

Contents

Notes to the Reader	xiii
1. Divisibility	1
1.1 Divisors	2
1.2 Bezout's identity	7
1.3 Least common multiples	12
1.4 Linear Diophantine equations	13
1.5 Supplementary exercises	16
2. Prime Numbers	19
2.1 Prime numbers and prime-power factorisations	19
2.2 Distribution of primes	25
2.3 Fermat and Mersenne primes	30
2.4 Primality-testing and factorisation	32
2.5 Supplementary exercises	35
3. Congruences	37
3.1 Modular arithmetic	37
3.2 Linear congruences	46
3.3 Simultaneous linear congruences	52
3.4 Simultaneous non-linear congruences	57
3.5 An extension of the Chinese Remainder Theorem	59
3.6 Supplementary exercises	62
4. Congruences with a Prime-power Modulus	65
4.1 The arithmetic of $\mathbb{Z}_p$	65
4.2 Pseudoprimes and Carmichael numbers	72

4.3	Solving congruences mod (p^e)	78
4.4	Supplementary exercises	82
5.	Euler's Function	83
5.1	Units	83
5.2	Euler's function	85
5.3	Applications of Euler's function	92
5.4	Supplementary exercises	96
6.	The Group of Units	97
6.1	The group U_n	97
6.2	Primitive roots	99
6.3	The group U_{p^e} , where p is an odd prime	103
6.4	The group U_{2^e}	106
6.5	The existence of primitive roots	108
6.6	Applications of primitive roots	110
6.7	The algebraic structure of U_n	113
6.8	The universal exponent	116
6.9	Supplementary exercises	117
7.	Quadratic Residues	119
7.1	Quadratic congruences	119
7.2	The group of quadratic residues	120
7.3	The Legendre symbol	123
7.4	Quadratic reciprocity	130
7.5	Quadratic residues for prime-power moduli	135
7.6	Quadratic residues for arbitrary moduli	138
7.7	Supplementary exercises	140
8.	Arithmetic Functions	143
8.1	Definition and examples	143
8.2	Perfect numbers	146
8.3	The Möbius Inversion Formula	148
8.4	An application of the Möbius Inversion Formula	152
8.5	Properties of the Möbius function	154
8.6	The Dirichlet product	157
8.7	Supplementary exercises	162
9.	The Riemann Zeta Function	163
9.1	Historical background	163
9.2	Convergence	165
9.3	Applications to prime numbers	166

9.4	Random integers	170
9.5	Evaluating $\zeta(2)$	174
9.6	Evaluating $\zeta(2k)$	176
9.7	Dirichlet series	179
9.8	Euler products	182
9.9	Complex variables	185
9.10	Supplementary exercises	188
10.	Sums of Squares	191
10.1	Sums of two squares	191
10.2	The Gaussian integers	196
10.3	Sums of three squares	201
10.4	Sums of four squares	202
10.5	Digression on quaternions	205
10.6	Minkowski's Theorem	206
10.7	Supplementary exercises	214
11.	Fermat's Last Theorem	217
11.1	The problem	217
11.2	Pythagoras's Theorem	218
11.3	Pythagorean triples	219
11.4	Isosceles triangles and irrationality	221
11.5	The classification of Pythagorean triples	223
11.6	Fermat	226
11.7	The case $n = 4$	227
11.8	Odd prime exponents	228
11.9	Lamé and Kummer	233
11.10	Modern developments	234
11.11	Further reading	237
Appendix A. Induction and Well-ordering		239
Appendix B. Groups, Rings and Fields		243
Appendix C. Convergence		247
Appendix D. Table of Primes $p < 1000$		249
Solutions to Exercises		251
Bibliography		289
Index of symbols		291