

Contents

| | |
|---|----------------|
| <i>Preface to first edition</i> | <i>page</i> ix |
| <i>Preface to second edition</i> | x |
| <i>Introduction</i> | xi |
| <i>Advice to the reader</i> | xiv |
| 1 Number theory | 1 |
| 1.1 The division algorithm and greatest common divisors | 1 |
| 1.2 Mathematical induction | 15 |
| 1.3 Primes and the Unique Factorisation Theorem | 25 |
| 1.4 Congruence classes | 36 |
| 1.5 Solving linear congruences | 49 |
| 1.6 Euler's Theorem and public key codes | 59 |
| Summary of Chapter 1 | 77 |
| 2 Sets, functions and relations | 78 |
| 2.1 Elementary set theory | 78 |
| 2.2 Functions | 86 |
| 2.3 Relations | 103 |
| 2.4 Finite state machines | 117 |
| Summary of Chapter 2 | 126 |
| 3 Logic and mathematical argument | 127 |
| 3.1 Propositional logic | 128 |
| 3.2 Quantifiers | 137 |
| 3.3 Some proof strategies | 141 |
| Summary of Chapter 3 | 146 |
| 4 Examples of groups | 147 |
| 4.1 Permutations | 148 |
| 4.2 The order and sign of a permutation | 159 |
| 4.3 Definition and examples of groups | 170 |

| | | |
|----------|--|-----|
| 4.4 | Algebraic structures | 184 |
| | Summary of Chapter 4 | 199 |
| 5 | Group theory and error-correcting codes | 200 |
| 5.1 | Preliminaries | 200 |
| 5.2 | Cosets and Lagrange's Theorem | 212 |
| 5.3 | Groups of small order | 219 |
| 5.4 | Error-detecting and error-correcting codes | 230 |
| | Summary of Chapter 5 | 253 |
| 6 | Polynomials | 255 |
| 6.1 | Introduction | 255 |
| 6.2 | The division algorithm for polynomials | 262 |
| 6.3 | Factorisation | 273 |
| 6.4 | Polynomial congruence classes | 279 |
| 6.5 | Cyclic codes | 284 |
| | Summary of Chapter 6 | 291 |
| | <i>Appendix on complex numbers</i> | 292 |
| | <i>Answers</i> | 296 |
| | <i>References and further reading</i> | 323 |
| | <i>Biography</i> | 326 |
| | <i>Name index</i> | 331 |
| | <i>Subject index</i> | 333 |