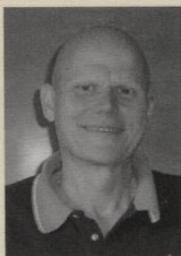


The idea behind this book is to provide the mathematical foundations for assessing modern developments in the Information Age. It deepens and complements the basic concepts, but it also considers instructive and more advanced topics. The treatise starts with a general chapter on algebraic structures; this part provides all the necessary knowledge for the rest of the book. The next chapter gives a concise overview of cryptography. Chapter 3 on number theoretic algorithms is important for developing cryptosystems, Chapter 4 presents the deterministic primality test of Agrawal, Kayal, and Saxena. The account to elliptic curves again focuses on cryptographic applications and algorithms. With combinatorics on words and automata theory, the reader is introduced to two areas of theoretical computer science where semigroups play a fundamental role. The last chapter is devoted to combinatorial group theory and its connections to automata.

- Contains brief chapter summaries as well as examples, problems and solutions.
- References for further reading in every chapter.
- Many illustrations of mathematical derivations.



Volker Diekert

studied in Hamburg and Montpellier. He earned his PhD in algebraic number theory in Regensburg and received the Habilitation in Munich. Since 1991 he holds the chair for Theoretical Informatics at the University of Stuttgart.



Manfred Kufleitner

teaches at the University of Stuttgart where he earned his PhD in computer science under the supervision of Volker Diekert. He has been a guest professor at TU Munich and an acting professor at the University of Hamburg.



Gerhard Rosenberger

did his doctorate in analytic number theory and habilitated in combinatorial group theory. Worldwide he worked for longer terms at nine universities. At present he teaches at the University of Hamburg.



Ulrich Hertrampf

studied Mathematics in Heidelberg, earned his PhD in Augsburg and his Habilitation at the University of Würzburg. Today he works as a Professor in the department for Theoretical Informatics at the University of Stuttgart.



www.degruyter.com

ISBN 978-3-11-041332-8

9 783110 413328

Contents

Preface — V

1 Algebraic structures — 1

- 1.1 Groups — 4
- 1.2 Regular polygons — 10
- 1.3 Symmetric groups — 13
- 1.4 Rings — 15
- 1.5 Modular arithmetic — 20
 - 1.5.1 Euclidean algorithm — 20
 - 1.5.2 Ideals in the integers — 22
 - 1.5.3 Chinese remainder theorem — 23
 - 1.5.4 Euler's totient function — 24
- 1.6 Polynomials and formal power series — 26
- 1.7 Hilbert's basis theorem — 32
- 1.8 Fields — 33
- 1.9 Finite fields — 35
- 1.10 Units modulo n — 37
- 1.11 Quadratic reciprocity — 38

Exercises — 41

Summary — 46

2 Cryptography — 49

- 2.1 Symmetric encryption methods — 50
- 2.2 Monoalphabetic cipher — 52
- 2.3 Polyalphabetic cipher — 53
- 2.4 Frequency analysis and coincidence index — 55
- 2.5 Perfect security and the Vernam one-time pad — 56
- 2.6 Asymmetric encryption methods — 58
- 2.7 RSA cryptosystem — 60
- 2.8 Rabin cryptosystem — 61
- 2.9 Diffie–Hellman key exchange — 63
- 2.10 ElGamal cryptosystem — 64
- 2.11 Cryptographic hash functions — 65
- 2.12 Digital signatures — 67
- 2.13 Secret sharing — 69
- 2.14 Digital commitment — 71
- 2.15 Shamir's attack on the Merkle–Hellman cryptosystem — 73

