{Z}_n^2$$

temos que a função

$$f : \mathbb{Z}_{26}^2 \to \mathbb{Z}_{26}^2 \text{ dada por } f(\mathbf{x}) = A\mathbf{x} + B$$

é um cripto-sistema. Portanto, para codificar o texto-original

$$JÁ,$$

primeiro fazemos a correspondência do texto-original com o vetor

$$\mathbf{x} = \begin{bmatrix} 9 \\ 0 \end{bmatrix} \in \mathbb{Z}_{26}^2$$

e depois calculamos

$$f(\mathbf{x}) = \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix} \begin{bmatrix} 9 \\ 0 \end{bmatrix} + \begin{bmatrix} 7 \\ 11 \end{bmatrix} = \begin{bmatrix} 25 \\ 22 \end{bmatrix},$$

logo a mensagem cifrada é

$$ZW.$$

Observação 7.8 *Para codificar um texto-original, com m blocos de dois símbolos, podemos escrevê-la como uma matriz* $2 \times m$*, onde cada coluna corresponde a um vetor de* $\mathbb{Z}_n^2$*, e usar o seguinte cripto-sistema*

$$f : M_{2\times m}(\mathbb{Z}_n) \to M_{2\times m}(\mathbb{Z}_n)$$

dado por

$$f([\ \mathbf{x}_1 \ \cdots \ \mathbf{x}_m\ ]) = [\ A\mathbf{x}_1 + B \ \cdots \ A\mathbf{x}_m + B\ ].$$

Exemplo 7.9 *Vamos continuar o exemplo acima. Assim, para codificar o texto-original*

$$AMANDA,$$

primeiro fazemos a correspondência do texto-original com a matriz 2×3

$$\begin{bmatrix} 0 & 0 & 3 \\ 12 & 13 & 0 \end{bmatrix}$$

e depois calculamos

$$f(\begin{bmatrix} 0 & 0 & 3 \\ 12 & 13 & 0 \end{bmatrix}) = \begin{bmatrix} 17 & 20 & 13 \\ 18 & 11 & 6 \end{bmatrix},$$

logo a mensagem cifrada é

$$RSULOF.$$

Um *codificador por substituição* com período p consiste de p cripo-sistemas $f_i : \mathcal{P} \to \mathcal{C}_i$, $i = 1, \ldots, p$. Uma mensagem

$$\mathbf{u} = (u_1, \ldots, u_p, u_{p+1}, \ldots, u_{2p}, \ldots)$$

é codificada como

$$\mathbf{c} = (f_1(u_1), \ldots, f_p(u_p), f_1(u_{p+1}), \ldots, f_p(u_{2p}), \ldots).$$

Por vários séculos um dos métodos mais populares de codificação por substituição foi a *Cifra de Vigenère*. Neste sistema de codificação, primeiro escolhemos um vetor

$$\mathbf{b} \in \mathbb{Z}_n^p,$$

onde $\mathbf{b}$ corresponde a uma palavra de fácil memorização, chamada de *palavra-chave* e depois usaremos o cripto-sistema

$$f : \mathbb{Z}_n^p \to \mathbb{Z}_n^p \text{ dado por } f(\mathbf{x}) = \mathbf{x} + \mathbf{b}.$$

Um modo prático para obter a Cifra de Vigenère é através do Arranjo Circulante dado na tabela abaixo.

A	B	$\cdots$	Y	Z
B	C	$\cdots$	Z	A
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
Y	Z	$\cdots$	W	X
Z	A	$\cdots$	X	Y

Exemplo 7.10 *A correspondência biunívoca entre o alfabeto $\mathbb{F}$ e números inteiros é dada pela Tabela* 7.1. *Agora escolhemos uma palavra-chave, digamos*

$$AMO,$$

a qual corresponde ao vetor

$$\mathbf{b} = (0, 12, 14) \in \mathbb{Z}_{27}^3.$$

Assim, usando o Arranjo Circulante para cifrar o texto-original

A	B	C	$\cdots$	$\sqcup$	
A	B	C	$\cdots$	$\sqcup$	$= f_1(A)f_1(B)f_1(C)\cdots f_1(\sqcup)$
M	N	O	$\cdots$	L	$= f_2(A)f_2(B)f_2(C)\cdots f_2(\sqcup)$
O	P	Q	$\cdots$	N	$= f_3(A)f_3(B)f_3(C)\cdots f_3(\sqcup)$

$$ROSÂNGELA\ ADORA\ FERNANDA,$$

obtemos a mensagem cifrada

$$R \sqcup FAZUEXO \sqcup MROCO \sqcup RSRZONPO,$$

a qual corresponde a

$$f_1(R)f_2(O)f_3(S)f_1(A)f_2(N)f_3(G)\cdots f_1(N)f_2(D)f_3(A).$$

Neste caso, os cripo-sistemas $f_i : \mathbb{Z}_{27} \to \mathbb{Z}_{27}$, $i = 1, 2, 3$, são dados por $f_1(x) = x$, $f_2(x) = x + 12$ e $f_3(x) = x + 14$, isto é, os f_i são Cifras de César.

Os sistemas clássicos de Criptografia, como a Cifra de César e de Vigenère, são todos simétricos; isto é, a chave usada para a codificação é igual à chave usada para a decodificação ou, equivalentemente, a partir de uma delas a outra é obtida facilmente. Nestes sistemas, conhecendo a chave de codificação

$$(a, b)$$

podemos calcular a chave de decodificação

$$(a^{-1} \bmod n^k, -a^{-1}b \bmod n^k)$$

pelo Algoritmo Euclidiano. Note que, estes sistemas são difíceis de ser "quebrados," pois a chave é usada apenas uma vez para cada texto-original. Portanto, os sistemas simétricos são interessantes quando um transmissor conversa apenas com o mesmo receptor. Caso um transmissor converse com vários receptores e a chave de codificação é mantida constante, então todos os receptores estarão aptos para decodificar o texto-cifrado. Caso a chave de codificação não seja mantida constante, então o sistema torna-se inviável. Na próxima seção apresentaremos um sistema de criptografia em que um transmissor conversa com vários receptores, onde chave de codificação não é mantida constante.

