Maria Welleda Baldoni • Ciro Ciliberto
Giulia Maria Piacentini Cattaneo

Elementary Number Theory, Cryptography and Codes

Springer

Maria Welleda Baldoni
Ciro Ciliberto
Giulia Maria Piacentini Cattaneo
Università di Roma - Tor Vergata
Dipartimento di Matematica
Via della Ricerca Scientifica, 1
00133 Roma
Italy
baldoni@mat.uniroma2.it
cilibert@mat.uniroma2.it
piacentini@mat.uniroma2.it

Translator:
Daniele A. Gewurz
Università di Roma "La Sapienza"
Dipartimento di Matematica
Ple Aldo Moro, 2
00185 Roma
Italy
gewurz@mat.uniroma1.it

Translation from the Italian language edition:
Aritmetica, crittografia e codici by W.M. Baldoni, C. Ciliberto, and G.M. Piacentini Cattaneo
Copyright © 2006 Springer-Verlag Italia
Springer is a part of Springer Science+Business Media
All Rights Reserved

ISBN 978-3-540-69199-0 e-ISBN 978-3-540-69200-3

Library of Congress Control Number: 2008938959

Mathematics Subject Classification (2000): 11G05, 14G50, 94B05

© 2009 Springer-Verlag Berlin Heidelberg

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilm or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Cover figure from *Balla, Ciacomo* © VG Bild-Kunst, Bonn 2008

Cover design: WMX Design GmbH, Heidelberg

Printed on acid-free paper

9 8 7 6 5 4 3 2 1

springer.com

Contents

1 A round-up on numbers 1
1.1 Mathematical induction 1
1.2 The concept of recursion 5
1.2.1 Fibonacci numbers 6
1.2.2 Further examples of population dynamics 11
1.2.3 The tower of Hanoi: a non-homogeneous linear case 13
1.3 The Euclidean algorithm 14
1.3.1 Division 14
1.3.2 The greatest common divisor 16
1.3.3 Bézout's identity 17
1.3.4 Linear Diophantine equations 20
1.3.5 Euclidean rings 21
1.3.6 Polynomials 23
1.4 Counting in different bases 30
1.4.1 Positional notation of numbers 30
1.4.2 Base 2 32
1.4.3 The four operations in base 2 33
1.4.4 Integer numbers in an arbitrary base 39
1.4.5 Representation of real numbers in an arbitrary base 40
1.5 Continued fractions 43
1.5.1 Finite simple continued fractions and rational numbers . 44
1.5.2 Infinite simple continued fractions and irrational numbers 48
1.5.3 Periodic continued fractions 56
1.5.4 A geometrical model for continued fractions 57
1.5.5 The approximation of irrational numbers by convergents 58
1.5.6 Continued fractions and Diophantine equations 61
Appendix to Chapter 1 62
A1 Theoretical exercises 62
B1 Computational exercises 73
C1 Programming exercises 84

2 Computational complexity ... 87
2.1 The idea of computational complexity ... 87
2.2 The symbol $\mathcal{O}$ ... 89
2.3 Polynomial time, exponential time ... 92
2.4 Complexity of elementary operations ... 95
2.5 Algorithms and complexity ... 97
2.5.1 Complexity of the Euclidean algorithm ... 98
2.5.2 From binary to decimal representation: complexity ... 101
2.5.3 Complexity of operations on polynomials ... 101
2.5.4 A more efficient multiplication algorithm ... 103
2.5.5 The Ruffini–Horner method ... 105
Appendix to Chapter 2 ... 107
A2 Theoretical exercises ... 107
B2 Computational exercises ... 109
C2 Programming exercises ... 113

