
Contents

Preface	ix
Exercise	xiv
Chapter 1. Why Factor Integers?	1
Introduction	1
§1.1. Public-Key Cryptography	2
§1.2. Repunits	5
§1.3. Repeating Decimal Fractions	6
§1.4. Perfect Numbers	8
§1.5. The Cunningham Project	9
Exercises	12
Chapter 2. Number Theory Review	13
Introduction	13
§2.1. Divisibility	17
§2.2. Prime Numbers	20
§2.3. Congruences	24
§2.4. Fermat and Euler	28
§2.5. Arithmetic Functions	33

§2.6. Quadratic Congruences	36
Exercises	39
Chapter 3. Number Theory Relevant to Factoring	41
Introduction	41
§3.1. Smooth Numbers	42
§3.2. Finding Modular Square Roots	44
§3.3. Cyclotomic Polynomials	47
§3.4. Divisibility Sequences and $b^m - 1$	49
§3.5. Factors of $b^m + 1$	55
§3.6. Factors of Fibonacci and Lucas Numbers	56
§3.7. Primality Testing	59
Exercises	71
Chapter 4. How Are Factors Used?	75
Introduction	75
§4.1. Aurifeuillian Factorizations	76
§4.2. Perfect Numbers	83
§4.3. Harmonic Numbers	88
§4.4. Prime Proving	91
§4.5. Linear Feedback Shift Registers	93
§4.6. Testing Conjectures	97
§4.7. Bernoulli Numbers	101
§4.8. Cryptographic Applications	104
§4.9. Other Applications	113
Exercises	116
Chapter 5. Simple Factoring Algorithms	119
Introduction	119
§5.1. Trial Division	120
§5.2. Fermat's Difference of Squares Method	123
§5.3. Hart's One-Line Factoring Algorithm	127
§5.4. Lehman's Variation of Fermat	128

Contents	vii
§5.5. The Lehmers' Factoring Method	132
§5.6. Pollard's Rho Method	135
§5.7. Pollard's $p - 1$ Method	138
Exercises	141
Chapter 6. Continued Fractions	143
Introduction	143
§6.1. Basic Facts about Continued Fractions	144
§6.2. McKee's Variation of Fermat	147
§6.3. Periodic Continued Fractions	149
§6.4. A General Plan for Factoring	153
§6.5. Lehmer and Powers	155
§6.6. Continued Fraction Factoring Algorithm	158
§6.7. SQUFOF—SQUare FOrms Factoring	163
§6.8. Pell's Equation	169
Exercises	170
Chapter 7. Elliptic Curves	173
Introduction	173
§7.1. Basic Properties of Elliptic Curves	174
§7.2. Factoring with Elliptic Curves	181
§7.3. Primality Proving with Elliptic Curves	187
§7.4. Applications of Factoring to Elliptic Curves	188
Exercises	190
Chapter 8. Sieve Algorithms	191
Introduction	191
§8.1. The Basic Sieve	192
§8.2. The Quadratic Sieve	195
§8.3. The Double Sieve	202
§8.4. Schroeppe's Linear Sieve	205
§8.5. The Number Field Sieve	207
Exercises	217

Chapter 9. Factoring Devices	219
Introduction	219
§9.1. Sieve Devices	219
§9.2. Special Computers	230
Exercise	237
Chapter 10. Theoretical and Practical Factoring	239
Introduction	239
§10.1. Theoretical Factoring	240
§10.2. Multiprecise Arithmetic	244
§10.3. Factoring—There’s an App for That	246
§10.4. Dirty Tricks	248
§10.5. Dirty Tricks with Lattices	253
§10.6. The Future of Factoring	262
Exercises	267
Appendix. Answers and Hints for Exercises	269
Introduction	269
§A.1. Chapter 1	269
§A.2. Chapter 2	270
§A.3. Chapter 3	270
§A.4. Chapter 4	271
§A.5. Chapter 5	271
§A.6. Chapter 6	271
§A.7. Chapter 7	272
§A.8. Chapter 8	272
§A.9. Chapter 10	272
Bibliography	273
Index	287