

CONTENTS

Preface	xi
New To This Edition	xiv
1 Some Preliminary Considerations	1
1.1 Mathematical Induction	1
1.2 The Binomial Theorem	8
1.3 Early Number Theory	12
2 Divisibility Theory in the Integers	17
2.1 The Division Algorithm	17
2.2 The Greatest Common Divisor	20
2.3 The Euclidean Algorithm	26
2.4 The Diophantine Equation $ax + by = c$	32
3 Primes and Their Distribution	40
3.1 The Fundamental Theorem of Arithmetic	40
3.2 The Sieve of Eratosthenes	45
3.3 The Goldbach Conjecture	51
4 The Theory of Congruences	62
4.1 Carl Friedrich Gauss	62
4.2 Basic Properties of Congruence	64
4.3 Special Divisibility Tests	70
4.4 Linear Congruences	75

5	Fermat's Theorem	84
5.1	Pierre de Fermat	84
5.2	Fermat's Factorization Method	86
5.3	The Little Theorem	91
5.4	Wilson's Theorem	98
6	Number-Theoretic Functions	102
6.1	The Functions τ and σ	102
6.2	The Möbius Inversion Formula	111
6.3	The Greatest Integer Function	116
6.4	An Application to the Calendar	121
7	Euler's Generalization of Fermat's Theorem	127
7.1	Leonhard Euler	127
7.2	Euler's Phi-Function	129
7.3	Euler's Theorem	134
7.4	Some Properties of the Phi-Function	139
7.5	An Application to Cryptography	144
8	Primitive Roots and Indices	157
8.1	The Order of an Integer Modulo n	157
8.2	Primitive Roots for Primes	162
8.3	Composite Numbers Having Primitive Roots	168
8.4	The Theory of Indices	173
9	The Quadratic Reciprocity Law	179
9.1	Euler's Criterion	179
9.2	The Legendre Symbol and Its Properties	185
9.3	Quadratic Reciprocity	195
9.4	Quadratic Congruences with Composite Moduli	202
10	Perfect Numbers	207
10.1	Marin Mersenne	207
10.2	The Search for Perfect Numbers	209
10.3	Mersenne Primes	215
10.4	Fermat Numbers	226
11	The Fermat Conjecture	234
11.1	Pythagorean Triples	234
11.2	The Famous "Last Theorem"	241
12	Representation of Integers as Sums of Squares	249
12.1	Joseph Louis Lagrange	249
12.2	Sums of Two Squares	251
12.3	Sums of More than Two Squares	260

13	Fibonacci Numbers	270
13.1	The Fibonacci Sequence	270
13.2	Certain Identities Involving Fibonacci Numbers	277
14	Continued Fractions	287
14.1	Srinivasa Ramanujan	287
14.2	Finite Continued Fractions	290
14.3	Infinite Continued Fractions	304
14.4	Pell's Equation	318
15	Some Twentieth-Century Developments	333
15.1	Hardy, Dickson, and Erdős	333
15.2	Primality Testing and Factorization	338
15.3	An Application to Factoring: Remote Coin Flipping	348
15.4	The Prime Number Theorem	352
	Miscellaneous Problems	360
	Appendixes	363
	General References	364
	Suggested Further Reading	367
	Tables	370
	Answers to Selected Problems	393
	Index	404