CAMBRIDGE

Cambridge University Press
978-0-521-40988-9 - Primes and Programming: An Introduction to Number Theory with Computing
Peter Giblin
Table of Contents
More information

Contents

Preface vii

Logical dependence of chapters xi

1. The Fundamental Theorem, Greatest Common Divisors and Least Common Multiples 1

1. Primes and the fundamental theorem 1
2. Greatest common divisor and least common multiple 7
3. Euclid's algorithm for the gcd 12
4. $[x]$ and applications 24
5*. Further projects 29

2. Listing Primes 37

1. Primes by division 37
2. Primes by multiplication (elimination of composites) 50
3. Approximations to $\pi(x)$ 52
4. The sieve of Eratosthenes 55

3. Congruences 69

1. Congruences: basic properties 69
2. Inverses mod m and solutions of certain congruences 74
3. Further examples of congruences 81

4. Powers and Pseudoprimes 86

1. Fermat's (little) theorem 86
2. The power algorithm 89
3. Head's algorithm for multiplication mod m 93

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-40988-9 - Primes and Programming: An Introduction to Number Theory with Computing
Peter Giblin
Table of Contents
More information

4. Pseudoprimes 98
5. Wilson's theorem 102

5. Miller's Test and Strong Pseudoprimes 104
1. Miller's test 104
2. Probabilistic primality testing 109

6. Euler's Theorem, Orders and Primality Testing 112
1. Euler's function (the ϕ-function or totient function) 112
2. Euler's theorem and the concept of order 119
3. Primality tests 124
4. Periods of decimals 130

7. Cryptography 133
1. Exponentiation ciphers 134
2. Public key cryptography: RSA ciphers 136
3. Coin-tossing by telephone 145

8. Primitive Roots 147
1. Properties and applications of primitive roots 147
2. Existence and nonexistence of primitive roots 149

9. The Number of Divisors d and the Sum of Divisors σ 158
1. The function $d(n)$ 158
2. Multiplicative functions and the sum function $\sigma(n)$ 162
3. Tests for primality of the Mersenne numbers $2^m - 1$ 170

10. Continued Fractions and Factoring 174
1. Continued fractions: initial ideas and definitions 175
2. The continued fraction for $\sqrt{n}$ 180
3. Proofs of some properties of continued fractions 186
4. Pell's equation 189
5. The continued fraction factoring method 191

11. Quadratic Residues 200
1. Definitions and examples 200
2. The quadratic character of 2 203
3. Quadratic reciprocity 206
4. The Jacobi symbol and a program for finding $\left(\frac{n}{p}\right)$ 211
5. Solving the equation $x^2 \equiv a \pmod{p}$: quadratic congruences 217

Bibliography 225

Index 231

Index of Listed Programs 236

Index of Notation 237

© Cambridge University Press www.cambridge.org