

---

# Contents

Preface	xvii
Gauss's <i>Disquisitiones Arithmeticae</i>	xxiii
Notation	xxv
The language of mathematics	xxvi
Prerequisites	xxvii
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
Appendices for Preliminary Chapter on Induction	
0A. A closed formula for sums of powers	9
0B. Generating functions	11
0C. Finding roots of polynomials	15
0D. What is a group?	19
0E. Rings and fields	22
0F. Symmetric polynomials	25
0G. Constructibility	30
Chapter 1. The Euclidean algorithm	33
1.1. Finding the gcd	33
1.2. Linear combinations	35
1.3. The set of linear combinations of two integers	37
1.4. The least common multiple	39

---

1.5. Continued fractions	39
1.6. Tiling a rectangle with squares	41
Appendices for Chapter 1:	
1A. Reformulating the Euclidean algorithm	45
1B. Computational aspects of the Euclidean algorithm	51
1C. Magic squares	54
1D. The Frobenius postage stamp problem	57
1E. Egyptian fractions	59
Chapter 2. Congruences	61
2.1. Basic congruences	61
2.2. The trouble with division	64
2.3. Congruences for polynomials	66
2.4. Tests for divisibility	66
Appendices for Chapter 2:	
2A. Congruences in the language of groups	71
2B. The Euclidean algorithm for polynomials	75
Chapter 3. The basic algebra of number theory	81
3.1. The Fundamental Theorem of Arithmetic	81
3.2. Abstractions	83
3.3. Divisors using factorizations	85
3.4. Irrationality	87
3.5. Dividing in congruences	88
3.6. Linear equations in two unknowns	90
3.7. Congruences to several moduli	92
3.8. Square roots of 1 (mod $n$ )	94
Appendices for Chapter 3:	
3A. Factoring binomial coefficients and Pascal's triangle modulo $p$	99
3B. Solving linear congruences	104
3C. Groups and rings	109
3D. Unique factorization revisited	112
3E. Gauss's approach	116
3F. Fundamental theorems and factoring polynomials	117
3G. Open problems	123
Chapter 4. Multiplicative functions	127
4.1. Euler's $\phi$ -function	128
4.2. Perfect numbers. " <i>The whole is equal to the sum of its parts.</i> "	129

---

Appendices for Chapter 4:	
4A. More multiplicative functions	134
4B. Dirichlet series and multiplicative functions	140
4C. Irreducible polynomials modulo $p$	144
4D. The harmonic sum and the divisor function	147
4E. Cyclotomic polynomials	153
Chapter 5. The distribution of prime numbers	155
5.1. Proofs that there are infinitely many primes	155
5.2. Distinguishing primes	157
5.3. Primes in certain arithmetic progressions	159
5.4. How many primes are there up to $x$ ?	160
5.5. Bounds on the number of primes	163
5.6. Gaps between primes	165
5.7. Formulas for primes	167
Appendices for Chapter 5:	
5A. Bertrand's postulate and beyond	171
Bonus read: A review of prime problems	175
Prime values of polynomials in one variable	175
Prime values of polynomials in several variables	177
Goldbach's conjecture and variants	179
5B. An important proof of infinitely many primes	182
5C. What should be true about primes?	187
5D. Working with Riemann's zeta-function	192
5E. Prime patterns: Consequences of the Green-Tao Theorem	198
5F. A panoply of prime proofs	202
5G. Searching for primes and prime formulas	204
5H. Dynamical systems and infinitely many primes	208
Chapter 6. Diophantine problems	215
6.1. The Pythagorean equation	215
6.2. No solutions to a Diophantine equation through descent	218
6.3. Fermat's "infinite descent"	220
6.4. Fermat's Last Theorem	221
Appendices for Chapter 6:	
6A. Polynomial solutions of Diophantine equations	225
6B. No Pythagorean triangle of square area via Euclidean geometry	229
6C. Can a binomial coefficient be a square?	233

---

Chapter 7. Power residues	235
7.1. Generating the multiplicative group of residues	236
7.2. Fermat's Little Theorem	237
7.3. Special primes and orders	240
7.4. Further observations	240
7.5. The number of elements of a given order, and primitive roots	241
7.6. Testing for composites, pseudoprimes, and Carmichael numbers	245
7.7. Divisibility tests, again	246
7.8. The decimal expansion of fractions	246
7.9. Primes in arithmetic progressions, revisited	248
Appendices for Chapter 7:	
7A. Card shuffling and Fermat's Little Theorem	252
7B. Orders and primitive roots	258
7C. Finding $n$ th roots modulo prime powers	265
7D. Orders for finite groups	269
7E. Constructing finite fields	273
7F. Sophie Germain and Fermat's Last Theorem	278
7G. Primes of the form $2^n + k$	280
7H. Further congruences	284
7I. Primitive prime factors of recurrence sequences	290
Chapter 8. Quadratic residues	295
8.1. Squares modulo prime $p$	295
8.2. The quadratic character of a residue	297
8.3. The residue $-1$	300
8.4. The residue $2$	301
8.5. The law of quadratic reciprocity	303
8.6. Proof of the law of quadratic reciprocity	305
8.7. The Jacobi symbol	307
8.8. The squares modulo $m$	309
Appendices for Chapter 8:	
8A. Eisenstein's proof of quadratic reciprocity	315
8B. Small quadratic non-residues	319
8C. The first proof of quadratic reciprocity	323
8D. Dirichlet characters and primes in arithmetic progressions	326
8E. Quadratic reciprocity and recurrence sequences	333

