Números, Relações e Criptografia

Textuniversitários 32

Antônio de Andrade e Silva

Números, Relações *e Criptografia*

LF Editorial
São Paulo — 2025

1a. Edição

Editor: Victor Pereira Marinho / José Roberto Marinho
Projeto gráfico e diagramação: Thiago Augusto Silva Dourado
Capa: Fabrício Ribeiro

Texto em conformidade com as novas regras ortográficas do Acordo da Língua Portuguesa.

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Silva, Antonio de Andrade e
Números, relações e criptografia / Antonio de Andrade e Silva. –– São Paulo : LF Editorial, 2025. –– (Textuniversitários ; 32)

Bibliografia.
ISBN 978-65-5563-652-9

1. Aritmética 2. Criptografia 3. Matemática 4. Teoria dos números I. Título. II. Série.

25-304427.0 CDD–510

Índices para catálogo sistemático:

1. Matemática 510

Eliete Marques da Silva – Bibliotecária – CRB-8/9380

Impresso no Brasil
Printed in Brazil

www.lfeditorial.com.br
Visite nossa livraria no Instituto de Física da USP
www.livrariadafisica.com.br
Telefones:
(11) 2648-6666 | Loja do Instituto de Física da USP
(11) 3936-3413 | Editora

À minha esposa,
Rosângela

Prefácio

"Quando jovem, aprendemos. Quando velho, compreendemos."

Albert Einstein

A ideia de escrever este texto 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. 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 abordagem 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 experiência 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.

Nos primeiros três capítulos, admitiremos que o leitor tenha familiaridade com as propriedades padrão dos conjuntos numéricos:

números naturais, os inteiros, os números racionais e os números reais, para exemplos concretos.

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 a construção axiomática dos sistemas de números, que não é apenas de interesse inerente, e fundamental para uma compreensão completa dos sistemas numéricos, mas torna uso extensivo do material dos capítulos anteriores, fornece uma adequada grande final para o nosso tratamento dos fundamentos da matemática moderna.

No capítulo 5, apresentaremos algumas definições e resultados básicos da Teoria dos Números.

No capítulo 6, é dedicado ao estudo da Aritmética Modular. No capítulo 7, aplicaremos os conhecimentos sobre números primos e congruências para apresentar uma introdução aos sistemas de criptografia clássicos e com chave pública.

Finalmente, no capítulo 8 apresentaremos a construção clássica do sistema de números reais via sequências fundamentais de Cantor.

Agradecemos aos colegas e alunos do Departamento de Matemática que direta ou indiretamente contribuíram para a realização deste texto. Especialmente, ao Professor Thiago Dourado pelo trabalho de editoração e por todo incentivo que nos dedicou. Finalmente, nossa gratidão à LF Editorial pela confiança em nosso trabalho.

Antônio de Andrade e Silva
Campina Grande, julho de 2025

Sumário

Prefácio **VII**

Parte I
Conjuntos e Relações

1 Conjuntos **1**
1.1 Sentenças 1
Exercícios 9
1.2 Conjuntos 11
Exercícios 19

2 Relações e Funções **25**
2.1 Relações 25
Exercícios 33
2.2 Funções 37
Exercícios 48

3 Relação de Ordem e Enumerabilidade **57**
3.1 Conjuntos Ordenados 57
Exercícios 67
3.2 Conjuntos Finitos e Infinitos 73
Exercícios 83

4 A Origem das frações **89**
4.1 Números Naturais 89
Exercícios 97
4.2 Números Inteiros 98
Exercícios 106
4.3 Números Racionais 106
Exercícios 113

Parte II
Números e Criptografia

5 Teoria dos Números **117**
5.1 Algoritmo da Divisão 117
Exercícios 127
5.2 Máximo Divisor Comum 129
Exercícios 139
5.3 Teorema Fundamental da Aritmética 144
Exercícios 154

6 Aritmética Modular **159**
6.1 Congruências 159
Exercícios 169
6.2 Congruências Lineares 172
Exercícios 180
6.3 Algumas Congruências Especiais 183
Exercícios 195

7 Introdução à Criptografia **199**
7.1 Criptossistemas 199
Exercícios 210
7.2 Criptossistema com Chave Pública 211
Exercícios 221
7.3 Criptossistema RSA 222
Exercícios 226

8 Números Reais **229**
8.1 Introdução 229
8.2 Sequências Convergentes 230
Exercícios 233
8.3 Construção dos Números Reais 234
Exercícios 246
8.4 Expansão Decimal 247
Exercícios 259

A Respostas e Sugestões **261**

Notações **354**

Índice Remissivo **360**

Parte I

Conjuntos e Relações

1

Conjuntos

Neste capítulo apresentaremos algumas definições e resultados clássicos de lógica simbólica informal e da teoria dos conjuntos que serão necessários para cursos subsequentes. O leitor interessado em mais detalhes pode consultar as referências no final do texto.

1.1 Sentenças

> *"A lógica é a higiene que o matemático pratica para manter suas ideias saudáveis e fortes."*
>
> Hermann Weyl

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.

