

Contents

1	Arithmetic	1
1.1	Divisors and multiples	1
1.2	Euclid's algorithm	2
1.3	Linear diophantine equations	5
1.4	Prime numbers	6
1.5	Factorization	7
1.6	Exercises	9
2	Modular arithmetic	10
2.1	Arithmetic modulo n	10
2.2	Linear congruences	12
2.3	The a -ary number system	14
2.4	The RSA cryptosystem	15
2.5	Radar detection	16
2.6	Exercises	18
3	Polynomials	20
3.1	The notion of a polynomial	20
3.2	Division of polynomials	22
3.3	Polynomial functions	25
3.4	Factorization	27
3.5	Shift registers	30
3.6	Exercises	33
4	Arithmetic modulo polynomials	35
4.1	Congruence modulo a polynomial	35
4.2	The residue class ring	37
4.3	Two special cases	41
4.4	Inverses and fields	43
4.5	Finite fields	45
4.6	Error correcting codes	46
4.7	Exercises	50
5	Permutations	53
5.1	Symmetric Groups	53
5.2	Cycles	55
5.3	Alternating groups	59
5.4	Exercises	62
6	Monoids and groups	65
6.1	Binary operations	65
6.2	Monoids	68
6.3	Invertibility in monoids	73
6.4	Groups	75
6.5	Cyclic groups	80
6.6	Cosets	82
6.7	Exercises	85
7	Rings and fields	88
7.1	The structure ring	88
7.2	Constructions with rings	93
7.3	Domains and fields	96
7.4	Fields	102
7.5	Ideals	109

7.6	Residue class rings	114
7.7	Finite fields	118
7.8	Exercises	124
8	Permutation groups	127
8.1	Permutation groups	127
8.2	Orbits	131
8.3	Order	135
8.4	Automorphisms	140
8.5	Quotient groups	144
8.6	Small groups	146
8.7	Exercises	150
9	Appendix: A guide to Algebra Interactive	157
9.1	Using Algebra Interactive	157
9.2	Authors	159
9.3	Acknowledgements	159