

A Course in Computational Number Theory

David Bressoud
Macalester College

Stan Wagon
Macalester College



CD-ROM
Included



Key College Publishing
Innovators in Higher Education

www.keycollege.com

in cooperation with



Springer

Contents

Preface	v
Notation	xi
 Chapter 1. Fundamentals	 1
1.0 Introduction.....	1
1.1 A Famous Sequence of Numbers.....	2
1.2 The Euclidean Algorithm.....	6
The Oldest Algorithm	
Reversing the Euclidean Algorithm	
The Extended GCD Algorithm	
The Fundamental Theorem of Arithmetic	
Two Applications	
1.3 Modular Arithmetic.....	25
1.4 Fast Powers.....	30
A Fast Algorithm for Exponentiation	
Powers of Matrices, Big-O Notation	
 Chapter 2. Congruences, Equations, and Powers	 41
2.0 Introduction.....	41
2.1 Solving Linear Congruences.....	41
Linear Diophantine Equations in Two Variables	
Linear Equations in Several Variables	
Linear Congruences	
The Conductor	
An Important Quadratic Congruence	
2.2 The Chinese Remainder Theorem.....	49

2.3 PowerMod Patterns.....	55
Fermat's Little Theorem	
More Patterns in Powers	
2.4 Pseudoprimes.....	59
Using the Pseudoprime Test	
Chapter 3. Euler's ϕ Function	65
3.0 Introduction.....	65
3.1 Euler's ϕ Function.....	65
3.2 Perfect Numbers and Their Relatives	72
The Sum of Divisors Function	
Perfect Numbers	
Amicable, Abundant, and Deficient Numbers	
3.3 Euler's Theorem.....	81
3.4 Primitive Roots for Primes.....	84
The Order of an Integer	
Primes Have Primitive Roots	
Repeating Decimals	
3.5 Primitive Roots for Composites.....	90
3.6 The Universal Exponent.....	93
Universal Exponents	
Power Towers	
The Form of Carmichael Numbers	
Chapter 4. Prime Numbers	99
4.0 Introduction.....	99
4.1 The Number of Primes.....	100
We'll Never Run Out of Primes	
The Sieve of Eratosthenes	
Chebyshev's Theorem and Bertrand's Postulate	
4.2 Prime Testing and Certification.....	114
Strong Pseudoprimes	
Industrial-Grade Primes	
Prime Certification Via Primitive Roots	
An Improvement	
Pratt Certificates	
4.3 Refinements and Other Directions.....	131
Other Primality Tests	
Strong Liars Are Scarce	
Finding the n th Prime	
4.4 A Dozen Prime Mysteries.....	141

Chapter 5. Some Applications	145
5.0 Introduction.....	145
5.1 Coding Secrets.....	145
Tossing a Coin into a Well	
The RSA Cryptosystem	
Digital Signatures	
5.2 The Yao Millionaire Problem.....	155
5.3 Check Digits.....	158
Basic Check Digit Schemes	
A Perfect Check Digit Method	
Beyond Perfection: Correcting Errors	
5.4 Factoring Algorithms.....	167
Trial Division	
Fermat's Algorithm	
Pollard Rho	
Pollard $p-1$	
The Current Scene	
 Chapter 6. Quadratic Residues	 179
6.0 Introduction.....	179
6.1 Pépin's Test.....	179
Quadratic Residues	
Pépin's Test	
Primes Congruent to 1 (Mod 4)	
6.2 Proof of Quadratic Reciprocity.....	185
Gauss's Lemma	
Proof of Quadratic Reciprocity	
Jacobi's Extension	
An Application to Factoring	
6.3 Quadratic Equations.....	194
 Chapter 7. Continued Fractions	 201
7.0 Introduction.....	201
7.1 Finite Continued Fractions.....	202
7.2 Infinite Continued Fractions.....	207
7.3 Periodic Continued Fractions.....	213
7.4 Pell's Equation.....	227
7.5 Archimedes and the Sun God's Cattle.....	232
Wurm's Version: Using Rectangular Bulls	
The Real Cattle Problem	
7.6 Factoring via Continued Fractions.....	238

Chapter 8. Prime Testing with Lucas Sequences	247
8.0 Introduction	247
8.1 Divisibility Properties of Lucas Sequences	248
8.2 Prime Tests Using Lucas Sequences	259
Lucas Certification	
The Lucas-Lehmer Algorithm Explained	
Lucas Pseudoprimes	
Strong Quadratic Pseudoprimes	
Primality Testing's Holy Grail	
Chapter 9. Prime Imaginaries and Imaginary Primes	279
9.0 Introduction	279
9.1 Sums of Two Squares	279
Primes	
The General Problem	
How Many Ways	
Number Theory and Salt	
9.2 The Gaussian Integers	302
Complex Number Theory	
Gaussian Primes	
The Moat Problem	
The Gaussian Zoo	
9.3 Higher Reciprocity	325
Appendix A. Mathematica Basics	333
A.0 Introduction	333
A.1 Plotting	335
A.2 Typesetting	338
Sending Files By E-Mail	
A.3 Types of Functions	341
A.4 Lists	343
A.5 Programs	345
A.6 Solving Equations	347
A.7 Symbolic Algebra	349
Appendix B. Lucas Certificates Exist	351
References	355
Index of Mathematica Objects	359
Subject Index	363