

Contents

	<i>Preface</i>	<i>page xi</i>
	<i>Introduction</i>	<i>xiii</i>
1	Divisibility	1
	1.1 Foundations	1
	1.2 Division algorithm	1
	1.3 Greatest common divisor	2
	1.4 Euclid’s algorithm	2
	1.5 Fundamental theorem	4
	1.6 Properties of the primes	4
	1.7 Further reading	6
	1.8 Exercises	7
2	Arithmetical functions	8
	2.1 The function $[x]$	8
	2.2 Multiplicative functions	9
	2.3 Euler’s (totient) function $\phi(n)$	9
	2.4 The Möbius function $\mu(n)$	10
	2.5 The functions $\tau(n)$ and $\sigma(n)$	12
	2.6 Average orders	13
	2.7 Perfect numbers	14
	2.8 The Riemann zeta-function	15
	2.9 Further reading	17
	2.10 Exercises	17
3	Congruences	19
	3.1 Definitions	19
	3.2 Chinese remainder theorem	19
	3.3 The theorems of Fermat and Euler	21
	3.4 Wilson’s theorem	21

vi	<i>Contents</i>	
	3.5	Lagrange’s theorem 22
	3.6	Primitive roots 23
	3.7	Indices 26
	3.8	Further reading 26
	3.9	Exercises 26
4	Quadratic residues	28
	4.1	Legendre’s symbol 28
	4.2	Euler’s criterion 28
	4.3	Gauss’ lemma 29
	4.4	Law of quadratic reciprocity 30
	4.5	Jacobi’s symbol 32
	4.6	Further reading 33
	4.7	Exercises 34
5	Quadratic forms	36
	5.1	Equivalence 36
	5.2	Reduction 37
	5.3	Representations by binary forms 38
	5.4	Sums of two squares 39
	5.5	Sums of four squares 40
	5.6	Further reading 41
	5.7	Exercises 42
6	Diophantine approximation	43
	6.1	Dirichlet’s theorem 43
	6.2	Continued fractions 44
	6.3	Rational approximations 46
	6.4	Quadratic irrationals 48
	6.5	Liouville’s theorem 51
	6.6	Transcendental numbers 53
	6.7	Minkowski’s theorem 55
	6.8	Further reading 58
	6.9	Exercises 59
7	Quadratic fields	61
	7.1	Algebraic number fields 61
	7.2	The quadratic field 62
	7.3	Units 63
	7.4	Primes and factorization 65

<i>Contents</i>		vii
7.5	Euclidean fields	66
7.6	The Gaussian field	68
7.7	Further reading	69
7.8	Exercises	70
8	Diophantine equations	71
8.1	The Pell equation	71
8.2	The Thue equation	74
8.3	The Mordell equation	76
8.4	The Fermat equation	80
8.5	The Catalan equation	83
8.6	The <i>abc</i> -conjecture	85
8.7	Further reading	87
8.8	Exercises	88
9	Factorization and primality testing	90
9.1	Fermat pseudoprimes	90
9.2	Euler pseudoprimes	91
9.3	Fermat factorization	93
9.4	Fermat bases	93
9.5	The continued-fraction method	94
9.6	Pollard’s method	96
9.7	Cryptography	97
9.8	Further reading	97
9.9	Exercises	98
10	Number fields	99
10.1	Introduction	99
10.2	Algebraic numbers	100
10.3	Algebraic number fields	100
10.4	Dimension theorem	101
10.5	Norm and trace	102
10.6	Algebraic integers	103
10.7	Basis and discriminant	104
10.8	Calculation of bases	106
10.9	Further reading	109
10.10	Exercises	109
11	Ideals	111
11.1	Origins	111

viii	<i>Contents</i>	
11.2	Definitions	111
11.3	Principal ideals	112
11.4	Prime ideals	113
11.5	Norm of an ideal	114
11.6	Formula for the norm	115
11.7	The different	117
11.8	Further reading	120
11.9	Exercises	120
12	Units and ideal classes	122
12.1	Units	122
12.2	Dirichlet's unit theorem	123
12.3	Ideal classes	126
12.4	Minkowski's constant	128
12.5	Dedekind's theorem	129
12.6	The cyclotomic field	131
12.7	Calculation of class numbers	136
12.8	Local fields	139
12.9	Further reading	144
12.10	Exercises	145
13	Analytic number theory	147
13.1	Introduction	147
13.2	Dirichlet series	148
13.3	Tchebychev's estimates	151
13.4	Partial summation formula	153
13.5	Mertens' results	154
13.6	The Tchebychev functions	156
13.7	The irrationality of $\zeta(3)$	157
13.8	Further reading	159
13.9	Exercises	160
14	On the zeros of the zeta-function	162
14.1	Introduction	162
14.2	The functional equation	163
14.3	The Euler product	166
14.4	On the logarithmic derivative of $\zeta(s)$	167
14.5	The Riemann hypothesis	170
14.6	Explicit formula for $\zeta'(s)/\zeta(s)$	171
14.7	On certain sums	173

<i>Contents</i>		ix
14.8	The Riemann–von Mangoldt formula	174
14.9	Further reading	177
14.10	Exercises	177
15	On the distribution of the primes	179
15.1	The prime-number theorem	179
15.2	Refinements and developments	182
15.3	Dirichlet characters	184
15.4	Dirichlet L -functions	186
15.5	Primes in arithmetical progressions	187
15.6	The class number formulae	189
15.7	Siegel’s theorem	191
15.8	Further reading	194
15.9	Exercises	194
16	The sieve and circle methods	197
16.1	The Eratosthenes sieve	197
16.2	The Selberg upper-bound sieve	198
16.3	Applications of the Selberg sieve	202
16.4	The large sieve	204
16.5	The circle method	207
16.6	Additive prime number theory	210
16.7	Further reading	213
16.8	Exercises	214
17	Elliptic curves	215
17.1	Introduction	215
17.2	The Weierstrass $\wp$ -function	216
17.3	The Mordell–Weil group	220
17.4	Heights on elliptic curves	222
17.5	The Mordell–Weil theorem	225
17.6	Computing the torsion subgroup	228
17.7	Conjectures on the rank	230
17.8	Isogenies and endomorphisms	232
17.9	Further reading	237
17.10	Exercises	238
	<i>Bibliography</i>	240
	<i>Index</i>	246