Contents

Preface ix

1 Integers and Computer Algebra 1

Integers 1
Computer Algebra versus Numerical Analysis 3
Sums and Products 5
Mathematical Induction 7

2 Codes 13

Binary and Hexadecimal Codes 13
ASCII Code 19
Morse Code 21
Braille 23
Two-out-of-Five Code 26
Hollerith Codes 27

3 Euclidean Algorithm 31

Modular Function 31
Greatest Common Divisors and the Euclidean Algorithm 33
Extended GCD Algorithm 38
Fundamental Theorem of Arithmetic 42
Modular Arithmetic 45

4 Ciphers 51

Cryptology 51
Cryptanalysis 57
Substitution and Permutation Ciphers 63
Block Ciphers 70
The Playfair Cipher 75
Unbreakable Ciphers 79
Enigma Machine 81

5 Error-Control Codes 87

Weights and Hamming Distance 87
Bar Codes Based on Code 2 of 5 91
Other Commercial Codes 96
Hamming (7, 4) Code 104

6 Chinese Remainder Theorem 111

Systems of Linear Equations Modulo n 111
Chinese Remainder Theorem 115
Extended Precision Arithmetic 119
Greatest Common Divisor of Polynomials 124
Hilbert Matrix 129

7 Theorems of Fermat and Euler 133

Wilson's Theorem 133
Powers Modulo n 135
Fermat's Little Theorem 138
Rabin's Probabilistic Primality Test 142
Exponential Ciphers 148
Euler's Theorem 150

8 Public Key Ciphers 155

The Rivest-Shamir-Adleman Cipher System 155
Electronic Signatures 159
A System for Exchanging Messages 162
RSA with Error Correction 166
Knapsack Ciphers 166
Digital Signature Standard 170

9 Finite Fields 175

The Galois Field GF_p 175
The Ring $GF_p\,[x]$ of Polynomials 180
The Galois Field GF_4 185
The Galois Fields GF_8 and GF_{16} 190
The Galois Field GF_{p^n} 199
The Multiplicative Group of GF_{p^n} 203
Random Number Generators 209

10 Error-Correcting Codes 215

The Bose-Chaudhuri-Hocquenghem Codes 215
A BCH Decoder 220
Reed-Solomon Codes 227
Two-Dimensional Bar Codes 229

11 Advanced Encryption Standard 231

Data Encryption Standard 232
The Galois Field GF_{256} 234
The Rijndael Block Cipher 239

12 Polynomial Algorithms and Fast Fourier Transforms 245

Lagrange Interpolation Formula 245
Kronecker's Algorithm 248
Neville's Iterated Interpolation Algorithm 252
Secure Multiparty Protocols 256
Mod p Fast Fourier Transforms 258
Fast Fourier Interpolation 266

Appendix A Hints for Using Technology 271

Appendix B Solutions to Odd Exercises 341

Bibliography 415

Index 417