EXERCÍCIOS

1. Determinar os valores de a para os quais, a matriz

$$A = \begin{bmatrix} 3 & 4 \\ a & 23 \end{bmatrix}$$

com entradas em $\mathbb{Z}_{26}$, satisfaça a condição $A^2 = I$.

2. Seja o alfabeto

$$\mathbb{F} = \{A, B, \ldots, Y, Z, \sqcup\}$$

com correspondência numérica

$$\mathbb{Z}_{27} = \{0, 1, \ldots, 24, 25, 26\}.$$

Suponhamos que interceptamos o texto-cifrado

$$ZKLXZBKPKWTYOZ.$$

Sabendo que foi cifrada usando a Cifra de César, com chave $b = 11$, deteminar o texto-original.

3. Seja o alfabeto

$$\mathbb{F} = \{A, B, \ldots, Y, Z, \sqcup\}$$

com correspondência numérica

$$\mathbb{Z}_{27} = \{0, 1, \ldots, 24, 25, 26\}.$$

Use o cripto-sistema de $\mathbb{Z}_{27}$ sobre $\mathbb{Z}_{27}$, com chave $a = 7$ e $b = 12$, para cifrar a mensagem

$$A\ MATEMÁTICA\ ELEMENTAR\ É\ COMPLETA.$$

4. Determinar uma fórmula para o número de diferentes cripto-sistemas da forma

$$f : \mathbb{Z}_n \to \mathbb{Z}_n \text{ dado por } f(x) = ax + b.$$

5. Uma mensagem unitária de um texto-original u é dita *fixada* por um cripto-sistema f se $f(u) = u$. Seja o cripto-sistema

$$f : \mathbb{Z}_n \to \mathbb{Z}_n \text{ dado por } f(x) = ax + b, \text{ com } a \neq 1.$$

Mostre que:

(a) Se n é um número primo, então existe exatamente um símbolo fixado;

(b) Se $b = 0$ e n qualquer, então existe pelo menos um símbolo fixado;

(c) Se $b = 0$ e n par, então existe pelo menos dois símbolos fixados;

(d) Dê exemplo de um cripto-sistema sem símbolos fixados.

6. Determinar uma fórmula para o número de diferentes cripto-sistemas da forma

$$f : \mathbb{Z}_{n^2} \to \mathbb{Z}_{n^2} \text{ dado por } f(x) = ax + b.$$

7. Seja o alfabeto

$$\mathbb{F} = \{A, B, \ldots, Y, Z, \sqcup\}$$

com correspondência numérica

$$\mathbb{Z}_{27} = \{0, 1, \ldots, 24, 25, 26\}.$$

Suponhamos que interceptamos o texto-cifrado

$$JANJRMFCFDNHMDVPADSTEPXAFDPZP \sqcup UJ.$$

Sabendo que foi cifrada usando um cripto-sistema de $\mathbb{Z}_{729}$ sobre $\mathbb{Z}_{729}$, com chave $a = 614$ e $b = 47$, deteminar o texto-original.

8. Seja o alfabeto

$$\mathbb{F} = \{A, B, \ldots, Y, Z\}$$

com correspondência numérica

$$Z_{27} = \{0, 1, \ldots, 24, 25\}.$$

Usando um cripto-sistema linear de $\mathbb{Z}_{26}^2$ sobre $\mathbb{Z}_{26}^2$, com chave

$$A = \begin{bmatrix} 2 & 23 \\ 3 & 1 \end{bmatrix},$$

codifique o texto-original

$$CRIPTOGRAFIA$$

e decodifique o texto-cifrado.

9. Seja o alfabeto

$$\mathbb{F} = \{A, B, \ldots, Y, Z, \sqcup, ?, !\}$$

com correspondência numérica

$$Z_{29} = \{0, 1, \ldots, 24, 25, 26, 27, 28\}.$$

Suponhamos que interceptamos o texto-cifrado

$$?QBHO \sqcup UNQLFMYBLOWJ?ICHEYZOXAC?I \sqcup .$$

Sabendo que foi cifrada usando um cripto-sistema linear de $\mathbb{Z}_{27}^2$ sobre $\mathbb{Z}_{27}^2$, com chave

$$A = \begin{bmatrix} 3 & 7 \\ 4 & 1 \end{bmatrix},$$

deteminar o texto-original.

7.2 Sistema Criptográfico com Chave Pública

Sistema criptográfico com chaves públicas foi proposto por Diffie e Hellman em 1976. Os sistemas criptográficos com chaves públicas se caracterizam por duas chaves diferentes: a chave (chave de codificação) da transmissora é pública e a chave (chave de decodificação) da receptora é secreta. Portanto, os sistemas criptográficos com chaves públicas possui uma estrutura assimétrica, isto é, a obtenção de uma chave a partir da outra, se constitui em um problema não realizável (confira Figura 7.1).

