

CONTENTS

Chapter 1. The Number of Primes Below a Given Limit

| | |
|---|----|
| What Is a Prime Number? | 1 |
| The Fundamental Theorem of Arithmetic | 2 |
| Which Numbers Are Primes? The Sieve of Eratosthenes | 2 |
| General Remarks Concerning Computer Programs | 4 |
| A Sieve Program | 5 |
| Compact Prime Tables | 7 |
| Hexadecimal Compact Prime Tables | 9 |
| Difference Between Consecutive Primes | 9 |
| The Number of Primes Below x | 10 |
| Meissel's Formula | 12 |
| Evaluation of $P_k(x, a)$ | 12 |
| Lehmer's Formula | 13 |
| Computations | 14 |
| A Computation Using Meissel's Formula | 18 |
| A Computation Using Lehmer's Formula | 20 |
| A Computer Program Using Lehmer's Formula | 22 |
| Mapes' Method | 23 |
| Deduction of Formulas | 24 |
| A Worked Example | 26 |
| Mapes' Algorithm | 30 |
| Programming Mapes' Algorithm | 32 |
| Recent Developments | 33 |
| Results | 34 |
| Computational Complexity | 35 |
| Comparison Between the Methods Discussed | 35 |
| Bibliography | 36 |

Chapter 2. The Primes Viewed at Large

| | |
|---|----|
| Introduction | 37 |
| No Polynomial Can Produce Only Primes | 37 |
| Formulas Yielding All Primes | 39 |
| The Distribution of Primes Viewed at Large. Euclid's Theorem | 40 |
| The Formulas of Gauss and Legendre for $\pi(x)$. The Prime Number Theorem | 41 |
| The Chebyshev Function $\theta(x)$ | 44 |
| The Riemann Zeta-function | 44 |

CONTENTS

| | |
|---|----|
| The Zeros of the Zeta-function | 47 |
| Conversion From $f(x)$ Back to $\pi(x)$ | 49 |
| The Riemann Prime Number Formula | 50 |
| The Sign of $\text{li } x - \pi(x)$ | 52 |
| The Influence of the Complex Zeros of $\zeta(s)$ on $\pi(x)$ | 53 |
| The Remainder Term in the Prime Number Theorem | 56 |
| Effective Inequalities for $\pi(x)$, p_n , and $\theta(x)$ | 56 |
| The Number of Primes in Arithmetic Progressions | 57 |
| Bibliography | 58 |

Chapter 3. Subtleties in the Distribution of Primes

| | |
|---|----|
| The Distribution of Primes in Short Intervals | 60 |
| Twins and Some Other Constellations of Primes | 60 |
| Admissible Constellations of Primes | 62 |
| The Hardy–Littlewood Constants | 64 |
| The Prime k -Tuples Conjecture | 66 |
| Theoretical Evidence in Favour of the Prime k -Tuples Conjecture | 67 |
| Numerical Evidence in Favour of the Prime k -Tuples Conjecture | 68 |
| The Second Hardy–Littlewood Conjecture | 68 |
| The Midpoint Sieve | 70 |
| Modification of the Midpoint Sieve | 70 |
| Construction of Superdense Admissible Constellations | 71 |
| Some Dense Clusters of Primes | 73 |
| The Distribution of Primes Between the Two Series $4n + 1$ and $4n + 3$ | 73 |
| Graph of the Function $\pi_{4,3}(x) - \pi_{4,1}(x)$ | 74 |
| The Negative Regions | 74 |
| The Negative Blocks | 77 |
| Large Gaps Between Consecutive Primes | 78 |
| The Cramér Conjecture | 79 |
| Bibliography | 82 |

Chapter 4. The Recognition of Primes

| | |
|---|----|
| Introduction | 84 |
| Tests of Primality and of Compositeness | 84 |
| Factorization Methods as Tests of Compositeness | 85 |
| Fermat's Theorem as Compositeness Test | 85 |
| Fermat's Theorem as Primality Test | 85 |
| Pseudoprimes and Probable Primes | 86 |
| A Computer Program for Fermat's Test | 87 |
| The Labor Involved in a Fermat Test | 88 |
| Carmichael Numbers | 89 |
| Euler Pseudoprimes | 90 |
| Strong Pseudoprimes and a Primality Test | 91 |
| A Computer Program for Strong Pseudoprime Tests | 93 |
| Counts of Pseudoprimes and Carmichael Numbers | 94 |