3 From infinite to finite ... 115
3.1 Congruence: fundamental properties ... 115
3.2 Elementary applications of congruence ... 120
3.2.1 Casting out nines ... 120
3.2.2 Tests of divisibility ... 121
3.3 Linear congruences ... 122
3.3.1 Powers modulo n ... 126
3.4 The Chinese remainder theorem ... 128
3.5 Examples ... 133
3.5.1 Perpetual calendar ... 133
3.5.2 Round-robin tournaments ... 136
Appendix to Chapter 3 ... 136
A3 Theoretical exercises ... 136
B3 Computational exercises ... 140
C3 Programming exercises ... 147

4 Finite is not enough: factoring integers ... 149
4.1 Prime numbers ... 149
4.1.1 The Fundamental Theorem of Arithmetic ... 150
4.1.2 The distribution of prime numbers ... 152
4.1.3 The sieve of Eratosthenes ... 157
4.2 Prime numbers and congruences ... 160
4.2.1 How to compute Euler function ... 160
4.2.2 Fermat's little theorem ... 162
4.2.3 Wilson's theorem ... 165
4.3 Representation of rational numbers in an arbitrary base ... 166
4.4 Fermat primes, Mersenne primes and perfect numbers ... 168
4.4.1 Factorisation of integers of the form $b^n \pm 1$ ... 168
4.4.2 Fermat primes ... 170

4.4.3 Mersenne primes . . . 172
4.4.4 Perfect numbers . . . 173
4.5 Factorisation in an integral domain . . . 173
4.5.1 Prime and irreducible elements in a ring . . . 174
4.5.2 Factorial domains . . . 175
4.5.3 Noetherian rings . . . 177
4.5.4 Factorisation of polynomials over a field . . . 179
4.5.5 Factorisation of polynomials over a factorial ring . . . 182
4.5.6 Polynomials with rational or integer coefficients . . . 188
4.6 Lagrange interpolation and its applications . . . 191
4.7 Kronecker's factorisation method . . . 195
Appendix to Chapter 4 . . . 198
A4 Theoretical exercises . . . 198
B4 Computational exercises . . . 204
C4 Programming exercises . . . 211

5 Finite fields and polynomial congruences . . . 213
5.1 Some field theory . . . 213
5.1.1 Field extensions . . . 213
5.1.2 Algebraic extensions . . . 214
5.1.3 Splitting field of a polynomial . . . 217
5.1.4 Roots of unity . . . 218
5.1.5 Algebraic closure . . . 219
5.1.6 Finite fields and their subfields . . . 220
5.1.7 Automorphisms of finite fields . . . 222
5.1.8 Irreducible polynomials over $\mathbb{Z}_p$ . . . 222
5.1.9 The field $\mathbb{F}_4$ of order four . . . 224
5.1.10 The field $\mathbb{F}_8$ of order eight . . . 225
5.1.11 The field $\mathbb{F}_{16}$ of order sixteen . . . 226
5.1.12 The field $\mathbb{F}_9$ of order nine . . . 226
5.1.13 About the generators of a finite field . . . 227
5.1.14 Complexity of operations in a finite field . . . 228
5.2 Non-linear polynomial congruences . . . 229
5.2.1 Degree two congruences . . . 234
5.2.2 Quadratic residues . . . 236
5.2.3 Legendre symbol and its properties . . . 238
5.2.4 The law of quadratic reciprocity . . . 243
5.2.5 The Jacobi symbol . . . 245
5.2.6 An algorithm to compute square roots . . . 248
Appendix to Chapter 5 . . . 251
A5 Theoretical exercises . . . 251
B5 Computational exercises . . . 255
C5 Programming exercises . . . 260