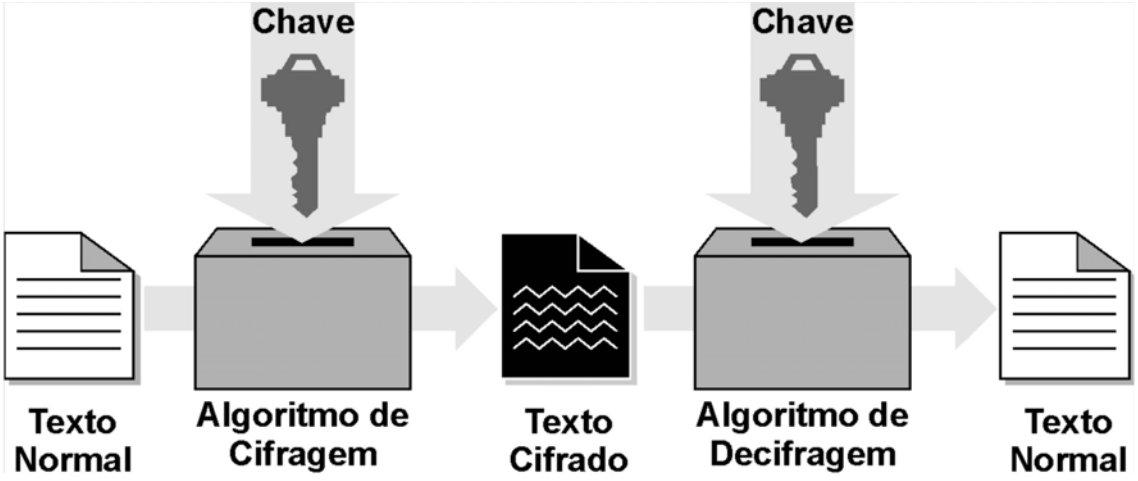

Figura 7.1: Cifragem e decifragem de uma mensagem

Os sistemas criptográficos com chaves públicas opera do seguinte modo: um usuário u_i desejando-se comunicar com um usuário u_j de maneira secreta, envia uma solicitação para início de comunicação. O usuário u_j determina um par chaves $k_{c,j}$ e $k_{d,j}$ tais que

$$k_{d,j} \circ k_{c,j}(\mathbf{u}) = \mathbf{u} \text{ e } k_{c,j} \circ k_{d,j}(\mathbf{u}) = \mathbf{u}$$

onde a chave $k_{d,j}$ é mantida secreta e usada para a decodificação, enquanto a chave $k_{c,j}$ é tornada pública e usada para a codificação. O usuário u_j obtém a chave pública $k_{c,j}$ e, assim, passa a codificar mensagens unitárias para o usuário u_j, pois só este conhece a chave secreta $k_{d,j}$. Estes processos de codificação e decodificação deverão satisfazer as seguintes condições:

1. O cálculo do par de chaves $k_{c,j}$ e $k_{d,j}$ deve ser simples;

2. O usuário (transmissor) u_i deve realizar a operação de codificação facilmente; isto é,
$$\mathbf{c} = k_{c,j}(\mathbf{u});$$

3. O usuário (receptor) u_j deve realizar a operação de decodificação facilmente; isto é,
$$\mathbf{u} = k_{d,j}(\mathbf{c});$$

4. É praticamente impossível descobrir $k_{d,j}$ a partir de $k_{c,j}$. É claro que dada $k_{c,j}$ temos uma maneira de descobrir $k_{d,j}(c)$, basta codificar toda mensagem unitária u e quando $c = k_{c,j}(u)$, teremos que $u = k_{d,j}(c)$ mas isto torna-se inviável.

O processo de codificação é dado pela função

$$f : \mathbb{Z}_{n_i} \to \mathbb{Z}_{n_i}, \;\; f(x) = x^{t_i}$$

e, pelo Corolário 6.38, o processo de decodificação é dado pela função

$$f^{-1} : \mathbb{Z}_{n_i} \to \mathbb{Z}_{n_i}, \;\; f(x) = x^{r_i}.$$

Seja F um alfabeto com n símbolos. Na prática queremos trabalhar com $P \neq C$. Assim, vamos dividir nosso texto-original em mensagens unitárias com blocos de k símbolos, os quais são vistos como um inteiro na base n^k

$$x = x_{k-1}n^{k-1} + \cdots + x_1 n + x_0 n^0 \in \mathbb{Z}_{n^k}, \;\; x_r \in \{0, 1, \ldots, n-1\},$$

e cada um destes blocos será codificado em um só bloco com l símbolos, onde $k < l$. Para fazer isto cada usuário u_i escolhe dois números primos distintos p_i e q_i, de modo que $n_i = p_i q_i$ satisfaça

$$n^k < n_i < n^l.$$

Então qualquer mensagem unitária u do texto-original; isto é, um inteiro menor do que n^k, corresponde a um elemento de $\mathbb{Z}_{n_i}$ e, como $n_i < n^l$, a imagem $c = f(u) \in \mathbb{Z}_{n_i}$ poder ser escrita de modo único como um bloco de l símbolos. Note que nem todos os blocos de l símbolos são usados, mas apenas aqueles correspondendo aos inteiros menores do que n^k para cada usuário u_i.

Notamos que uma desvantagem dos sistemas de criptografia com chave pública é que são bem mais lentos do que os sistemas de criptografia clássicos, pois eles usam potências ao invés de somas em compensação, por isso mesmo, são mais seguros. Note, também, que um modo de calcular a chave secreta (n, r) a partir da chave pública (n, t) é fatorar n em fatores primos e depois recupera r tal que

$$rt \equiv 1 \pmod{\phi(n)}.$$

O ponto importante neste procedimento é que não se conhece um algoritmo rápido para determinar a decomposição de n.

7.3 Sistema de Criptografia DH

Em um sistema de criptografia com chave pública Diffie-hellman DH, dois usuários u_i e u_j desejam formar uma chave secreta k_{ij}, onde u_i tem uma chave secreta $k_{d,i}$ e u_j tem uma chave secreta $k_{d,j}$. Primeiro eles escolhem um sistema de parâmetros público: um número primo p extremamente grande (com aproximadamente 100 dígitos) e t um número aleatoriamente tal que

$$\text{mdc}(t, p) = 1.$$

A seguir o usuário u_i calcula

$$k_{c,i} \equiv t^{k_{d,i}} \pmod{p},$$

e envia $k_{c,i}$. Similarmente, o usuário u_j calcula

$$k_{c,j} \equiv t^{k_{d,j}} \pmod{p},$$

e envia $k_{c,j}$. Finalmente, calculam

$$\begin{aligned} k_{ij} &\equiv t^{k_{d,i}k_{d,j}} \pmod p \\ &\equiv k_{c,i}^{k_{d,j}} \pmod p \\ &\equiv k_{c,j}^{k_{d,i}} \pmod p. \end{aligned}$$

Portanto, ambos u_i e u_j são capazes de calcular k_{ij}.

