

---

# Contents

---

## PART I FOUNDATIONS

<b>1. Statements and proofs</b>	
1.1 Some mathematical statements	3
1.2 How to do mathematics	4
1.3 Compound statements	6
1.4 Existential statements	7
1.5 Universal statements	8
1.6 Proof techniques	10
1.7 Miscellaneous Exercises	11
<b>2. Set notation</b>	
2.1 Sets of objects and numbers	12
2.2 Subsets	13
2.3 Union and intersection	14
2.4 Miscellaneous Exercises	15
<b>3. The logical framework</b>	
3.1 The basic logical operations: not, or, and	17
3.2 Logical equivalence	18
3.3 if - then	19
3.4 The converse statement	20
3.5 The contrapositive statement	21
3.6 Universal and existential quantifiers	22
3.7 Miscellaneous Exercises	24
<b>4. Natural numbers</b>	
4.1 The 'laws of algebra'	25
4.2 Putting the natural numbers in order	26
4.3 The principle of induction	28
4.4 Summation formulae	29
4.5 Recursive definitions	31
4.6 Other forms of the principle of induction	32
4.7 Greatest and least members	34
4.8 How a conjecture becomes a theorem	35
4.9 Miscellaneous Exercises	38

**5. Functions**

5.1	The concept of a function	39
5.2	Surjections, injections, bijections	40
5.3	Composition of functions	42
5.4	Bijections and inverse functions	43
5.5	Miscellaneous Exercises	45

**6. How to count**

6.1	Counting as a bijection	46
6.2	The size of a set	47
6.3	A counting problem	49
6.4	Some applications of the pigeonhole principle	50
6.5	Infinite sets	51
6.6	Strange properties of infinite sets	53
6.7	Miscellaneous Exercises	55

**7. Integers**

7.1	Negative numbers	56
7.2	Equivalence relations	56
7.3	Classification	58
7.4	Construction of the integers	60
7.5	Properties of the integers	61
7.6	Bounded subsets of $\mathbb{Z}$	63
7.7	Miscellaneous Exercises	64

**8. Divisibility and prime numbers**

8.1	Divisibility	65
8.2	Quotient and remainder	65
8.3	Representation of integers	66
8.4	The greatest common divisor	67
8.5	Prime numbers	70
8.6	Existence and uniqueness of prime factorization	71
8.7	Miscellaneous Exercises	73

**9. Fractions and real numbers**

9.1	Construction and properties of rational numbers	75
9.2	Density of fractions	76
9.3	Decimal representations of fractions	78
9.4	Real numbers	80
9.5	Approximations for real numbers	82
9.6	The greatest lower bound property	84
9.7	The real numbers are more plentiful than the rationals	85
9.8	Miscellaneous Exercises	87

## PART II TECHNIQUES

### 10. Principles of counting

10.1	The addition principle	91
10.2	Counting sets of pairs	92
10.3	Euler's function	95
10.4	Functions, words, and selections	97
10.5	Injections as ordered selections without repetition	99
10.6	Permutations	100
10.7	Miscellaneous Exercises	103

### 11. Subsets and designs

11.1	Binomial numbers	105
11.2	Unordered selections with repetition	108
11.3	The binomial theorem	110
11.4	The sieve principle	112
11.5	Some arithmetical applications	114
11.6	Designs	118
11.7	$t$ -designs	122
11.8	Miscellaneous Exercises	124

### 12. Partition, classification, and distribution

12.1	Partitions of a set	126
12.2	Classification and equivalence relations	128
12.3	Distributions and the multinomial numbers	129
12.4	Partitions of a positive integer	132
12.5	Classification of permutations	134
12.6	Even and odd permutations	136
12.7	Miscellaneous Exercises	140

### 13. Modular arithmetic

13.1	Congruences	142
13.2	$\mathbb{Z}_m$ and its arithmetic	144
13.3	Invertible elements of $\mathbb{Z}_m$	147
13.4	Cyclic constructions for designs	149
13.5	Latin squares	153
13.6	Miscellaneous Exercises	156

## PART III ALGORITHMS AND GRAPHS

### 14. Algorithms and their efficiency

14.1	What is an algorithm?	159
14.2	The language of programs	161
14.3	Algorithms and programs	164
14.4	Proving that an algorithm is correct	165

