ÍNDICE

PREFÁCIO **ix**

1 O PRINCÍPIO DE INDUÇÃO **1**

1.1 Princípio de indução 3
1.1.1 Desafio ao leitor 17
1.2 Binómio de Newton 23
1.2.1 Desafio ao leitor 27
1.3 Bibliografia do capítulo 28

2 TEORIA DOS NÚMEROS E CRIPTOGRAFIA **29**

2.1 Máximo divisor comum 31
2.1.1 Desafio ao leitor 47
2.2 Equações diofantinas lineares 58
2.2.1 Desafio ao leitor 63
2.3 Congruências 67
2.3.1 Calendários 67
2.3.2 Congruências do calendário 72
2.3.3 Resolução de congruências 79
2.3.4 Inversos 85
2.3.5 Teorema de Fermat 86
2.3.6 Os conjuntos $\mathbb{Z}_{\mathbf{n}}$ 89
2.3.7 Desafio ao leitor 91
2.4 Critérios de divisibilidade 92
2.4.1 Divisão por 2 e por 5 94
2.4.2 Divisão por 3 e por 9 95
2.4.3 Divisão por 4 95
2.4.4 Divisão por 7 95

2.4.5 Divisão por 11 96
2.4.6 Divisão por 13 97
2.4.7 Desafio ao leitor 98
2.5 Sistemas de congruências 109
2.5.1 Teorema Chinês dos Restos 109
2.5.2 Desafio ao leitor 126
2.6 Primos 131
2.6.1 Primos: estudo elementar 131
2.6.2 Desafio ao leitor 136
2.6.3 Primos: estudo avançado 141
2.7 Criptografia 146
2.7.1 O método da autochave de Vigenère 146
2.7.2 Desafio ao leitor 152
2.7.3 Criptografia de chave simétrica (Hill) 152
2.7.4 Desafio ao leitor 158
2.7.5 Criptografia de chave pública (RSA) 159
2.7.6 Desafio ao leitor 168
2.8 Partilha de segredo com protocolo de limiar 170
2.9 Bibliografia do capítulo 173

3 ALGORITMO FFT 177

3.1 Conceitos elementares 179
3.1.1 Método de Horner 184
3.1.2 Desafio ao leitor 187
3.1.3 Algoritmo de Sturm 189
3.1.4 Desafio ao leitor 192
3.2 Multiplicação de polinómios 192
3.2.1 Método tradicional 192
3.2.2 Método de dividir para conquistar 193
3.2.3 Desafio ao leitor 196
3.3 Introdução à transformada discreta de Fourier 197
3.3.1 Nota histórica 197
3.3.2 Valoração e interpolação 200
3.3.3 Método FFT 202
3.3.4 Multiplicação de polinómios 213
3.3.5 Desafio ao leitor 224
3.4 Bibliografia do capítulo 229

4 SOMATÓRIOS **231**

4.1 Somas e produtos iterados 233
4.2 Somas parciais dos termos de uma sucessão 243
4.3 Verificação de formas fechadas 252
4.4 Sucessão harmónica 260
4.5 Método das perturbações 262
4.5.1 Desafio ao leitor 270
4.6 Bibliografia do capítulo 272

5 CÁLCULO FINITO **275**

5.1 Operadores 277
5.1.1 Desafio ao leitor 280
5.2 Polinómios fatoriais 281
5.2.1 Conceito e aplicação 281
5.2.2 Números de Stirling 289
5.2.3 Paradigma I - Do polinómio para o polinómio fatorial 294
5.2.4 Desafio ao leitor 296
5.3 Primeira aplicação ao cálculo de somatórios 296
5.3.1 Paradigma II - Somatório de funções polinomiais 300
5.4 Funções exponenciais 302
5.5 Frações racionais 304
5.5.1 Desafio ao leitor 307
5.6 Segunda aplicação ao cálculo de somatórios 308
5.7 Integração finita por partes — fórmula de Abel 312
5.8 Outros exemplos 316
5.9 Fórmula de Euler-MacLaurin 319
5.10 Casos particulares 322
5.11 Desafio ao leitor 324
5.12 Nota sobre o princípio da inclusão–exclusão 327
5.12.1 Motivação 327
5.12.2 Teoremas de exclusão e inclusão 329
5.12.3 Desarranjos 333
5.12.4 Desafio ao leitor 334
5.13 Bibliografia do capítulo 338

