
Contents

	Introduction	1
Chapter 1.	The Integers	
1.1	The well-ordering property	4
1.2	Divisibility	18
1.3	Representations of integers	24
1.4	Computer operations with integers	33
1.5	Prime numbers	45
Chapter 2.	Greatest Common Divisors and Prime Factorization	
2.1	Greatest common divisors	53
2.2	The Euclidean algorithm	58
2.3	The fundamental theorem of arithmetic	69
2.4	Factorization of integers and the Fermat numbers	79
2.5	Linear diophantine equations	87
Chapter 3.	Congruences	
3.1	Introduction to congruences	91
3.2	Linear congruences	102
3.3	The Chinese remainder theorem	107
3.4	Systems of linear congruences	116
Chapter 4.	Applications of Congruences	
4.1	Divisibility tests	129
4.2	The perpetual calendar	134
4.3	Round-robin tournaments	139
4.4	Computer file storage and hashing functions	141

Chapter 5. Some Special Congruences

5.1	Wilson's theorem and Fermat's little theorem	147
5.2	Pseudoprimes.....	152
5.3	Euler's theorem.....	161

Chapter 6. Multiplicative Functions

6.1	Euler's phi-function	166
6.2	The sum and number of divisors.....	174
6.3	Perfect numbers and Mersenne primes	180

Chapter 7. Cryptology

7.1	Character ciphers	188
7.2	Block ciphers.....	198
7.3	Exponentiation ciphers	205
7.4	Public-key cryptography	212
7.5	Knapsack ciphers	219
7.6	Some applications to computer science	227

Chapter 8. Primitive Roots

8.1	The order of an integer and primitive roots.....	232
8.2	Primitive roots for primes	238
8.3	Existence of primitive roots	243
8.4	Index arithmetic	252
8.5	Primality testing using primitive roots.....	263
8.6	Universal exponents.....	268
8.7	Pseudo-random numbers.....	275
8.8	The splicing of telephone cables.....	280

Chapter 9. Quadratic Residues and Reciprocity

9.1	Quadratic residues.....	288
9.2	Quadratic reciprocity	304
9.3	The Jacobi symbol.....	314
9.4	Euler pseudoprimes	325

Chapter 10. Decimal Fractions and Continued Fractions

10.1	Decimal fractions.....	336
10.2	Finite continued fractions.....	350
10.3	Infinite continued fractions.....	361
10.4	Periodic continued fractions	375

Chapter 11. Some Nonlinear Diophantine Equations

11.1	Pythagorean triples.....	391
11.2	Fermat's last theorem	397
11.3	Pell's equations	401

Appendix	410
Answers to selected problems	426
Bibliography	438
List of symbols	445
Index	447