

ARITMÉTICA

Aritmética

Copyright ©2022 Abramo Hefez

Direitos reservados pela Sociedade Brasileira de Matemática.

A reprodução não autorizada desta publicação, no todo ou em parte, constitui violação de direitos autorais. (Lei 9.610/98). Impresso Abr. 2022

Sociedade Brasileira de Matemática

Presidente: Paolo Piccione

Vice-Presidente: Jaqueline Godoy Mesquita

Diretores: Walcy Santos

Jorge Herbert Soares de Lira

Daniel Gonçalves

Roberto Imbuzeiro

Editor Executivo

Hilário Alencar

Assessor Editorial

Tiago Costa Rocha

Coleção PROFMAT

Comitê Editorial da Coleção PROFMAT

Hilário Alencar (Editor-Chefe)

Marcela Souza (Editora-Adjunta)

Mariana Cassol

Paulo Leandro Dattori

Vanderlei Horita

Projeto gráfico e capa

Pablo Diego Regino

Editoração Eletrônica

Yunelsy Nápoles Alvarez

Distribuição e vendas

Sociedade Brasileira de Matemática

Estrada Dona Castorina, 110 Sala 109 - Jardim Botânico

22460-320 Rio de Janeiro RJ

Telefones: (21) 2529-5073

<http://www.sbm.org.br> / [email:lojavirtual@sbm.org.br](mailto:lojavirtual@sbm.org.br)

ISBN 978-85-8337-181-6

Hefez, Abramo

Aritmética / Abramo Hefez. – 3. ed. – Rio de Janeiro, RJ :
Sociedade Brasileira de Matemática, 2022.

306 p. (Coleção Profmat; COP 08)

ISBN 978-85-8337-181-6

1. Números Inteiros. 2. Aplicações da indução. 3. Divisão
nos inteiros. 4. Números primos. I. Hefez, Abramo. II.
Aritmética.

Abramo Hefez

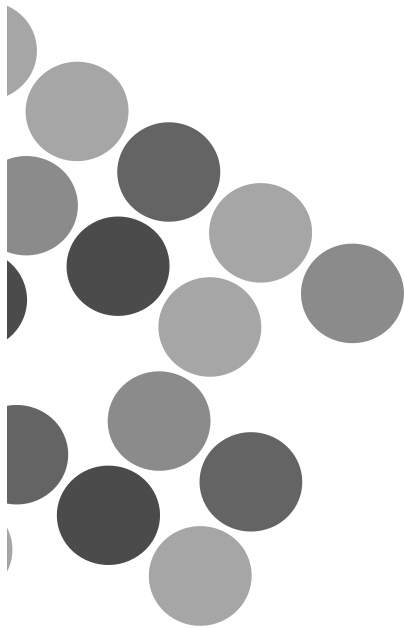
ARITMÉTICA

3ª edição
2022
Rio de Janeiro



*Este livro é dedicado aos professores de
matemática que, buscando o seu contínuo
aprimoramento, com notável esforço e sacrifício,
nos permitem sonhar com um futuro melhor.*