6 FUNÇÕES GERADORAS E APLICAÇÕES **341**

6.1 Séries formais 343

6.2 Funções geradoras 351
6.2.1 Motivação 351
6.2.2 Conceito 353
6.2.3 Desafio ao leitor 357
6.2.4 Operadores notáveis sobre funções geradoras 362
6.2.5 Desafio ao leitor 365
6.3 Aplicação a problemas de contagem 367
6.3.1 Desafio ao leitor 373
6.4 Aplicação ao cálculo de somatórios 373
6.5 Decomposição de frações racionais 377
6.5.1 O polinómio $t(z)$ tem raízes reais distintas 377
6.5.2 O polinómio $t(z)$ tem raízes reais múltiplas 378
6.5.3 O polinómio $t(z)$ tem raízes imaginárias 379
6.5.4 Desafio ao leitor 379
6.6 Paradigma 379
6.6.1 Desafio ao leitor 381
6.7 Resolução de equações às diferenças finitas 383
6.7.1 Paradigma 385
6.7.2 Torre de Hanoi e sucessão de Fibonacci 390
6.7.3 Dinâmica de populações 392
6.7.4 Leis físicas 394
6.7.5 Desafio ao leitor 396
6.8 Função geradora geral da solução 398
6.8.1 Fórmula resolvente 398
6.8.2 Paradigma 402
6.8.3 Desafio ao leitor 403
6.8.4 Reversão da função geradora 404
6.8.5 Primeiro caso 404
6.8.6 Segundo caso 405
6.8.7 Terceiro caso 406
6.9 Funções geradoras dos momentos 407
6.10 Aplicação à complexidade computacional 409
6.11 Bibliografia do capítulo 416

7 GRAFOS 417

7.1 Conceitos elementares 419
7.1.1 Desafio ao leitor 429
7.2 Grafos bipartidos e o relacionamento estável 435

7.3 Atalhos eulerianos 441
7.4 Grafos aleatoriamente eulerianos 454
7.4.1 Desafio ao leitor 460
7.5 Labirintos 465
7.6 Ciclo hamiltoniano 476
7.6.1 Desafio ao leitor 481
7.7 Árvores 483
7.7.1 Desafio ao leitor 484
7.8 Grafos planares 488
7.8.1 Desafio ao leitor 494
7.9 Conectividade 495
7.9.1 Problema da conexão mínima 495
7.9.2 Como aplicar uma lei física 498
7.9.3 Desafio ao leitor 502
7.9.4 Trajetória mínima numa rede 503
7.9.5 Desafio ao leitor 508
7.10 Transportes: redes de estradas 511
7.10.1 Desafio ao leitor 514
7.11 Fluxos em redes 514
7.11.1 Algoritmo de Ford e Fulkerson 519
7.11.2 Desafio ao leitor 523
7.12 Fluxo em redes sobre grafos planares 526
7.12.1 Paradigma 527
7.12.2 Teorema 530
7.13 Bibliografia do capítulo 531

8 AUTÓMATOS FINITOS E DE PILHA 535

8.1 Autómatos 537
8.1.1 Autómatos finitos determinísticos 537
8.1.2 Desafio ao leitor 546
8.1.3 Classe das linguagens regulares 546
8.1.4 Lema de *pumping* 548
8.1.5 Desafio ao leitor 550
8.1.6 Autómatos finitos não determinísticos 553
8.1.7 Autómato determinístico equivalente 558
8.2 Do autómato à expressão regular e vice-versa 567
8.3 Gramáticas regulares 572
8.3.1 Desafio ao leitor 582

8.4 Autómatos de pilha 582
8.4.1 Desafio ao leitor 587
8.5 Gramáticas livres de contexto 588
8.6 Funções geradoras de linguagens 600
8.6.1 Números de Catalan 600
8.6.2 Ainda sobre a linguagem de Dyck 607
8.6.3 Desafio ao leitor 608
8.7 Bibliografia do capítulo 608

9 MÁQUINAS DE TURING 609

9.1 A máquina de Turing de k fitas 611
9.1.1 A ideia de um computador abstrato 611
9.1.2 Configurações 613
9.1.3 Definição formal de máquina de Turing 614
9.1.4 Computações 616
9.1.5 Exemplos 618
9.1.6 Desafio ao leitor 627
9.2 Indecidibilidades 632
9.2.1 O problema da aceitação 634
9.2.2 O problema da paragem 635
9.3 Exemplos de conjuntos indecidíveis 638
9.3.1 $\text{HALT}_{\mathbf{TM}}$ 640
9.3.2 $\text{EMPTY}_{\mathbf{TM}}$ 640
9.3.3 $\text{EQ}_{\mathbf{TM}}$ 641
9.3.4 $\text{REGULAR}_{\mathbf{TM}}$ 641
9.3.5 $\text{DOM}^{\mathbf{a}}_{\mathbf{TM}}$ 642
9.3.6 $\text{CODOM}^{\mathbf{a}}_{\mathbf{TM}}$ 643
9.3.7 Teorema de Rice 644
9.4 Conjetura de Collatz e predicados Π_2 645
9.5 Mais sobre o problema da paragem 647
9.6 A máquina acelerada 650
9.6.1 A eficiência de uma máquina de Turing 650
9.6.2 Aceleração 652
9.7 Máquina de Turing não determinística 654
9.8 Máquinas de Turing enumeradoras 660
9.9 *Busy beaver* 661
9.10 Bibliografia do capítulo 664

A ORDENS DE MAGNITUDE **667**

B CODIFICAÇÃO **673**

B.1 Cardinalidade e equipotência de conjuntos 675
B.2 Cardinalidade da classe das linguagens 681
B.3 Codificação de sequências 682
B.4 Codificação linear 685
B.5 Bibliografia 686

BIBLIOGRAFIA **687**

ÍNDICE REMISSIVO **693**

CRÉDITOS FOTOGRÁFICOS **709**