Exemplo 7.11 *Sejam* $t = 6$ *tal que* $\text{mdc}(6, 733) = 1$, $k_{d,i} = 29$ *e* $k_{d,j} = 19$ *as chaves de decodificação dos usuários* u_i *e* u_j, *respectivamente. Então o usuário* u_i *calcula a chave de codificação*

$$k_{c,i} \equiv t^{k_{d,i}} \pmod{733} \equiv 6^{29} \pmod{733} \equiv 578 \pmod{733}$$

e envia $k_{c,i} = 578$. *Do mesmo modo, o usuário* u_j *calcula*

$$k_{c,j} \equiv t^{k_{d,j}} \pmod{733} \equiv 6^{19} \pmod{733} \equiv 327 \pmod{733}$$

e envia $k_{c,j} = 327$. *Finalmente calculam*

$$k_{ij} \equiv t^{k_{d,i}k_{d,j}} \pmod{733} \equiv 6^{19 \cdot 29} \pmod{733} \equiv 247 \pmod{733}.$$

Agora, suponhamos que u_i deseje enviar a u_j uma mensagem u, onde $1 \leq u \leq p-1$. Primeiro, u_i escolhe uma chave secreta $k_{d,i}$, isto é, um número aleatório $k_{d,i}$ tal que

$$1 \leq k_{d,i} \leq p-1.$$

A seguir u_i calcula

$$k_{ij} \equiv k_{c,j}^{k_{d,i}} \pmod p,$$

onde $k_{c,j} \equiv t^{k_{d,j}} \pmod p$ está em um arquivo público ou é enviada por u_j. O texto-cifrado é o par

$$\mathbf{c} = (c_1, c_2),$$

onde

$$c_1 \equiv t^{k_{d,i}} \pmod p \text{ e } c_2 \equiv k_{ij}\mathbf{u} \pmod p. \tag{7.3}$$

É aconselhável utilizar chaves de decodificacão $k_{d.i}$ diferentes, para cada mensagem u do texto-original.

O processo de decodificação é composto de duas etapas.

1.ª Etapa. Recuperar k_{ij}, isto é, calcular

$$\begin{aligned} k_{ij} &\equiv t^{k_{d,i}k_{d,j}} \pmod p \\ &\equiv c_1^{k_{d,j}} \pmod p. \end{aligned}$$

Mas isto é fácil, pois $k_{d,j}$ é conhecida somente por u_j.

2.ª Etapa. Divide c_2 por k_{ij} para recuperar u.

Exemplo 7.12 *A correspondência entre o alfabeto F e números inteiros é dada pela tabela* 7.1. *Sejam $t = 6 \in Z_{733}$ tal que* $\mathrm{mdc}(6, 733) = 1$, *$k_{d,i_1} = 29$, $k_{d,i_2} = 8$ e $k_{d,j} = 19$ as chaves de decodificação, $k_{c,i} = 578$ e $k_{c,j} = 327$ as chaves de codificação dos usuários u_i e u_j, respectivamente. Assim, para codificar o texto-original*

$$AMOR$$

dividido em blocos de dois símbolos, com correspondência numérica

$$\begin{array}{cc} AM & OR \\ \updownarrow & \updownarrow \\ 12 & 395 \end{array}$$

o usuário u_i calcula

$$k_{(ij)_1} \equiv 247 \,(\mathrm{mod}\, 733) \;\; e \;\; k_{(ij)_2} \equiv 373 \,(\mathrm{mod}\, 733).$$

A seguir calcula

$$\begin{aligned} c_{11} &\equiv t^{k_{d,i_1}} \equiv 6^{29} \equiv 578 \,(\mathrm{mod}\, 733) \\ c_{12} &\equiv k_{(ij)_1} \cdot \mathbf{u}_1 \equiv 247 \cdot 12 \equiv 32 \,(\mathrm{mod}\, 733) \\ c_{21} &\equiv t^{k_{d,i_2}} \equiv 6^{8} \equiv 313 \,(\mathrm{mod}\, 733) \\ c_{22} &\equiv k_{(ij)_2} \cdot \mathbf{u}_2 \equiv 313 \cdot 395 \equiv 2 \,(\mathrm{mod}\, 733). \end{aligned}$$

Logo, o texto-cifrado são os pares

$$\mathbf{c}_1 = (c_{11}, c_{12}) \;\; e \;\; \mathbf{c}_2 = (c_{21}, c_{22}),$$

onde

$$\begin{aligned} c_{11} &\equiv 578 \equiv 21 \cdot 27 + 11 \,(\mathrm{mod}\, 733) \\ c_{12} &\equiv 32 \equiv 1 \cdot 27 + 5 \,(\mathrm{mod}\, 733) \\ c_{21} &\equiv 313 \equiv 11 \cdot 27 + 16 \,(\mathrm{mod}\, 733) \\ c_{22} &\equiv 2 \equiv 0 \cdot 27 + 2 \,(\mathrm{mod}\, 733). \end{aligned}$$

Portanto, o usuário u_i envia para o usuário u_j, o texto-cifrado

$$VLBFLQAC.$$

Para decodificar o texto-cifrado com correspondência numérica

$$\begin{array}{cccccccc} V & L & B & F & L & Q & A & C \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 21 & 11 & 1 & 5 & 11 & 16 & 0 & 2 \end{array},$$

o usuário u_j recupera

$$c_{11} = 578,\ \ c_{12} = 32,\ \ c_{21} = 313\ \ e\ \ c_{22} = 2.$$

A seguir calcula

$$(c_{11})^{k_{d,j}} \equiv 578^{19} \equiv 247 \equiv k_{(ij)_1} \pmod{733}$$

e

$$\mathbf{u}_1 \equiv \frac{c_{12}}{k_{(ij)_1}} \equiv 32 \cdot 92 \equiv 12 \pmod{733}.$$

Do mesmo modo calcula

$$(c_{21})^{k_{d,j}} \equiv 313^{19} \equiv 373 \equiv k_{(ij)_2} \pmod{733}$$

e

$$\mathbf{u}_2 \equiv \frac{c_{22}}{k_{(ij)_2}} \equiv 2 \cdot 564 \equiv 395 \pmod{733}.$$

Como

$$\mathbf{u}_1 \equiv 12 \equiv 0 \cdot 27 + 12 \pmod{733}$$

e

$$\mathbf{u}_2 \equiv 395 \equiv 14 \cdot 27 + 17 \pmod{733},$$

o texto-original é

$$\begin{array}{cccc} A & M & O & R \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 0 & 12 & 14 & 17 \end{array}.$$

7.4 Sistema RSA

Nesta seção apresentaremos um sistema de criptografia com chave pública proposto por Rivest, Shamir e Adleman RSA em 1978.

