Contents

Preface ix

Introduction x

Advice to the reader xiii

1 Number theory 1

1.1 Mathematical induction 1

1.2 The division algorithm and greatest common divisors 10

1.3 Primes and the Unique Factorisation Theorem 19

1.4 Congruence classes 28

1.5 Solving linear congruences 40

1.6 Euler's Theorem and public key codes 50

2 Sets, functions and relations 67

2.1 Elementary set theory 67

2.2 Functions 75

2.3 Relations 92

2.4 Finite state machines 106

3 Logic, boolean algebra and normal forms 115

3.1 Propositional calculus 115

3.2 Boolean algebras 125

3.3 Karnaugh maps and switching circuits 140

4 Examples of groups 155

4.1 Permutations 155

4.2 The order and sign of a permutation 167

4.3 Definition and examples of groups 178

4.4 Algebraic structures 192

5 Group theory and error-correcting codes 206

5.1 Preliminaries 206

5.2 Cosets and Lagrange's Theorem 215

5.3 Groups of small order 221

5.4 Error-detecting and error-correcting codes 232

Answers 257

References and further reading 275

Biography 278

Name index 283

Subject index 285