Sumário



Sumário

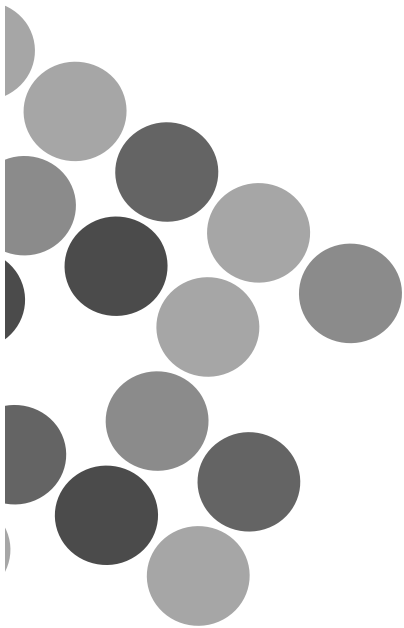
Prefácio	xi
1 Os Números Inteiros	1
1.1 Introdução	2
1.2 A Adição e a Multiplicação	3
Exercícios	5
1.3 Ordenação dos Inteiros	6
Exercícios	9
1.4 Princípio da Boa Ordenação	10
Exercícios	17
2 Aplicações da Indução	19
2.1 Definição por Recorrência	20
Exercícios	22
2.2 Binômio de Newton	23
Exercícios	26
2.3 Aplicações Lúdicas	28
Exercícios	35
3 Divisão nos Inteiros	37
3.1 Divisibilidade	38
Exercícios	42
3.2 Divisão Euclidiana	44
Exercícios	48
3.3 A Aritmética na Magna Grécia	51
4 Representação dos Números Inteiros	55
4.1 Sistemas de Numeração	56
Exercícios	64
4.2 Jogo de Nim	65
Exercícios	69
5 Algoritmo de Euclides	71
5.1 Máximo Divisor Comum	72
Exercícios	77
5.2 Propriedades do mdc	78
Exercícios	82
5.3 Algoritmo de Euclides Estendido	83
Exercícios	86
5.4 Mínimo Múltiplo Comum	86

Exercícios	89
5.5 A Equação Pitagórica	90
Exercícios	93
6 Aplicações do Máximo Divisor Comum	97
6.1 Equações Diofantinas Lineares	98
Exercícios	105
6.2 Expressões Binômias	106
Exercícios	113
6.3 Números de Fibonacci	113
Exercícios	115
7 Números Primos	117
7.1 Teorema Fundamental da Aritmética	118
Exercícios	126
7.2 Sobre a Distribuição dos Números Primos	127
Exercícios	130
7.3 Pequeno Teorema de Fermat	131
Exercícios	134
7.4 O Renascimento da Aritmética	135
8 Números Especiais	137
8.1 Primos de Fermat, de Mersenne e em PA	138
Exercícios	142
8.2 Números Perfeitos	142
Exercícios	145
8.3 Decomposição do Fatorial em Primos	146
Exercícios	152
8.4 A equação $E_p(x!) = \alpha$	153
Exercícios	157
8.5 Euler, um Gigante da Matemática	158
9 Congruências	159
9.1 Aritmética dos Restos	160
Exercícios	168
9.2 Aplicações	169
Exercícios	174
9.3 Congruências e Números Binomiais	175
Exercícios	179
9.4 O Calendário	179

Sumário

Exercícios	184
9.5 Gauss, um Príncipe da Matemática	185
10 Os Teoremas de Euler e Wilson	189
10.1 Teorema de Euler	190
Exercícios	201
10.2 Teorema de Wilson	202
Exercícios	204
11 Congruências Lineares e Classes Residuais	207
11.1 Resolução de Congruências Lineares	208
Exercícios	212
11.2 Teorema Chinês dos Restos	213
Exercícios	221
11.3 Classes Residuais	222
Exercícios	230
12 Congruências Quadráticas	233
12.1 Congruências Quadráticas	234
Exercícios	240
12.2 Resíduos Quadráticos	241
Exercícios	246
12.3 Somas de Quadrados	246
Exercícios	252
12.4 Lei da Reciprocidade Quadrática	252
Exercícios	260
13 Noções de Criptografia	263
13.1 As Origens da Criptografia	264
13.2 O Advento dos Computadores	269
13.3 A Grande Revolução: O Sistema RSA	272
Bibliografia	277
Índice Remissivo	280

Prefácio



Este livro, do qual ora apresentamos a segunda edição, nasceu de notas de aula de um curso de especialização para professores de ensino fundamental e médio, organizado pela SBM, que ministrei em 2003 e foi posteriormente transformado no livro *Elementos de Aritmética*, publicado na Coleção Textos Universitários, da SBM. Este material foi utilizado a partir de 2011 na disciplina Aritmética, do Curso de Mestrado Profissional em Matemática em Rede Nacional - Profmat - por dois anos seguidos, tendo sido submetido ao longo desse processo a uma profunda revisão e ampliação, resultando na primeira edição deste livro.