6 Primality and factorisation tests 261
6.1 Pseudoprime numbers and probabilistic tests 261
6.1.1 Pseudoprime numbers 261
6.1.2 Probabilistic tests and deterministic tests 263
6.1.3 A first probabilistic primality test 263
6.1.4 Carmichael numbers 264
6.1.5 Euler pseudoprimes 265
6.1.6 The Solovay–Strassen probabilistic primality test 268
6.1.7 Strong pseudoprimes 268
6.1.8 The Miller–Rabin probabilistic primality test 272
6.2 Primitive roots 273
6.2.1 Primitive roots and index 278
6.2.2 More about the Miller–Rabin test 279
6.3 A polynomial deterministic primality test 281
6.4 Factorisation methods 290
6.4.1 Fermat factorisation method 291
6.4.2 Generalisation of Fermat factorisation method 292
6.4.3 The method of factor bases 294
6.4.4 Factorisation and continued fractions 299
6.4.5 The quadratic sieve algorithm 300
6.4.6 The ρ method 309
6.4.7 Variation of ρ method 311
Appendix to Chapter 6 313
A6 Theoretical exercises 313
B6 Computational exercises 315
C6 Programming exercises 317

7 Secrets... and lies 319
7.1 The classic ciphers 319
7.1.1 The earliest secret messages in history 319
7.2 The analysis of the ciphertext 325
7.2.1 Enciphering machines 329
7.3 Mathematical setting of a cryptosystem 330
7.4 Some classic ciphers based on modular arithmetic 334
7.4.1 Affine ciphers 336
7.4.2 Matrix or Hill ciphers 340
7.5 The basic idea of public key cryptography 341
7.5.1 An algorithm to compute discrete logarithms 344
7.6 The knapsack problem and its applications to cryptography 345
7.6.1 Public key cipher based on the knapsack problem, or Merkle–Hellman cipher 348
7.7 The *RSA* system 349
7.7.1 Accessing the *RSA* system 351
7.7.2 Sending a message enciphered with the *RSA* system 352
7.7.3 Deciphering a message enciphered with the *RSA* system 354

7.7.4 Why did it work? 356
7.7.5 Authentication of signatures with the *RSA* system 360
7.7.6 A remark about the security of *RSA* system 362
7.8 Variants of *RSA* system and beyond 363
7.8.1 Exchanging private keys 363
7.8.2 ElGamal cryptosystem 364
7.8.3 Zero-knowledge proof: persuading that a result is known without revealing its content nor its proof 365
7.8.4 Historical note 366
7.9 Cryptography and elliptic curves 366
7.9.1 Cryptography in a group 367
7.9.2 Algebraic curves in a numerical affine plane 368
7.9.3 Lines and rational curves 369
7.9.4 Hyperelliptic curves 370
7.9.5 Elliptic curves 372
7.9.6 Group law on elliptic curves 374
7.9.7 Elliptic curves over $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Q}$ 380
7.9.8 Elliptic curves over finite fields 381
7.9.9 Elliptic curves and cryptography 384
7.9.10 Pollard's $p-1$ factorisation method 385
Appendix to Chapter 7 386
A7 Theoretical exercises 386
B7 Computational exercises 390
C7 Programming exercises 401

8 Transmitting without... fear of errors 405
8.1 Birthday greetings 406
8.2 Taking photos in space or tossing coins, we end up at codes . . . 407
8.3 Error-correcting codes 410
8.4 Bounds on the invariants 413
8.5 Linear codes 419
8.6 Cyclic codes 425
8.7 Goppa codes 429
Appendix to Chapter 8 436
A8 Theoretical exercises 436
B8 Computational exercises 439
C8 Programming exercises 443

9 The future is already here: quantum cryptography 445
9.1 A first foray into the quantum world: Young's experiment 446
9.2 Quantum computers 449
9.3 Vernam's cipher 451
9.4 A short glossary of quantum mechanics 454
9.5 Quantum cryptography 460
Appendix to Chapter 9 467

A9 Theoretical exercises 467
B9 Computational exercises 468
C9 Programming exercises 469

Solution to selected exercises 471
Exercises of Chapter 1 471
Exercises of Chapter 2 482
Exercises of Chapter 3 483
Exercises of Chapter 4 487
Exercises of Chapter 5 492
Exercises of Chapter 6 496
Exercises of Chapter 7 498
Exercises of Chapter 8 501
Exercises of Chapter 9 504

References 507

Index 511