CONTENTS

| | |
|---|-----|
| Rigorous Primality Proofs | 95 |
| Lehmer's Converse of Fermat's Theorem | 96 |
| Formal Proof of Theorem 4.3 | 97 |
| Ad Hoc Search for a Primitive Root | 98 |
| The Use of Several Bases | 99 |
| Fermat Numbers and Pepin's Theorem | 100 |
| Cofactors of Fermat Numbers | 102 |
| Generalized Fermat Numbers | 102 |
| A Relaxed Converse of Fermat's Theorem | 103 |
| Proth's Theorem | 104 |
| Tests of Compositeness for Numbers of the form $N = h \cdot 2^n \pm k$ | 105 |
| An Alternative Approach | 105 |
| Certificates of Primality | 106 |
| Primality Tests of Lucasian Type | 107 |
| Lucas Sequences | 107 |
| The Fibonacci Numbers | 108 |
| Large Subscripts | 108 |
| An Alternative Deduction | 111 |
| Divisibility Properties of the Numbers U_n | 112 |
| Primality Proofs by Aid of Lucas Sequences | 115 |
| Lucas Tests for Mersenne Numbers | 117 |
| A Relaxation of Theorem 4.8 | 120 |
| Pocklington's Theorem | 121 |
| Lehmer-Pocklington's Theorem | 122 |
| Pocklington-Type Theorems for Lucas Sequences | 123 |
| Primality Tests for Integers of the form $N = h \cdot 2^n - 1$, when $3 \nmid h$ | 124 |
| Primality Tests for $N = h \cdot 2^n - 1$, when $3 \mid h$ | 125 |
| The Combined $N - 1$ and $N + 1$ Test | 129 |
| Lucas Pseudoprimes | 130 |
| Modern Primality Proofs | 130 |
| The Jacobi Sum Primality Test | 131 |
| Three Lemmas | 132 |
| Lenstra's Theorem | 134 |
| The Sets P and Q | 135 |
| Running Time for the APRCL Test | 136 |
| Elliptic Curve Primality Proving, ECPP | 136 |
| The Goldwasser-Kilian Test | 137 |
| Atkin's Test | 138 |
| Bibliography | 139 |

Chapter 5. Classical Methods of Factorization

| | |
|---|-----|
| Introduction | 141 |
| When Do We Attempt Factorization? | 141 |
| Trial Division | 141 |
| A Computer Implementation of Trial Division | 143 |
| Euclid's Algorithm as an Aid to Factorization | 145 |

CONTENTS

| | |
|---|-----|
| Fermat's Factoring Method | 147 |
| Legendre's Congruence | 149 |
| Euler's Factoring Method | 151 |
| Gauss' Factoring Method | 152 |
| Legendre's Factoring Method | 155 |
| The Number of Prime Factors of Large Numbers | 156 |
| How Does a Typical Factorization Look? | 157 |
| The Erdős-Kac Theorem | 158 |
| The Distribution of Prime Factors of Various Sizes | 159 |
| Dickman's Version of Theorem 5.4 | 161 |
| A More Detailed Theory | 161 |
| The Size of the k th Largest Prime Factor of N | 162 |
| Smooth Integers | 164 |
| Searching for Factors of Certain Forms | 165 |
| Legendre's Theorem for the Factors of $N = a^n \pm b^n$ | 165 |
| Adaptation to Search for Factors of the Form $p = 2kn + 1$ | 169 |
| Adaptation of Trial Division | 169 |
| Adaptation of Fermat's Factoring Method | 170 |
| Adaptation of Euclid's Algorithm as an Aid to Factorization | 171 |
| Bibliography | 171 |
| Chapter 6. Modern Factorization Methods | |
| Introduction | 173 |
| Choice of Method | 173 |
| Pollard's $(p - 1)$ -Method | 174 |
| Phase 2 of the $(p - 1)$ -Method | 176 |
| The $(p + 1)$ -Method | 177 |
| Pollard's rho Method | 177 |
| A Computer Program for Pollard's rho Method | 180 |
| An Algebraic Description of Pollard's rho Method | 182 |
| Brent's Modification of Pollard's rho Method | 183 |
| The Pollard-Brent Method for $p = 2kn + 1$ | 185 |
| Shanks' Factoring Method SQUFOF | 186 |
| A Computer Program for SQUFOF | 190 |
| Comparison Between Pollard's rho Method and SQUFOF | 193 |
| Morrison and Brillhart's Continued Fraction Method CFRAC | 193 |
| The Factor Base | 194 |
| An Example of a Factorization with CFRAC | 196 |
| Further Details of CFRAC | 200 |
| The Early Abort Strategy | 202 |
| Results Achieved with CFRAC | 203 |
| Running Time Analysis of CFRAC | 204 |
| The Quadratic Sieve, QS | 204 |
| Smallest Solutions to $Q(x) \equiv 0 \pmod{p}$ | 205 |
| Special Factors | 206 |
| Results Achieved with QS | 206 |