O nosso objetivo aqui é estudar as propriedades dos números inteiros junto com as suas operações de adição e de multiplicação, enfatizando as questões relacionadas com a divisibilidade.

O livro cobre o material para um primeiro curso de Aritmética e destina-se à formação complementar daqueles que estão no exercício da docência no ensino fundamental e médio, bem como à formação básica dos alunos de graduação em Matemática.

Apesar deste material não ser ensinado neste grau de detalhe e de profundidade nas escolas, ele deve, obrigatoriamente, fazer parte da bagagem mínima de todo professor de Matemática.

A Aritmética, como usualmente é chamada a parte elementar da Teoria dos Números, teve como principal marco inicial a obra *Os Elementos*, de Euclides (aprox. 300 a.C.), encontrando o seu auge nos trabalhos de Pierre de Fermat (1601-1665) e Leonhard Euler (1707-1783), o que a levou a tornar-se um dos principais pilares da Matemática. A partir do início do século XIX, graças à obra de Carl Friedrich Gauss (1777-1855), a Aritmética transforma-se em Teoria dos Números e começa a ter um desenvolvimento extraordinário. São esses os quatro principais protagonistas da história que iremos contar aqui.

A Gauss deve-se a fecunda ideia, entre muitas outras, de efetuar a fatoração de números naturais em anéis de números algébricos. Essa ideia foi grandemente desenvolvida nos trabalhos de Ernst Kummer, Richard Dedekind e Leopold Kronecker, iniciando o que se chama atualmente a Teoria Algébrica dos Números. Por outro lado, com os trabalhos de Lejeune Dirichlet e Bernhard Riemann, também no século XIX, foram utilizadas técnicas de Análise Real e Complexa para se compreender melhor a distribuição dos números primos, iniciando, assim, uma outra maneira de se tratar os problemas da Aritmética, a Teoria Analítica dos Números. Hoje, há pelo menos uma terceira abordagem, a Geometria Aritmética, cujos métodos são tomados da Geometria Algébrica e cujos precursores foram Emil Artin, Helmut Hasse, Louis Joel Mordell e André Weil. Essa última abordagem tem-se mostrado extremamente fecunda, permitindo provar profundos teoremas em Teoria dos Números, e culminando com a publicação, em 1995, da demonstração, por Andrew Wiles, do chamado Último Teorema de Fermat.

Prefácio

O livro é organizado como segue: são 13 capítulos, divididos em seções. Cada seção contém inúmeros exemplos e, ao seu final, uma lista de problemas, numerados com dois números; o primeiro indicando o capítulo ao qual o problema pertence e o segundo, o número do problema em si. Além disso, no final de alguns dos capítulos, o leitor encontrará uma lista de problemas suplementares.

Para tornar possível a utilização do livro em um curso semestral, algumas partes, apesar de importantes, poderão ser omitidas, a critério do professor, sem comprometer a compreensão do todo. Essas partes são as Seções 4.2, 5.5, 6.2, 6.3, 8.3, 8.4, 9.3, 9.4 e o Capítulo 13.

Gostaria de reiterar o meu agradecimento à colega Maria Lúcia Torres Villela pelo minucioso trabalho de revisão da primeira edição, responsabilizando-me, para todos os efeitos, por eventuais erros ou imprecisões.

Nessa edição foram feitas apenas algumas pequenas correções, sendo a grande novidade o simultâneo lançamento nessa mesma coleção de um livro companheiro deste, contendo as soluções de todos os problemas nele propostos, acrescidos de listas de novos problemas.

Niterói, agosto de 2016.

Abramo Hefez

Prefácio à terceira edição

Essa edição só se diferencia da anterior pela nova diagramação e pela correção de alguns poucos erros tipográficos.

Niterói, novembro de 2021.

Abramo Hefez