Contents

1 **Integers** 1
1.1 Natural Numbers 1
1.1.1 Basic Principles 1
1.1.2 Divisibility and Primes 4
1.1.3 Factoring Integers. The Sieve of Eratosthenes 9
1.2 The Euclidean Algorithm 14
1.2.1 Greatest Common Divisor and Least Common Multiple 14
1.2.2 Extended Euclidean Algorithm. Chinese Remainder Theorem 17
1.3 Fermat's Little Theorem and Its Generalisations 22
1.3.1 Euler's ϕ-Function 22
1.3.2 Congruences. Euler's Theorem 24
1.4 The Ring of Integers Modulo n. The Field $\mathbb{Z}_p$ 27
1.5 Representation of Numbers 32

2 **Cryptology** 37
2.1 Classical Secret-Key Cryptology 38
2.1.1 The One-Time Pad 39
2.1.2 An Affine Cryptosystem 41
2.1.3 Hill's Cryptosystem 43
2.2 Modern Public-Key Cryptology 47
2.2.1 One-Way Functions and Trapdoor Functions 47
2.3 Computational Complexity 49
2.3.1 Orders of Magnitude 50
2.3.2 The Time Complexity of Several Number-Theoretic Algorithms 54
2.4 The RSA Public-Key Cryptosystem 58
2.4.1 How Does the RSA System Work? 58
2.4.2 Why Does the RSA System Work? 61
2.4.3 Pseudoprimality Tests 64

2.5 Applications of Cryptology 69
References. 71

3 Groups 73
3.1 Permutations 73
3.1.1 Composition of Mappings. The Group of Permutations of Degree n. 73
3.1.2 Block Permutation Cipher 78
3.1.3 Cycles and Cycle Decomposition 79
3.1.4 Orders of Permutations 81
3.1.5 Analysis of Repeated Actions. 84
3.1.6 Transpositions. Even and Odd 86
3.1.7 Puzzle 15. 89
3.2 General Groups 93
3.2.1 Definition of a Group. Examples 93
3.2.2 Powers, Multiples and Orders. Cyclic Groups. 95
3.2.3 Isomorphism 97
3.2.4 Subgroups 100
3.3 The Abelian Group of an Elliptic Curve 103
3.3.1 Elliptic Curves. The Group of Points of an Elliptic Curve 104
3.3.2 Quadratic Residues and Hasse's Theorem 109
3.3.3 Calculating Large Multiples Efficiently 112
3.4 Applications to Cryptography. 114
3.4.1 Encoding Plaintext 114
3.4.2 Additive Diffie–Hellman Key Exchange and the Elgamal Cryptosystem 115
References. 116

4 Fields 117
4.1 Introduction to Fields 117
4.1.1 Examples and Elementary Properties of Fields 117
4.1.2 Vector Spaces 119
4.1.3 The Cardinality of a Finite Field. 124
4.2 The Multiplicative Group of a Finite Field Is Cyclic 125
4.2.1 Lemmas on Orders of Elements 126
4.2.2 Proof of the Main Theorem 128
4.2.3 Discrete Logarithms 129
4.3 The Elgamal Cryptosystem Revisited 130

5 Polynomials 133
5.1 The Ring of Polynomials. 133
5.1.1 Introduction to Polynomials 133
5.1.2 Lagrange Interpolation. 138

5.1.3 Factoring Polynomials . . . 140
5.1.4 Greatest Common Divisor and Least Common Multiple . . . 142
5.2 Finite Fields . . . 145
5.2.1 Polynomials Modulo $m(x)$ . . . 145
5.2.2 Minimal Annihilating Polynomials . . . 148

6 Secret Sharing . . . 153
6.1 Introduction to Secret Sharing . . . 154
6.1.1 Access Structure . . . 154
6.1.2 Shamir's Threshold Access Scheme . . . 155
6.2 A General Theory of Secret Sharing Schemes . . . 158
6.2.1 General Properties of Secret Sharing Schemes . . . 158
6.2.2 Linear Secret Sharing Schemes . . . 163
6.2.3 Ideal and Non-ideal Secret Sharing Schemes . . . 167
References . . . 170

7 Error-Correcting Codes . . . 171
7.1 Binary Error-Correcting Codes . . . 172
7.1.1 The Hamming Weight and the Hamming Distance . . . 172
7.1.2 Encoding and Decoding. Simple Examples . . . 175
7.1.3 Minimum Distance, Minimum Weight. Linear Codes . . . 178
7.1.4 Matrix Encoding Technique . . . 182
7.1.5 Parity Check Matrix . . . 187
7.1.6 The Hamming Codes . . . 190
7.1.7 Polynomial Codes . . . 193
7.1.8 Bose–Chaudhuri–Hocquenghem (BCH) Codes . . . 196
7.2 Non-binary Error-Correcting Codes . . . 199
7.2.1 The Basics of Non-binary Codes . . . 199
7.2.2 Reed–Solomon (RS) Codes . . . 201
7.3 Fingerprinting Codes . . . 204
7.3.1 The Basics of Fingerprinting . . . 204
7.3.2 Frameproof Codes . . . 207
7.3.3 Codes with the Identifiable Parent Property . . . 208
References . . . 211

8 Compression . . . 213
8.1 Prefix Codes . . . 214
8.1.1 Information and Information Relative to a Partition . . . 214
8.1.2 Non-uniform Encoding. Prefix Codes . . . 217
8.2 Fitingof's Compression Code . . . 221
8.2.1 Encoding . . . 221
8.2.2 Fast Decoding . . . 224

8.3 Information and Uncertainty 226
References 228

9 Appendix A: GAP 229
9.1 Computing with GAP 229
9.1.1 Starting with GAP 229
9.1.2 The GAP Interface 229
9.1.3 Programming in GAP: Variables, Lists, Sets and Loops 230
9.2 Number Theory 231
9.2.1 Basic Number-Theoretic Algorithms 232
9.2.2 Arithmetic Modulo m 234
9.2.3 Digitising Messages 235
9.3 Matrix Algebra 237
9.4 Algebra 238
9.4.1 Permutations 238
9.4.2 Elliptic Curves 239
9.4.3 Finite Fields 245
9.4.4 Polynomials 246

10 Appendix B: Miscellanies 249
10.1 Linear Dependency Relationship Algorithm 249
10.2 The Vandermonde Determinant 250

11 Solutions to Exercises 253
11.1 Solutions to Exercises of Chap. 1 253
11.2 Solutions to Exercises of Chap. 2 266
11.3 Solutions to Exercises of Chap. 3 283
11.4 Solutions to Exercises of Chap. 4 296
11.5 Solutions to Exercises of Chap. 5 301
11.6 Solutions to Exercises of Chap. 6 309
11.7 Solutions to Exercises of Chap. 7 315
11.8 Solutions to Exercises of Chap. 8 327