
Contents

Preface	xiii
Gauss's <i>Disquisitiones Arithmeticae</i>	xix
Notation	xxi
The language of mathematics	xxii
Prerequisites	xxiii
Preliminary Chapter on Induction	1
0.1. Fibonacci numbers and other recurrence sequences	1
0.2. Formulas for sums of powers of integers	3
0.3. The binomial theorem, Pascal's triangle, and the binomial coefficients	4
Chapter 1. The Euclidean algorithm	11
1.1. Finding the gcd	11
1.2. Linear combinations	13
1.3. The set of linear combinations of two integers	15
1.4. The least common multiple	17
1.5. Continued fractions	17
1.6. Tiling a rectangle with squares	19
Appendix 1A. Reformulating the Euclidean algorithm	23
Chapter 2. Congruences	29
2.1. Basic congruences	29
2.2. The trouble with division	32
2.3. Congruences for polynomials	34
2.4. Tests for divisibility	34

Appendix 2A. Congruences in the language of groups	39
Chapter 3. The basic algebra of number theory	43
3.1. The Fundamental Theorem of Arithmetic	43
3.2. Abstractions	45
3.3. Divisors using factorizations	47
3.4. Irrationality	49
3.5. Dividing in congruences	50
3.6. Linear equations in two unknowns	52
3.7. Congruences to several moduli	54
3.8. Square roots of 1 (mod n)	56
Appendix 3A. Factoring binomial coefficients and Pascal's triangle modulo p	61
Chapter 4. Multiplicative functions	67
4.1. Euler's ϕ -function	68
4.2. Perfect numbers. " <i>The whole is equal to the sum of its parts.</i> "	69
Appendix 4A. More multiplicative functions	74
Chapter 5. The distribution of prime numbers	81
5.1. Proofs that there are infinitely many primes	81
5.2. Distinguishing primes	83
5.3. Primes in certain arithmetic progressions	85
5.4. How many primes are there up to x ?	86
5.5. Bounds on the number of primes	89
5.6. Gaps between primes	91
5.7. Formulas for primes	93
Appendix 5A. Bertrand's postulate and beyond	97
Bonus read: A review of prime problems	101
Prime values of polynomials in one variable	101
Prime values of polynomials in several variables	103
Goldbach's conjecture and variants	105
Chapter 6. Diophantine problems	109
6.1. The Pythagorean equation	109
6.2. No solutions to a Diophantine equation through descent	112
6.3. Fermat's "infinite descent"	114
6.4. Fermat's Last Theorem	115
Appendix 6A. Polynomial solutions of Diophantine equations	119

Chapter 7. Power residues	123
7.1. Generating the multiplicative group of residues	124
7.2. Fermat's Little Theorem	125
7.3. Special primes and orders	128
7.4. Further observations	128
7.5. The number of elements of a given order, and primitive roots	129
7.6. Testing for composites, pseudoprimes, and Carmichael numbers	133
7.7. Divisibility tests, again	134
7.8. The decimal expansion of fractions	134
7.9. Primes in arithmetic progressions, revisited	136
Appendix 7A. Card shuffling and Fermat's Little Theorem	140
Chapter 8. Quadratic residues	147
8.1. Squares modulo prime p	147
8.2. The quadratic character of a residue	149
8.3. The residue -1	152
8.4. The residue 2	153
8.5. The law of quadratic reciprocity	155
8.6. Proof of the law of quadratic reciprocity	157
8.7. The Jacobi symbol	159
8.8. The squares modulo m	161
Appendix 8A. Eisenstein's proof of quadratic reciprocity	167
Chapter 9. Quadratic equations	173
9.1. Sums of two squares	173
9.2. The values of $x^2 + dy^2$	176
9.3. Is there a solution to a given quadratic equation?	177
9.4. Representation of integers by $ax^2 + by^2$ with x, y rational, and beyond	180
9.5. The failure of the local-global principle for quadratic equations in integers	181
9.6. Primes represented by $x^2 + 5y^2$	181
Appendix 9A. Proof of the local-global principle for quadratic equations	184
Chapter 10. Square roots and factoring	189
10.1. Square roots modulo n	189
10.2. Cryptosystems	190
10.3. RSA	192
10.4. Certificates and the complexity classes P and NP	194

10.5. Polynomial time primality testing	196
10.6. Factoring methods	197
Appendix 10A. Pseudoprime tests using square roots of 1	200
Chapter 11. Rational approximations to real numbers	205
11.1. The pigeonhole principle	205
11.2. Pell's equation	208
11.3. Descent on solutions of $x^2 - dy^2 = n$, $d > 0$	212
11.4. Transcendental numbers	213
11.5. The <i>abc</i> -conjecture	216
Appendix 11A. Uniform distribution	220
Chapter 12. Binary quadratic forms	227
12.1. Representation of integers by binary quadratic forms	228
12.2. Equivalence classes of binary quadratic forms	230
12.3. Congruence restrictions on the values of a binary quadratic form	231
12.4. Class numbers	232
12.5. Class number one	233
Appendix 12A. Composition rules: Gauss, Dirichlet, and Bhargava	240
Hints for exercises	251
Recommended further reading	261
Index	263