CONTENTS

Preface *xiii*

Chapter 1: A Brief Survey of Elementary Functions **1**

1.1 Mathematical Induction 1

1.2 Factorials and The Stirling Formula 11

1.3 Recursive Definitions 12

1.4 Elementary Functions 14

1.4.1 Quadratic Functions 16

1.4.2 Exponential and Logarithmic Functions 17

1.4.3 Trigonometric Functions 19

1.5 Stirling Asymptotic Formula 20

1.6 Exercises 23

Chapter 2: Propositional Algebra **27**

2.1 Propositions 27

2.2 Connectives: Truth Tables 31

2.2.1 Order of Operations 44

2.3 Exercises 48

Chapter 3: Naïve and Formal (Axiomatic) Set Theory **51**

3.1 Classes and Sets. Axioms and Theorems 51

3.1.1 Classical Set Theory 54

3.1.2 Operations on Sets: Set Diagrams 60

3.2 Exercises 65

Chapter 4: Groups, Rings, and Fields **67**
4.1 Groups, Rings, and Fields 67
4.2 Matrices and Determinants 71
4.3 Finite Groups 75
4.3.1 Cyclic Groups 77
4.4 The Discrete Logarithm Problem 78
4.5 Exercises 78

Chapter 5: Predicates and Quantifiers—Algebraic Theory **79**
5.1 Predicates 79
5.2 Quantifiers 81
5.2.1 Commutativity of Quantifiers and Boolean Operations 83
5.3 Exercises 91

Chapter 6: Binary Relations and Relational Databases **93**
6.1 Ordered Totalities and Cartesian Products 93
6.2 Relations 96
6.2.1 Special Classes of Relations 98
6.3 Orderings and Posets 100
6.3.1 Equivalence Relations 104
6.3.2 Equivalence Classes 106
6.4 Relation Databases 110
6.5 Exercises 115

Chapter 7: Combinatorics **117**
7.1 Finite and Infinite Sets: Basic Rules 117
7.1.1 The Sum and Product Rules 118
7.1.2 Unions, Cartesian Products, Booleans 119
7.1.3 Arrangements and Combinations 124
7.1.4 Stirling Numbers 129
7.1.5 Combinations With Repetitions 131
7.1.6 Permutations With Identified Elements 133
7.2 Exercises 136

Chapter 8: Elements of Number Theory 139
8.1 Divisibility and FTA 139
8.1.1 Divisibility, the FTA, and the Euclidean Algorithm 139
8.1.2 Euclidean Algorithm 140
8.1.3 Algorithms 142
8.1.4 Modular or Clock Arithmetic: Linear Congruences 143
8.1.5 Totient Function 152
8.1.6 Pseudorandom Numbers 154
8.1.7 Cryptography Application: Sharing Secrets 157
8.1.8 Affine Ciphers 158
8.2 Exercises 160
Chapter 9: Boolean Functions 163
9.1 Boolean Degree: DNF and CNF 163
9.2 Boolean Polynomials 167
9.3 Boolean Derivatives 169
9.4 Exercises 170
Chapter 10: Hashing Functions and Cryptographic Maps 171
10.1 Rosetta Stone 171
10.2 Hashing Functions 172
10.3 Substitution Ciphers 173
10.4 Exercises 178
Chapter 11: Generating Polynomials and Inversion Formulas 179
11.1 Partitions of the Integers 180
11.1.1 Compositions 182
11.1.2 Inversion Formulas 183
11.2 Exercises 184
Chapter 12: Systems of Representatives 187
12.1 SDRs 187
12.1.1 Systems of Triples 190
12.2 Exercises 191

Chapter 13: Boolean Algebras **193**
13.1 Operations and Axioms 193
13.2 Boolean Rings 195
13.3 Exercises 200

Chapter 14: Combinatorial Circuits **201**
14.1 Graphs and Schemes 201
14.2 Logical Problems 203
14.2.1 Binary Adders 204
14.3 Exercises 209

Chapter 15: Complete Systems of Boolean Functions and Bases **211**
15.1 Complete Systems and Bases 211
15.2 Post Theorem 217
15.2.1 Bases 222
15.3 Exercises 223

Chapter 16: Introductory Graph Theory, Euler's Formula, and Unbreakable Ciphers **225**
16.1 Graphs and Diagrams 225
16.2 Connectivity in Graphs 229
16.2.1 Unbreakable Ciphers 230
16.2.2 Bipartite Graphs 241
16.3 Exercises 243

Chapter 17: Trees and Digraphs **245**
17.1 Spanning Trees 247
17.2 Binary Search 260
17.3 Exercises 261

Chapter 18: Computations and Algorithms **263**
18.1 Exercise 270

Chapter 19: Finite Automata **271**
19.1 Simple Model 271
19.2 Tables and Graphs of Automata 273

19.3 Classification: Equivalent States and Equivalent Automata 275
19.3.1 Minimization of Automata 277
19.3.2 Automaton Operators 281
19.3.3 Regular Grammars 286
19.4 Exercises 296

Chapter 20: Introduction to Game Theory 297
20.1 Classification of Strategies 302
20.2 Exercises 307

Chapter 21: Information Theory and Coding 309
21.1 Measure of Information 312
21.2 Channels 313
21.3 Exercises 317

Chapter 22: Probability Theory with a Finite Sample Space and the Birthday Problem 319
22.1 Random Experiments 319
22.2 Probability Distributions 320
22.3 Expectation: Bayes Formula 329
22.4 Bernoulli Trials and The Birthday Problem 332
22.5 Exercises 338

Chapter 23: Turing Machines, P and NP Classes, and Other Models of Computation 341
23.1 Turing Machines 341
23.2 Exercise 349

Chapter 24: Answers and Solutions to Selected Exercises 351

Bibliography 361
Index 365