---

Chapter 9. Quadratic equations	337
9.1. Sums of two squares	337
9.2. The values of $x^2 + dy^2$	340
9.3. Is there a solution to a given quadratic equation?	341
9.4. Representation of integers by $ax^2 + by^2$ with $x, y$ rational, and beyond	344
9.5. The failure of the local-global principle for quadratic equations in integers	345
9.6. Primes represented by $x^2 + 5y^2$	345
Appendices for Chapter 9:	
9A. Proof of the local-global principle for quadratic equations	348
9B. Reformulation of the local-global principle	353
9C. The number of representations	356
9D. Descent and the quadratics	360
Chapter 10. Square roots and factoring	365
10.1. Square roots modulo $n$	365
10.2. Cryptosystems	366
10.3. RSA	368
10.4. Certificates and the complexity classes P and NP	370
10.5. Polynomial time primality testing	372
10.6. Factoring methods	373
Appendices for Chapter 10:	
10A. Pseudoprime tests using square roots of 1	376
10B. Factoring with squares	380
10C. Identifying primes of a given size	383
10D. Carmichael numbers	387
10E. Cryptosystems based on discrete logarithms	391
10F. Running times of algorithms	393
10G. The AKS test	395
10H. Factoring algorithms for polynomials	399
Chapter 11. Rational approximations to real numbers	403
11.1. The pigeonhole principle	403
11.2. Pell's equation	406
11.3. Descent on solutions of $x^2 - dy^2 = n$ , $d > 0$	410
11.4. Transcendental numbers	411
11.5. The $abc$ -conjecture	414

---

Appendices for Chapter 11:	
11A. Uniform distribution	418
11B. Continued fractions	423
11C. Two-variable quadratic equations	438
11D. Transcendental numbers	439
Chapter 12. Binary quadratic forms	443
12.1. Representation of integers by binary quadratic forms	444
12.2. Equivalence classes of binary quadratic forms	446
12.3. Congruence restrictions on the values of a binary quadratic form	447
12.4. Class numbers	448
12.5. Class number one	449
Appendices for Chapter 12:	
12A. Composition rules: Gauss, Dirichlet, and Bhargava	456
12B. The class group	465
12C. Binary quadratic forms of positive discriminant	468
12D. Sums of three squares	471
12E. Sums of four squares	475
12F. Universality	479
12G. Integers represented in Apollonian circle packings	482
Chapter 13. The anatomy of integers	487
13.1. Rough estimates for the number of integers with a fixed number of prime factors	487
13.2. The number of prime factors of a typical integer	488
13.3. The multiplication table problem	491
13.4. Hardy and Ramanujan's inequality	492
Appendices for Chapter 13:	
13A. Other anatomies	493
13B. Dirichlet $L$ -functions	497
Chapter 14. Counting integral and rational points on curves, modulo $p$	501
14.1. Diagonal quadratics	501
14.2. Counting solutions to a quadratic equation and another proof of quadratic reciprocity	503
14.3. Cubic equations modulo $p$	504
14.4. The equation $E_b : y^2 = x^3 + b$	505
14.5. The equation $y^2 = x^3 + ax$	507
14.6. A more general viewpoint on counting solutions modulo $p$	509

---

Appendices for Chapter 14:	
14A. Gauss sums	511
Chapter 15. Combinatorial number theory	515
15.1. Partitions	515
15.2. Jacobi's triple product identity	517
15.3. The Freiman-Ruzsa Theorem	519
15.4. Expansion and the Plünnecke-Ruzsa inequality	522
15.5. Schnirel'man's Theorem	523
15.6. Classical additive number theory	525
15.7. Challenging problems	528
Appendices for Chapter 15:	
15A. Summing sets modulo $p$	530
15B. Summing sets of integers	532
Chapter 16. The $p$ -adic numbers	535
16.1. The $p$ -adic norm	535
16.2. $p$ -adic expansions	536
16.3. $p$ -adic roots of polynomials	537
16.4. $p$ -adic factors of a polynomial	539
16.5. Possible norms on the rationals	541
16.6. Power series convergence and the $p$ -adic logarithm	542
16.7. The $p$ -adic dilogarithm	545
Chapter 17. Rational points on elliptic curves	547
17.1. The group of rational points on an elliptic curve	548
17.2. Congruent number curves	551
17.3. No non-trivial rational points by descent	553
17.4. The group of rational points of $y^2 = x^3 - x$	553
17.5. Mordell's Theorem: $E_A(\mathbb{Q})$ is finitely generated	554
17.6. Some nice examples	558
Appendices for Chapter 17:	
17A. General Mordell's Theorem	561
17B. Pythagorean triangles of area 6	563
17C. 2-parts of abelian groups	565
17D. Waring's problem	566
Hints for exercises	569
Recommended further reading	583
Index	585