Em um sistema de criptografia com chave pública RSA, cada usuário u_i escolhe dois números primos distintos extremamente grandes p_i e q_i (com aproximadamente 100 dígitos cada, cf. Lema 7.13 abaixo) e aleatoriamente um número t_i tal que

$$\mathrm{mdc}(t_i, (p_i - 1)(q_i - 1)) = 1.$$

A seguir u_i calcula

$$n_i = p_i q_i \ \text{ e } \ \phi(n_i) = \phi(p_i)\phi(p_i) = n_i + 1 - (p_i + q_i),$$

e também

$$r_i \equiv t_i^{-1} \pmod{\phi(n_i)}.$$

Agora, o usuário u_i torna público a chave de codificação

$$k_{c,i} = (n_i, t_i)$$

e mantém secreta a chave de decodificação

$$k_{d,i} = (n_i, r_i).$$

Lema 7.13 *Seja* $f : \mathbb{N}^* \times \mathbb{N} \to \mathbb{N}$ *a função definida por*

$$f((m,n)) = \frac{n-1}{2}\left[\left|a^2-1\right| - (a^2-1)\right] + 2,$$

onde $a = m(n+1) - (n!+1)$. *Então* $f(\mathbb{N}^* \times \mathbb{N}) \subseteq \mathbb{P}$, *onde* $\mathbb{P}$ *é o conjunto de todos os números primos de* $\mathbb{N}$.

Prova. É claro que $a \in \mathbb{Z}$, para todos $m, n \in \mathbb{N}$, com $m \neq 0$. Como $a^2 \geq 0$ temos dois casos a ser considerado:

1.º **Caso**. Se $a^2 > 0$, então $a^2 \geq 1$ e $a^2 - 1 \geq 0$. Logo, $|a^2-1| = a^2-1$. Portanto,

$$\begin{aligned} f((m,n)) &= \frac{n-1}{2}\left[\left|a^2-1\right| - (a^2-1)\right] + 2 \\ &= 2, \end{aligned}$$

isto é, $f((m,n)) = 2$ é um número primo.

2.º **Caso**. Se $a^2 = 0$, então

$$\begin{aligned} f((m,n)) &= \frac{n-1}{2}\left[\left|a^2-1\right| - (a^2-1)\right] + 2 \\ &= n+1. \end{aligned}$$

Afirmação. $f((m,n)) = n+1$ é um número primo, para todos $m, n \in \mathbb{N}$, com $m \neq 0$. De fato, note que

$$0 = a = m(n+1) - (n!+1) \Leftrightarrow n!+1 = m(n+1) \Leftrightarrow (n+1) \mid (n!+1).$$

Assim, fazendo $p = n+1$, obtemos $n = p-1$ e

$$p \mid (p-1)!+1 \Leftrightarrow p \text{ é um número primo.}$$

Se p é um número primo e $p = 2$, então

$$2 \mid (2-1)!+1.$$

Se $p > 2$ e

$$X = \{1, 2, \ldots, p-1\},$$

então para cada $k \in X$ existe um único $l \in X$ tal que

$$k \cdot l \equiv 1 \pmod{p},$$

pois como $k < p$ temos que $\text{mdc}(k,p) = 1$. Logo, existem $r, s \in \mathbb{Z}$ tais que

$$kr + ps = 1.$$

Assim , existe um único $l \equiv r \pmod{p} \in X$ tal que

$$k \cdot l \equiv 1 \pmod{p}.$$

Agora, se $k = l$, então

$$k^2 \equiv 1 \,(\mathrm{mod}\, p) \Leftrightarrow k \equiv \pm 1 \,(\mathrm{mod}\, p) \Leftrightarrow k = 1 \text{ ou } k = p - 1.$$

Se $k \not\equiv \pm 1 \,(\mathrm{mod}\, p)$, então $k \neq l$ e

$$2 \cdot 3 \cdots (p-2) = \prod_{k,l \in X - \{1, p-1\}} kl \equiv \prod 1 \,(\mathrm{mod}\, p),$$

isto é,

$$2 \cdot 3 \cdots (p-2) \equiv 1 \,(\mathrm{mod}\, p).$$

Como $(p-1) \equiv (-1) \,(\mathrm{mod}\, p)$ temos que

$$1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) \equiv 1(-1) \,(\mathrm{mod}\, p) \equiv (-1) \,(\mathrm{mod}\, p).$$

Portanto,

$$p \mid (p-1)! + 1.$$

Reciprocamente, se

$$p \mid (p-1)! + 1$$

e p não é um número primo, então existe $r \in \mathbb{Z}$ tal que $1 < r < p$ e $r \mid p$. Logo,

$$r \mid (p-1)! \text{ e } r \mid (p-1)! + 1 \Rightarrow r \mid 1,$$

o que é uma contradição. Portanto, $f((m,n))$ é um número primo, para todos $m, n \in \mathbb{N}$, com $m \neq 0$. ■

Exemplo 7.14 *A correspondência biunívoca entre o alfabeto* $\mathbb{F}$ *e números inteiros é dada pela tabela* 7.2 *e escolhemos* $k = 3$ *e* $l = 4$. *Para enviar o texto-original*

$$AMO$$

para um usuário u_j *com chave de codificação*

$$k_{c,j} = (46927, 39423),$$

primeiro determinamos a equivalência numérica

$$\begin{array}{c} AMO \\ \updownarrow \\ 326 \end{array}$$

e então calculamos

$$326^{39423} \,(\mathrm{mod}\, 46927) = 41309.$$

Como

$$41309 = 2 \cdot 26^3 + 9 \cdot 26^2 + 2 \cdot 26 + 21$$

temos que o texto-cifrado é

$$CJCV.$$

O receptor u_j conhece a chave de decodificação

$$k_{d,j} = (46927, 26767)$$

e, assim, calcula

$$41309^{26767} \pmod{46927} = 326.$$

Como

$$326 = 0 \cdot 26^2 + 12 \cdot 26 + 14$$

temos que o texto-original é

$$AMO.$$

Observação 7.15 *Como o usuário u_i gerou suas chaves? Primeiro ele multiplicou os números primos $p_i = 281$ e $q_i = 167$ para obter n_i; e então escolheu t_i aleatoriamente tal que*

$$mdc(t_i, p_i) = mdc(t_i, q_i) = 1.$$

Finalmente determinou

$$r_i \equiv t_i^{-1} \pmod{(p_i - 1)(q_i - 1)}.$$

Note que os números p_i, q_i e r_i permanecem secretos.

