

Contents

	PREFACE	v
0.	BACKGROUND: PRIME NUMBERS	1
	1. Prime Numbers	2
	2. The Sieve of Eratosthenes	4
	3. The Distribution of Primes	5
	4. Largest Known Primes	8
	5. Conjectures About Primes	9
	Exercises 0	11
	Computer Problems 0	12
1.	BASIC CONCEPTS	14
	1. Mathematical Induction	14
	2. Divisibility. The Euclidean Algorithm	23
	3. Efficiency of Algorithms. Multiprecision Arithmetic	34
	4. The Fibonacci Sequence and the Efficiency of the Euclidean Algorithm	43
	5. Prime Numbers	48

6.	Diophantine Equations	51
	Exercises I	55
	Computer Problems I	59
II.	CONGRUENCES	62
	1. Congruence	62
	2. Modular Arithmetic	77
	3. Fermat's Little Theorem and the Euler Phi-Function	94
	4. Random Number Generators and Primitive Roots	107
	Exercises II	128
	Computer Problems II	135
III.	PRIMALITY TESTING AND FACTORISATION	138
	1. Perfect Numbers and Mersenne Primes	139
	2. Public Key Cryptography	153
	3. Primality Testing	163
	4. Factorisation Techniques	178
	Exercises III	191
	Computer Problems III	197
	RECOMMENDED FURTHER READING	202
	INDEX OF NOTATION	203
	INDEX	204