14.5	Efficiency of algorithms	168
14.6	Growth rates: the $O$ notation	170
14.7	Comparison of algorithms	171
14.8	Introduction to sorting algorithms	173
14.9	Miscellaneous Exercises	176
<b>15.</b>	<b>Graphs</b>	
15.1	Graphs and their representation	178
15.2	Isomorphism of graphs	179
15.3	Degree	181
15.4	Paths and cycles	183
15.5	Trees	185
15.6	Colouring the vertices of a graph	187
15.7	The greedy algorithm for vertex-colouring	188
15.8	Miscellaneous Exercises	191
<b>16.</b>	<b>Trees, sorting, and searching</b>	
16.1	Counting the leaves on a rooted tree	193
16.2	Trees and sorting algorithms	196
16.3	Spanning trees and the MST problem	199
16.4	Depth-first search	202
16.5	Breadth-first search	205
16.6	The shortest path problem	206
16.7	Miscellaneous Exercises	208
<b>17.</b>	<b>Bipartite graphs and matching problems</b>	
17.1	Relations and bipartite graphs	210
17.2	Edge colourings of graphs	212
17.3	Application of edge colouring to latin squares	213
17.4	Matchings	216
17.5	Maximum matchings	219
17.6	Transversals for families of finite sets	221
17.7	Miscellaneous Exercises	223
<b>18.</b>	<b>Digraphs, networks, and flows</b>	
18.1	Digraphs	225
18.2	Networks and critical paths	227
18.3	Flows and cuts	229
18.4	The max-flow min-cut theorem	232
18.5	The labelling algorithm for network flows	235
18.6	Miscellaneous Exercises	239
<b>19.</b>	<b>Recursive techniques</b>	
19.1	Generalities about recursion	240
19.2	Linear recursion	241

19.3	Recursive bisection	243
19.4	Recursive optimization	245
19.5	The framework of dynamic programming	248
19.6	Examples of the dynamic programming method	250
19.7	Miscellaneous Exercises	253

## PART IV ALGEBRAIC METHODS

### 20. Groups

20.1	The axioms for a group	259
20.2	Examples of groups	260
20.3	Basic algebra in groups	263
20.4	The order of a group element	265
20.5	Isomorphism of groups	266
20.6	Cyclic groups	268
20.7	Subgroups	270
20.8	Cosets and Lagrange's theorem	273
20.9	Characterization of cyclic groups	277
20.10	Miscellaneous Exercises	279

### 21. Groups of permutations

21.1	Definitions and examples	281
21.2	Orbits and stabilizers	283
21.3	The size of an orbit	285
21.4	The number of orbits	288
21.5	Representation of groups by permutations	290
21.6	Applications to group theory	292
21.7	Miscellaneous Exercises	295

### 22. Rings, fields, and polynomials

22.1	Rings	296
22.2	Invertible elements of a ring	297
22.3	Fields	299
22.4	Polynomials	301
22.5	The division algorithm for polynomials	304
22.6	The Euclidean algorithm for polynomials	306
22.7	Factorization of polynomials in theory	309
22.8	Factorization of polynomials in practice	310
22.9	Miscellaneous Exercises	313

### 23. Finite fields and some applications

23.1	A field with nine elements	314
23.2	The order of a finite field	315
23.3	Construction of finite fields	317
23.4	The primitive element theorem	318
23.5	Finite fields and latin squares	322

23.6	Finite geometry and designs	324
23.7	Projective planes	327
23.8	Squares in finite fields	330
23.9	Existence of finite fields	333
23.10	Miscellaneous Exercises	336
<b>24.</b>	<b>Error-correcting codes</b>	
24.1	Words, codes, and errors	338
24.2	Linear codes	341
24.3	Construction of linear codes	343
24.4	Correcting errors in linear codes	345
24.5	Cyclic codes	349
24.6	Classification and properties of cyclic codes	351
24.7	Miscellaneous Exercises	355
<b>25.</b>	<b>Generating functions</b>	
25.1	Power series and their algebraic properties	357
25.2	Partial fractions	360
25.3	The binomial theorem for negative exponents	364
25.4	Generating functions	367
25.5	The homogeneous linear recursion	369
25.6	Non-homogeneous linear recursions	372
25.7	Miscellaneous Exercises	374
<b>26.</b>	<b>Partitions of a positive integer</b>	
26.1	Partitions and diagrams	376
26.2	Conjugate partitions	378
26.3	Partitions and generating functions	379
26.4	Generating functions for restricted partitions	382
26.5	A mysterious identity	384
26.6	The calculation of $p(n)$	387
26.7	Miscellaneous Exercises	388
<b>27.</b>	<b>Symmetry and counting</b>	
27.1	The cycle index of a group of permutations	390
27.2	Cyclic and dihedral symmetry	392
27.3	Symmetry in three dimensions	395
27.4	The number of inequivalent colourings	397
27.5	Sets of colourings and their generating functions	400
27.6	Pólya's theorem	402
27.7	Miscellaneous Exercises	405
	<b>Answers to exercises</b>	407
	<b>Index</b>	421