EXERCÍCIOS

1. Seja o alfabeto

$$\mathbb{F} = \{A, B, \ldots, Y, Z, \sqcup, \text{“}, \text{J}, ?, \$, 0, \ldots, 9\}$$

com correspondência numérica

$$\mathbb{Z}_{41} = \{0, 1, \ldots, 24, 25, 26, 27, 28, 29, 30, \ldots, 40\}.$$

Suponhamos que as mensagens unitárias do texto-original e do texto-cifrado são blocos de dois e três símbolos, respectivamente.

(a) Envie o texto-original

$$ENVIE \ \ R\$25000,00.$$

para um usuário u_j cuja chave de codificação é

$$k_{c,j} = (2047, 179).$$

(b) Fatore $n_j = 2047$, calcule r_j e decodifique o texto-cifrado.

2. Sejam $a, b \in \mathbb{Z}$ tais que

$$b \equiv a^{67} \pmod{91} \text{ e } \text{mdc}(a, 91) = 1.$$

Determinar $r \in \mathbb{N}$ tal que

$$b^r \equiv a \pmod{91}.$$

Se $b = 53$, o que é $a \pmod{91}$?

3. Suponhamos que $k_{c,1} = (2773, 17)$, $k_{c,2} = (2773, 3)$ e que uma mensagem unitária $\mathbf{u}$ é codificada como $\mathbf{c}_1 = 948$ e $\mathbf{c}_2 = 1870$ por dois usuários, respectivamente. Determinar a correspondência numérica de $\mathbf{u}$ sem a fatoração de 2773.

4. Sabendo que $n = 3552377$ é um produto de dois números primos distintos e que $\phi(n) = 3548580$. Determinar a fatoração de n.

5. Suponhamos que conhecemos os números n, $\phi(n)$ e que n é um produto de dois números primos distintos. Determinar esses fatores em função n e $\phi(n)$.

6. Sejam $n \in \mathbb{N}$ livre de quadrados e $r, t \in \mathbb{N}$ tais que $rt - 1$ é divisível por $p - 1$ para todo número primo p que divide n. Mostrar que

$$a^{rs} \equiv a \pmod{n}, \forall a \in \mathbb{Z},$$

que a tenha ou não fator em comum com n. (Sugestão: Basta mostrar que

$$a^{rs} \equiv a \pmod{p}, \forall a \in \mathbb{Z}.)$$

7. Sejam $k, n \in \mathbb{N}$, com k fixado. Mostrar que a equação $\phi(n) = k$ tem somente um número finito de soluções inteiras. (Sugestão: Se $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ é a decomposição em fatores primos distintos, então

$$n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = k \Leftrightarrow n = \frac{k}{\prod_{i=1}^{r}(p_i - 1)} \prod_{i=1}^{r} p_i.$$

Assim, os inteiros $d_i = p_i - 1, i = 1, \ldots, r$, podem ser determinados pelas seguintes condições:

(a) $d_i \mid k$;

(b) $d_i + 1$ é um número primo;

(c) $\frac{k}{\prod_{i=1}^{r} d_i}$ não contém fatores primos diferentes de $\prod_{i=1}^{r} p_i$.)

Apêndice A

Decimais

Inicialmente formalizaremos o conceito de decimais. Quando lidamos com números do tipo

$$0,47$$

trata-se de

$$\frac{47}{100} \text{ ou } \frac{4}{10}+\frac{7}{100}$$

que é um número racional.

Entretanto, quando encontramos expressões da forma

$$0,33\cdots$$

logo dizemos que é igual a

$$\frac{1}{3}$$

e, portanto um número racional. Mas

$$0,33\cdots$$

é, na verdade

$$\frac{3}{10}+\frac{3}{100}+\cdots,$$

que é uma série (soma infinita) de números racionais que, em geral, não é um número racional, como é o caso de

$$0,1010010001\cdots$$

Note que

$$0,1010010001\cdots = 0,x_1x_2x_3x_4\cdots$$

onde

$$x_n = \begin{cases} 1 & \text{se } n \text{ é um número da forma } \frac{k(k+1)}{2}, \\ 0 & \text{caso contrário.} \end{cases}$$

A expressão

$$\mathbf{a} = a_0a_1\cdots a_{n-1}a_n, b_1b_2\cdots$$

com $0 \leq a_i, b_j < 10$, é chamada de *decimal*, isto é, uma função

$$f : \mathbb{N} \cup \{0\} \to \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

e significará

$$\mathbf{a} = a_0 10^n + a_1 10^{n-1} + \cdots + a_{n-1} 10 + a_n + \sum_{j=1}^{\infty} \frac{b_j}{10^j}.$$

A decimal

$$\mathbf{a} = a_0 a_1 \cdots a_{n-1} a_n, b_1 b_2 \cdots$$

será uma *dízima periódica* se existirem $p, q \in \mathbb{N}$ tais que

$$b_j = b_{j+q}, \forall j \geq p.$$

Quando temos uma dízima periódica podemos escolher p e q mínimos e a dízima será dita *simples* se $p = 1$ ou *composta* se $p > 1$. O número $p - 1$ será dito o *comprimento da parte não periódica* ou o *comprimento do período*. Em ambos os casos usaremos a notação

$$\mathbf{a} = a_0 a_1 \cdots a_{n-1} a_n, b_1 b_2 \cdots b_{p-1} \overline{b_p \cdots b_{p+q-1}}.$$

