

Contents

Preface	v
Flowchart of Chapter Dependencies	ix
Introduction	1
1 What Is Number Theory?	6
2 Pythagorean Triples	13
3 Pythagorean Triples and the Unit Circle	21
4 Sums of Higher Powers and Fermat's Last Theorem	26
5 Divisibility and the Greatest Common Divisor	30
6 Linear Equations and the Greatest Common Divisor	37
7 Factorization and the Fundamental Theorem of Arithmetic	46
8 Congruences	55
9 Congruences, Powers, and Fermat's Little Theorem	65
10 Congruences, Powers, and Euler's Formula	71
11 Euler's Phi Function and the Chinese Remainder Theorem	75
12 Prime Numbers	83
13 Counting Primes	90
14 Mersenne Primes	96
15 Mersenne Primes and Perfect Numbers	101
16 Powers Modulo m and Successive Squaring	111
17 Computing k^{th} Roots Modulo m	118
18 Powers, Roots, and "Unbreakable" Codes	123
19 Primality Testing and Carmichael Numbers	129
20 Squares Modulo p	141
21 Is -1 a Square Modulo p ? Is 2 ?	148
22 Quadratic Reciprocity	159

23	Proof of Quadratic Reciprocity	171
24	Which Primes Are Sums of Two Squares?	181
25	Which Numbers Are Sums of Two Squares?	193
26	As Easy as One, Two, Three	199
27	Euler's Phi Function and Sums of Divisors	206
28	Powers Modulo p and Primitive Roots	211
29	Primitive Roots and Indices	224
30	The Equation $X^4 + Y^4 = Z^4$	231
31	Square-Triangular Numbers Revisited	236
32	Pell's Equation	245
33	Diophantine Approximation	251
34	Diophantine Approximation and Pell's Equation	260
35	Number Theory and Imaginary Numbers	267
36	The Gaussian Integers and Unique Factorization	281
37	Irrational Numbers and Transcendental Numbers	297
38	Binomial Coefficients and Pascal's Triangle	313
39	Fibonacci's Rabbits and Linear Recurrence Sequences	324
40	Oh, What a Beautiful Function	339
41	Cubic Curves and Elliptic Curves	353
42	Elliptic Curves with Few Rational Points	366
43	Points on Elliptic Curves Modulo p	373
44	Torsion Collections Modulo p and Bad Primes	384
45	Defect Bounds and Modularity Patterns	388
46	Elliptic Curves and Fermat's Last Theorem	394
	Further Reading	396
	Index	397
47	The Topsy-Turvy World of Continued Fractions [online]	410
48	Continued Fractions and Pell's Equation [online]	426
49	Generating Functions [online]	442
50	Sums of Powers [online]	452
A	Factorization of Small Composite Integers [online]	464
B	A List of Primes [online]	466