



ELEMENTARY NUMBER THEORY AND ITS APPLICATIONS

Third Edition

Kenneth H. Rosen

AT&T Bell Laboratories



ADDISON-WESLEY PUBLISHING COMPANY

Reading, Massachusetts • Menlo Park, California • New York
Don Mills, Ontario • Wokingham, England • Amsterdam • Bonn
Sydney • Singapore • Tokyo • Madrid • San Juan • Milan • Paris

Contents

	Introduction	1
Chapter 1.	The Integers	
1.1	Basic properties.....	4
1.2	Summations and products	9
1.3	Mathematical induction	15
1.4	Binomial coefficients	28
1.5	Divisibility	36
1.6	Representations of integers	42
1.7	Computer operations with integers	51
1.8	Complexity of integer operations	57
1.9	Prime numbers	64
Chapter 2.	Greatest Common Divisors and Prime Factorization	
2.1	Greatest common divisors	74
2.2	The Euclidean algorithm	80
2.3	The fundamental theorem of arithmetic	90
2.4	Fermat numbers and factorization methods	103
2.5	Linear diophantine equations	112
Chapter 3.	Congruences	
3.1	Introduction to congruences	119
3.2	Linear congruences	131
3.3	The Chinese remainder theorem.....	135
3.4	Systems of linear congruences	145
3.5	Factoring using the Pollard rho method	156
Chapter 4.	Applications of Congruences	
4.1	Divisibility tests	160
4.2	The perpetual calendar	166
4.3	Round-robin tournaments.....	171
4.4	Computer file storage and hashing functions.....	173
4.5	Check digits	178

Chapter 5. Some Special Congruences

5.1	Wilson's theorem and Fermat's little theorem	185
5.2	Pseudoprimes	192
5.3	Euler's theorem	201

Chapter 6. Multiplicative Functions

6.1	Euler's phi-function	207
6.2	The sum and number of divisors	217
6.3	Perfect numbers and Mersenne primes	223

Chapter 7. Cryptology

7.1	Character ciphers	234
7.2	Block ciphers	245
7.3	Exponentiation ciphers	253
7.4	Public-key cryptography	259
7.5	Knapsack ciphers	266
7.6	Some applications to computer science	274

Chapter 8. Primitive Roots

8.1	The order of an integer and primitive roots	278
8.2	Primitive roots for primes	285
8.3	Existence of primitive roots	290
8.4	Index arithmetic	298
8.5	Primality testing using primitive roots	308
8.6	Universal exponents	312
8.7	Pseudo-random numbers	318
8.8	An application to the splicing of telephone cables	324

Chapter 9. Quadratic Residues and Reciprocity

9.1	Quadratic residues and nonresidues	331
9.2	Quadratic reciprocity	348
9.3	The Jacobi symbol	357
9.4	Euler pseudoprimes	367
9.5	Zero-knowledge proofs	377

Chapter 10. Decimal Fractions and Continued Fractions

10.1	Decimal fractions	384
10.2	Finite continued fractions	394
10.3	Infinite continued fractions.....	405
10.4	Periodic continued fractions	417
10.5	Factoring using continued fractions	432

Chapter 11. Some Nonlinear Diophantine Equations

11.1	Pythagorean triples.....	436
11.2	Fermat's last theorem	442
11.3	Sums of squares	447
11.4	Pell's equation.....	457

Appendix.....	465
Answers to odd-numbered exercises.....	481
Bibliography.....	527
Index	537