Seja

$$\mathbf{a} = a_0 a_1 \cdots a_{n-1} a_n, b_1 b_2 \cdots b_r \overline{c_1 \cdots c_s},$$

uma dízima periódica. Então

$$\mathbf{a} = a_0 a_1 \cdots a_{n-1} a_n + \frac{b_1 b_2 \cdots b_r}{10^r} + \frac{0, \overline{c_1 \cdots c_s}}{10^r}.$$

Mas

$$0, \overline{c_1 \cdots c_s} = \frac{1}{10^s} c_1 \cdots c_s, \overline{c_1 \cdots c_s};$$

isto é,

$$(10^s - 1) 0, \overline{c_1 \cdots c_s} = c_1 \cdots c_s,$$

logo,

$$0, \overline{c_1 \cdots c_s} = \frac{c_1 \cdots c_s}{10^s - 1}$$

e, assim,

$$\mathbf{a} = \frac{(10^s - 1)(a_0 a_1 \cdots a_{n-1} a_n 10^r + b_1 b_2 \cdots b_r) + c_1 \cdots c_s}{10^r (10^s - 1)}$$

Consequentemente, podemos dizer que toda dízima periódica é igual a um número racional. Antes de provarmos a recíproca, veremos o seguinte:

Pelo Teorema 5.1 temos que, dados $a, b \in \mathbb{Z}$ com $b > 0$ existem únicos $q, r \in \mathbb{Z}$ tais que

$$a = qb + r, \text{ onde } 0 \leq r < b.$$

Assim,

$$\frac{a}{b} = q + \frac{r}{b}, \text{ e } 10r = q_1 b + r_1 \text{ onde } 0 \leq r_1 < b.$$

Como $r < b$ temos que

$$q_1 b + r_1 = 10r < 10b,$$

donde $q_1 < 10$.

Se $r_1 = 0$, então

$$\frac{r}{b} = \frac{q_1}{10} \text{ e } \frac{a}{b} = q, q_1.$$

Se $r_1 \neq 0$, então

$$10r_1 = q_2 b + r_2 \text{ onde } 0 \leq r_2 < b.$$

Se $r_2 = 0$, então

$$\frac{a}{b} = q, q_1 q_2$$

e, prosseguindo assim, obtemos

$$\frac{a}{b} = q, q_1 q_2 \cdots \text{ onde } q = a_0 a_1 \cdots a_{n-1} a_n.$$

Teorema A.1 *Todo número racional é igual a uma dízima periódica.*

Prova. Como vimos acima, o processo para se obter a representação decimal de um número racional consiste no seguinte:

$$\begin{aligned} a &= q_0 b + r_0, \quad 0 \leq r_0 < b; \\ 10r_0 &= q_1 b + r_1, \quad 0 \leq r_1 < b \quad \text{e } 0 \leq q_1 < 10; \\ 10r_1 &= q_2 b + r_2, \quad 0 \leq r_2 < b \quad \text{e } 0 \leq q_2 < 10, \end{aligned}$$

e assim por diante. Como

$$\{r_i : i \in \mathbb{N} \cup \{0\}\} \subseteq \{0, 1, \ldots, (b-1)\}$$

temos que $r_i = r_j$ para algum par i, j. Sejam

$$p = \min\{i \in \mathbb{N} \cup \{0\} : r_i = r_j \text{ para algum } j > i\}$$

e

$$s = \min\{j : r_p = r_j \text{ com } j > p\}.$$

Então

$$\frac{a}{b} = a_0 a_1 \cdots a_{n-1} a_n, q_1 q_2 \cdots q_{p-1} \overline{q_p \cdots q_{s-1}}.$$

Tendo em vista a unicidade de p, s, q_i e r_i, a representação decimal de todo número racional é única. ■

Exemplo A.2 *Calcular a representação decimal do número racional* $\frac{11}{6}$.

Solução. De

$$\begin{aligned} 11 &= 1 \cdot 6 + 5, \quad q_0 = 1 \text{ e } r_0 = 5; \\ 10 \cdot 5 &= 8 \cdot 6 + 2, \quad q_1 = 8 \text{ e } r_1 = 2; \\ 10 \cdot 2 &= 3 \cdot 6 + 2, \quad q_2 = 3 \text{ e } r_2 = r_1 = 2, \end{aligned}$$

obtemos que

$$\frac{11}{6} = 1,8\overline{3}$$

Observação A.3 *Pela prova do teorema acima, os restos encontrados no processo da representação decimal do número racional $\frac{a}{b}$, com $a < b$ e $mdc(a, b) = 1$, são*

$$a, 10 \cdot a, 10^2 \cdot a, \ldots, 10^p \cdot a \,(\mathrm{mod}\, b).$$

Em particular, se $b = 2^r 5^s$ e $p = \max\{r, s\}$, então $10^p \equiv 0 \,(\mathrm{mod}\, b)$ e, neste caso, temos que a representação decimal do número racional $\frac{a}{b}$ é exata, isto é, tem zeros a partir da p-ésima posição. Agora, se $mdc(10, b) = 1$, então $10 \in \mathbb{Z}_b^\bullet$, assim, seja p o menor inteiro positivo tal que $10^p \equiv 1 \,(\mathrm{mod}\, b)$. Então a representação decimal do número racional $\frac{a}{b}$ é periódica de período p.

Exemplo A.4 *Mostrar que o número de dígitos no período da representação decimal do número racional $\frac{10.000}{7.699}$ é 7.698.*

Solução. Como $\frac{10.000}{7.699} = 1 + \frac{2.301}{7.699}$ basta considerar o número racional $\frac{2.301}{7.699}$. É fácil verificar que 7.699 é um número primo e $\mathrm{mdc}(10, 7.699) = 1$. Assim, pelo Teorema de Fermat,

$$10^{7.698} \equiv 1 \,(\mathrm{mod}\, 7.699).$$

Portanto, pela observação acima, o número de dígitos no período da representação decimal do número racional $\frac{10.000}{7.699}$ é 7.698.