Uma *sentença* (ou *proposição* ou *afirmação*) significa uma oração declarativa à qual, num dado contexto, é, sem equívoco, *verdade* 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 verdade ou falsidade de uma sentença chama-se *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. Frequentemente, 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 $\neg p$ (leia-se não p). O valor-verdade da negação de uma sentença satisfaz: se p for verdadeira, então $\neg p$ será falsa; se p for falsa, então $\neg p$ será verdade. Por exemplo, seja p a sentença "este é um curso fácil." Então sua negação $\neg p$ representa a sentença "este não é um curso fácil." É conveniente exibir a relação entre $\neg p$ e p em uma tabela que chama-se *tabela verdade*, em que V e F denotam os valores verdade e falso, respectivamente. A definição precisa de $\neg p$ é dada pela Tabela (1.1.1).

p	$\neg p$
V	F
F	V

(1.1.1)

A *lei da contradição* afirma que dadas duas sentenças contraditórias, isto é, tais que uma é a negação da outra, uma delas é falsa. O *princípio do terceiro excluído* afirma que dadas duas sentenças contraditórias, uma delas é verdadeira.

Se p e q são sentenças, a *conjunção* de p e q, em símbolos $p \wedge q$ (leia-se p e q) é uma sentença que, intuitivamente, é verdadeira se p e q forem ambas verdadeiras. Caso contrário, são falsas. A definição precisa de $p \wedge q$ é dada pela Tabela (1.1.2).

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

(1.1.2)

É muito importante observar que essa tabela verdade, e todas as outras semelhantes, prova se a nova sentença é verdadeira ou falsa, para cada combinação possível da verdade ou falsidade de cada um de p e q.

Se p e q são sentenças, a *disjunção* de p e q, em símbolos $p \vee q$ (leia-se p ou q com sentido de e/ou) é uma sentença que, intuitivamente, é verdadeira se p for verdadeiro ou q for verdadeiro ou ambos forem verdadeiros, isto é, pelo menos um de p ou q for verdadeiro. Caso contrário, é falso, ou seja, se p e q forem ambas falsas. A definição precisa de $p \vee q$ é dada pela Tabela (1.1.3).

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

(1.1.3)

Uma operação importante em sentenças, principalmente em matemática, é a *implicação*: se p e q são sentenças, então $p \to q$ (leia-se p implica q). Note que: em uso comum, se p for verdadeiro, então q for verdadeiro significa que existe uma *relação de causa* entre p e q, como em "se Bob passa no curso, então Bob pode colar grau." Em matemática, portanto, implicação é *no sentido formal*: $p \to q$ é, intuitivamente, verdadeira se nunca for o caso em que p é verdadeiro e q é falso. A definição precisa de $p \to q$ é dada pela Tabela (1.1.4). Neste caso, diremos que "p é condição suficiente para q" e "q é condição necessária para p." Além disso, p chama-se *hipótese* e q chama-se *tese* ou *conclusão*.

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

(1.1.4)

As duas primeiras linhas da Tabela são intuitivamente claras, pois se p for verdadeiro e q for verdadeiro, então é claro $p \to q$ deve ser verdadeiro; se p for verdade e q for falso, então $p \to q$ deve ser falso. A terceira e quarta linhas da Tabela, que dizem que a sentença $p \to q$ é verdadeira sempre que p for falso, independentemente do

valor de q, são menos intuitivas. Para um exemplo concreto, sejam p a sentença "dois ângulos opostos pelo vértice" e q a sentença "dois ângulos congruentes." Então comprove intuitivamente a tabela da sentença $p \to q$: sendo verdadeira se podemos desenhar o diagrama dos ângulos. Caso contrário, é falsa.

Teorema 1.1.1 *Sejam p e q sentenças. Então as seguintes sentenças são verdadeiras:*

1. $p \to p \vee q; q \to p \vee q$ *(adição).*

2. $p \wedge q \to p; p \wedge q \to q$ *(simplificação).*

Prova. Provaremos apenas uma das sentenças do 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

(1.1.5)

Como a última coluna da tabela verdade é constituída de valores "verdades" temos que a sentença $p \to p \vee q$ é verdadeira. □

Teorema 1.1.2 *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

(1.1.6)

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

Teorema 1.1.3 *Sejam p, q e r três sentenças. Se $q \to r$ for uma sentença verdadeira, então as seguintes sentenças são verdadeiras:*

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

PROVA. Vamos derivar apenas a tabela para a sentença $(p \vee q) \to (p \vee r)$.

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

(1.1.7)

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

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

Exemplo 1.1.4 Sejam p e q sentenças. Mostre que as sentenças $p \to q$ e $\neg p \vee q$ são equivalentes, isto é, $(p \to q) \leftrightarrow (\neg p \vee q)$ ou $(p \to q) = (\neg p \vee q)$.

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

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

(1.1.8)

Como a quarta e quinta coluna da tabela verdade são constituídas dos mesmos valores, temos que $(p \to q) = (\neg\, p \vee q)$ é uma sentença verdadeira. □

Dadas sentenças p e q, existem quatro sentenças, as quais resultam do uso de $\to$ para conectá-las, a saber: $p \to q$ condicional e $q \to p$ recíproca; $\neg\, q \to \neg\, p$ contrapositiva e $\neg\, p \to \neg\, q$ inversa. Note que a condicional e a contrapositiva são sentenças logicamente equivalentes. De fato, basta derivar a tabela para a sentença $(p \to q) = (\neg\, q \to \neg\, p)$.

p	q	$\neg\, q$	$\neg\, p$	$p \to q$	$\neg\, q \to \neg\, p$
V	V	F	F	V	V
V	F	V	F	F	F
F	V	F	V	V	V
F	F	V	V	V	V

(1.1.9)

Como a quina e sexta coluna da tabela verdade são constituídas dos mesmos valores, temos que $(p \to q) = (\neg\, q \to \neg\, p)$ é uma sentença verdadeira. Por exemplo,"todos os humanos são mamíferos" pode ser reescrita em sua forma condicional "Se algo for humano, então