Contents

	Preface	v
0	**Introduction**	1
0.1	Fascinating numbers	1
0.2	Well ordering	5
0.3	The division algorithm	7
0.4	Mathematical induction	10
0.5	The Fibonacci sequence	12
	Portrait and biography of Fibonacci	12
0.6	A method of proof (reductio ad absurdum)	15
0.7	A method of disproof (the counterexample)	16
0.8	Iff	18
1	**Divisibility**	19
1.1	Primes and composites	19
1.2	The sieve of Eratosthenes	22
1.3	The infinitude of primes	25
1.4	The fundamental theorem of arithmetic	29
	Portrait and biography of Hilbert	32
1.5	GCDs and LCMs	34
1.6	The Euclidean algorithm	37
1.7	Computing GCDs	40
1.8	Factorisation revisited	43
2	**More About Primes—A Historical Diversion**	47
2.1	A false dawn and two sorry tales	47
	Portrait and biography of Dickson	50
2.2	Formulae generating primes	51
	Portrait and biography of Dirichlet	53
2.3	Prime pairs and Goldbach's conjecture	56
2.4	A wider view of the primes. The prime number theorem	58
2.5	Bertrand's conjecture	67
	Biography of Mersenne	70
2.6	Mersenne's and Fermat's primes	70

3 Congruences 76

3.1 Basic properties 76
3.2 Fermat's little theorem 82
Portrait and biography of Fermat 83
3.3 Euler's ϕ function 88
3.4 Euler's theorem 95
3.5 Wilson's theorem 97

4 Congruences Involving Unknowns 102

4.1 Linear congruences 102
4.2 Congruences of higher degree 109
4.3 Quadratic congruences modulo a prime 115
Portrait and biography of Lagrange 117
4.4 Lagrange's theorem 118

5 Primitive Roots 123

5.1 A converse for the FLT 123
5.2 Primitive roots of primes. Order of an element 125
Biography of Legendre 126
5.3 Gauss's theorem 132
5.4 Some simple primality tests. Pseudoprimes. Carmichael numbers 136
5.5 Special repeating decimals 142

6 Diophantine Equations and Fermat's Last Theorem 146

6.1 Introduction 146
6.2 Pythagorean triples 148
6.3 Fermat's last theorem 153
6.4 History of the FC 155
Portrait and biography of Germain 158
6.5 Sophie Germain's theorem 159
6.6 Cadenza 161

7 Sums of Squares 163

7.1 Sums of two squares 163
Portrait and biography of Mordell 166
7.2 Sums of more than two squares 169
7.3 Diverging developments and a little history 174

8 Quadratic Reciprocity 179

8.1 Introduction 179
8.2 The law of quadratic reciprocity 179
Portrait and biography of Euler 180

8.3 Euler's criterion 185
8.4 Gauss's lemma and applications 188
8.5 Proof of the LQR—more applications 193
Portrait and biography of Jacobi 197
8.6 The Jacobi symbol 198
8.7 Programming points 200

9 The Gaussian Integers 202

9.1 Introduction 202
Portrait and biography of Gauss 203
9.2 Divisibility in the Gaussian integers 205
9.3 Computer manipulation of Gaussian integers 209
9.4 The fundamental theorem 212
9.5 Generalisation. Two problems of Fermat 214
9.6 Lucas's test 221

10 Arithmetic Functions 224

10.1 Introduction 224
10.2 Multiplicative arithmetic functions 229
Portrait and biography of Möbius 235
10.3 The Möbius function 235
10.4 Averaging—a smoothing process 240

11 Continued Fractions and Pell's Equation 249

11.1 Finite continued fractions 249
11.2 Infinite continued fractions 252
11.3 Computing continued fractions for irrational numbers 258
11.4 Approximating irrational numbers 261
11.5 iscfs for square roots and other quadratic irrationals 264
Biography of Pell 267
11.6 Pell's Equation 267
11.7 Two more applications 272

12 Sending Secret Messages 277

12.1 A cautionary tale 277
12.2 The Remedy: the RSA cipher system 279

Appendices I Multiprecision arithmetic 285
II Table of least prime factors of integers 293

Bibliography 299

Index 303

Index of Notation 310