Teorema A.5 *Sejam $x \in [0, 1[$ e $b \in \mathbb{N}$. Então para cada $n \in \mathbb{Z}_+$ existe uma única expressão*

$$x = \frac{a_0}{b} + \frac{a_1}{b^2} + \cdots + \frac{a_{n-1}}{b^n} + \frac{a_n}{b^{n+1}} + d_n,$$

onde $0 \leq a_i < b$ e $0 \leq d_n < \frac{1}{b^{n+1}}$.

Prova. Seja $a = \lfloor b^{n+1} x \rfloor$. Então

$$a \in \mathbb{Z}_+ \text{ e } b^{n+1} x = a + c_n$$

para algum c_n tal que $0 \leq c_n < 1$. Assim, pelo Teorema 5.9, existem únicos $a_i \in \mathbb{Z}$ tais que

$$a = a_0 b^n + a_1 b^{n-1} + \cdots + a_{n-1} b + a_n,$$

onde $a_i \in \{0, 1, \ldots, b-1\}$, $\forall i = 0, 1, \ldots, n$. Portanto,

$$x = \frac{a_0}{b} + \frac{a_1}{b^2} + \cdots + \frac{a_{n-1}}{b^n} + \frac{a_n}{b^{n+1}} + d_n,$$

onde $0 \leq a_i < b$ e $0 \leq d_n = \frac{c_n}{b^{n+1}} < \frac{1}{b^{n+1}}$. ■

A recíproca do Teorema acima vale, mas a sua prova está fora dos objetivos deste trabalho.

EXERCÍCIOS

1. Determinar se a representação decimal dos números racionais abaixo é exata ou periódica:

   (a) $\frac{7}{30}$;

   (b) $\frac{11}{50}$;

   (c) $\frac{4}{45}$;

   (d) $\frac{13}{40}$;

   (e) $\frac{7}{13}$;

   (f) $\frac{17}{5}$.

2. Calcular a representação decimal do número racional $\frac{2}{7}$.

3. Calcular a representação decimal do número racional $\frac{1}{17}$.

4. Determinar o número racional da dízima periódica $8,\overline{17}$.

5. Determinar o número racional da dízima periódica $2,3\overline{18}$.

6. Mostrar que o número $0,1010010001\ldots$ não é racional.

7. Mostrar que o número $\sqrt{2}+\sqrt{3}$ não é racional.

8. Determinar o número de dígitos no período da representação decimal do número racional $\frac{1.955}{1.997}$.

9. Seja $\frac{a}{b}$ número racional com $a < b$ e $\text{mdc}(a,b) = 1$. Se $b = 2^r 5^s d$ com $\text{mdc}(10,d) = 1$, então a representação decimal de $\frac{a}{b}$ é da forma

$$0, q_1 q_2 \cdots q_p \overline{q_1 \cdots q_k},$$

onde $p = \max\{r,s\}$ e $10^k \equiv 1 \pmod{d}$. (Sugestão: Note que $10^p = 2 \cdot 5c$ e

$$\frac{10^p}{b} = \frac{c}{d}$$

com $\text{mdc}(c,d) = 1$, assim, a partir da p-ésima posição, começam os dígitos da expanção decimal de $\frac{c}{d}$.)

Bibliografia

[1] **AYRES**, F. Jr. - *Álgebra Moderna*, Coleção Schaum, McGraw-Hill, 1965.

[2] **BIRKHOFF**, G. e **MAC LANE**, S. - *Álgebra Moderna Básica*, Guanabara Dois, 1980.

[3] **BURTON**, D. M. - *Elementary Number Theory*, Allyn and Bacon, Inc., 1976.

[4] **GENTILE**, E. R. - *Aritmetica Elemental*, Monografia de Matemática, O.E.A., 1985.

[5] **GONÇALVES**, A. - *Introdução à Álgebra*, Projeto Euclides, IMPA, 1979.

[6] **HALMOS**, P. R. - *Naive Set Theory*, Princeton, N.J., Van Nostrand, 1960.

[7] **HEFEZ**, A. - *Curso de Álgebra*, Vol. I, Coleção Matemática Universitária, IMPA, 1993.

[8] **IZAR**, S. A. e **TADINI**, W. M. - *Teoria dos Conjuntos*, Notas de Matemática N.^{o} 2, IBILCE, 1994.

[9] **MONTEIRO**, L. H. - *Elementos de Álgebra*, Elementos de Matemática, IMPA, 1969.

[10] **KOBLITZ**, N. - *A Course in Number Theory and Cryptography*, 2nd ed., Springer-Verlag, 1994.

[11] **KONHEIN**, A. G. - *Cryptography, a primer*, Wiley (New York), 1981.

[12] **LEMOS**, M. - *Criptografia, Números Primos e Algoritmos*, 17.^{0} Colóquio Brasileiro de Matemática, IMPA, 1989.

[13] **LIMA**, E. L. - *Curso de Análise*, Vol. I, Projeto Euclides, IMPA, 1976.

[14] **LANG**, S. - *Estruturas Algébricas*, LTC, 1972.

[15] **LIPSCHUTZ**, S. - *Teoria dos Conjuntos*, Coleção Schaum, McGraw-Hill, 1978.

[16] **NIVEN**, I., **ZUKERMAN**, H. S. and **MONTGOMERY**, H. L. - *An Introduction to the Theory of Numbers*, Wiley (New York), 1991.

[17] **PINTER**, C. C. - *Set Theory*, Addison-Wesley, 1971.

[18] **SHOKRANIAN**, S., **SOARES**, M. e **GODINHO**, H. - *Teoria dos Números*, Editora Universidade de Brasília, 1994.

[19] **SIDKI**, S. - *Introdução à Teoria dos Números*, $10.^0$ Colóquio Brasileiro de Matemática, IMPA, 1975.

[20] **SIERPINSKI**, W. - *A Selection of Problems in the Theory of Numbers*, Pergamon Press, 1964.

[21] **SIERPINSKI**, W. - 250 *Problems in Elementary Number Theory*, American Elsevier Publishing Company, 1970.

[22] *Revistas do Professor de Matemática* - SBM.

[23] *The USSR Olympiad Problem Book*, W.H. Freeman and Company, 1962.