Exercises — 78

Summary — 81

3	Number theoretic algorithms — 83
3.1	Runtime analysis of algorithms — 83
3.2	Fast exponentiation — 86
3.3	Binary GCD — 87
3.4	Probabilistic recognition of primes — 88
3.4.1	Fermat primality test and Carmichael numbers — 88
3.4.2	Solovay–Strassen primality test — 89
3.4.3	Miller–Rabin primality test — 90
3.4.4	Applications of the Miller–Rabin scheme — 93
3.4.5	Miller–Rabin versus Solovay–Strassen — 95
3.5	Extracting roots in finite fields — 96
3.5.1	Tonelli’s algorithm — 97
3.5.2	Cipolla’s algorithm — 98
3.6	Integer factorization — 99
3.6.1	Pollard’s $p - 1$ algorithm — 100
3.6.2	Pollard’s rho algorithm for factorization — 100
3.6.3	Quadratic sieve — 101
3.7	Discrete logarithm — 103
3.7.1	Shanks’ baby-step giant-step algorithm — 104
3.7.2	Pollard’s rho algorithm for the discrete logarithm — 105
3.7.3	Pohlig–Hellman algorithm for group order reduction — 106
3.7.4	Index calculus — 107
3.8	Multiplication and division — 108
3.9	Discrete Fourier transform — 109
3.10	Primitive roots of unity — 112
3.11	Schönhage–Strassen integer multiplication — 113
Exercises	— 117
Summary	— 119
4	Polynomial time primality test — 121
4.1	Basic idea — 121
4.2	Combinatorial tools — 122
4.3	Growth of the least common multiple — 123
4.4	Of small numbers and large orders — 125
4.5	Agrawal–Kayal–Saxena primality test — 125
Summary	— 129
5	Elliptic curves — 131
5.1	Group law — 135
5.1.1	Lines — 135
5.1.2	Polynomials over elliptic curves — 137
5.1.3	Divisors — 141

5.1.4	Picard group — 143
5.2	Applications of elliptic curves — 144
5.2.1	Diffie–Hellman key exchange with elliptic curves — 145
5.2.2	Pseudocurves — 146
5.2.3	Factorization using elliptic curves — 148
5.2.4	Goldwasser–Kilian primality certificates — 150
5.3	Endomorphisms of elliptic curves — 153
Exercises	— 158
Summary	— 159

6 Combinatorics on words — 161

6.1	Commutation, transposition and conjugacy — 162
6.2	Fine and Wilf’s periodicity lemma — 164
6.3	Kruskal’s tree theorem — 165
Exercises	— 170
Summary	— 171

7 Automata — 173

7.1	Recognizable sets — 174
7.2	Rational sets — 181
7.3	Regular languages — 186
7.4	Star-free languages — 189
7.5	Krohn–Rhodes theorem — 193
7.6	Green’s relations — 205
7.7	Automata over infinite words — 210
7.7.1	Deterministic Büchi automata — 211
7.7.2	Union and intersection — 213
7.7.3	Omega-rational languages — 214
7.7.4	Recognizability of omega-regular languages — 216
7.7.5	Monadic second-order logic over infinite words — 219
7.8	Presburger arithmetic — 223
7.9	Solutions of linear Diophantine systems — 228
Exercises	— 231
Summary	— 234

8 Discrete infinite groups — 236

8.1	Classical algorithmic problems — 236
8.2	Residually finite monoids — 236
8.3	Presentations — 237
8.4	Rewriting systems — 238
8.4.1	Termination and confluence — 238
8.4.2	Semi-Thue systems — 241

8.5	Solving the word problem in finitely presented monoids —	246
8.6	Free partially commutative monoids and groups —	248
8.7	Semidirect products —	252
8.8	Amalgamated products and HNN extensions —	253
8.9	Rational sets and Benois' theorem —	259
8.10	Free groups —	262
8.11	The automorphism group of free groups —	268
8.12	The special linear group $SL(2, \mathbb{Z})$ —	277
	Exercises —	281
	Summary —	284

Solutions to exercises — 286

Chapter 1 —	286
Chapter 2 —	293
Chapter 3 —	297
Chapter 5 —	303
Chapter 6 —	306
Chapter 7 —	308
Chapter 8 —	318

Bibliography — 325

Index — 329