CONTENTS

| | |
|---|-----|
| The Multiple Polynomial Quadratic Sieve, MPQS | 207 |
| Results Achieved with MPQS | 207 |
| Running Time Analysis of QS and MPQS | 208 |
| The Schnorr–Lenstra Method | 209 |
| Two Categories of Factorization Methods | 209 |
| Lenstra’s Elliptic Curve Method, ECM | 210 |
| Phase 2 of ECM | 210 |
| The Choice of A , B , and P_1 | 212 |
| Running Times of ECM | 212 |
| Recent Results Achieved with ECM | 214 |
| The Number Field Sieve, NFS | 214 |
| Factoring Both in \mathbb{Z} and in $\mathbb{Z}(z)$ | 215 |
| A Numerical Example | 215 |
| The General Number Field Sieve, GNFS | 216 |
| Running Times of NFS and GNFS | 217 |
| Results Achieved with NFS. Factorization of F_9 | 218 |
| Strategies in Factoring | 219 |
| How Fast Can a Factorization Algorithm Be? | 221 |
| Bibliography | 224 |
| Chapter 7. Prime Numbers and Cryptography | |
| Practical Secrecy | 226 |
| Keys in Cryptography | 226 |
| Arithmetical Formulation | 228 |
| RSA Cryptosystems | 228 |
| How to Find the Recovery Exponent | 229 |
| A Worked Example | 230 |
| Selecting Keys | 233 |
| Finding Suitable Primes | 234 |
| The Fixed Points of an RSA System | 235 |
| How Safe is an RSA Cryptosystem? | 236 |
| Superior Factorization | 237 |
| Bibliography | 237 |
| Appendix 1. Basic Concepts in Higher Algebra | |
| Introduction | 239 |
| Modules | 239 |
| Euclid’s Algorithm | 240 |
| The Labor Involved in Euclid’s Algorithm | 242 |
| A Definition Taken from the Theory of Algorithms | 242 |
| A Computer Program for Euclid’s Algorithm | 243 |
| Reducing the Labor | 244 |
| Binary Form of Euclid’s Algorithm | 244 |
| The Diophantine Equation $ax + by = c$ | 246 |
| Groups | 246 |

CONTENTS

| | |
|--|-----|
| Lagrange's Theorem. Cosets | 248 |
| Abstract Groups. Isomorphic Groups | 250 |
| The Direct Product of Two Given Groups | 251 |
| Cyclic Groups | 252 |
| Rings | 252 |
| Zero Divisors | 253 |
| Fields | 255 |
| Mappings. Isomorphisms and Homomorphisms | 257 |
| Group Characters | 258 |
| The Conjugate or Inverse Character | 259 |
| Homomorphisms and Group Characters | 260 |
| Bibliography | 260 |
| Appendix 2. Basic Concepts in Higher Arithmetic | |
| Divisors. Common Divisors | 261 |
| The Fundamental Theorem of Arithmetic | 261 |
| Congruences | 262 |
| Linear Congruences | 264 |
| Linear Congruences and Euclid's Algorithm | 265 |
| Systems of Linear Congruences | 266 |
| The Residue Classes mod p Constitute a Field | 267 |
| The Primitive Residue Classes mod p | 268 |
| The Structure of the Group M_n | 270 |
| Homomorphisms of M_q when q is a Prime | 272 |
| Carmichael's Function | 273 |
| Carmichael's Theorem | 274 |
| Bibliography | 275 |
| Appendix 3. Quadratic Residues | |
| Legendre's Symbol | 276 |
| Arithmetic Rules for Residues and Non-Residues | 276 |
| Euler's Criterion for the Computation of (a/p) | 278 |
| The Law of Quadratic Reciprocity | 279 |
| Jacobi's Symbol | 281 |
| A PASCAL Function for Computing (a/n) | 283 |
| The Quadratic Congruence $x^2 \equiv c \pmod{p}$ | 284 |
| The Case $p = 4k + 1$ | 284 |
| Bibliography | 285 |
| Appendix 4. The Arithmetic of Quadratic Fields | |
| Integers of $\mathbf{Q}(\sqrt{D})$ | 286 |
| Units of $\mathbf{Q}(\sqrt{D})$ | 289 |
| Associated Numbers in $\mathbf{Q}(\sqrt{D})$ | 290 |
| Divisibility in $\mathbf{Q}(\sqrt{D})$ | 290 |

CONTENTS

| | |
|---|-----|
| Fermat's Theorem in $\mathbf{Q}(\sqrt{D})$ | 291 |
| Primes in $\mathbf{Q}(\sqrt{D})$ | 293 |
| Factorization of Integers in $\mathbf{Q}(\sqrt{D})$ | 295 |
| Bibliography | 296 |

Appendix 5. Higher Algebraic Number Fields

| | |
|--|-----|
| Introduction | 297 |
| Algebraic Numbers | 297 |
| Numbers in $\mathbf{Q}(z)$. The Ring $\mathbf{Z}(z)$ of Integers in $\mathbf{Q}(z)$ | 298 |
| The Norm in $\mathbf{Q}(z)$. Units of $\mathbf{Q}(z)$ | 298 |
| Divisibility and Primes in $\mathbf{Z}(z)$ | 299 |
| The Field $\mathbf{Q}(\sqrt[3]{-2})$ and the Ring $\mathbf{Z}(\sqrt[3]{-2})$ | 299 |
| Primes in $\mathbf{Z}(\sqrt[3]{-2})$ | 300 |
| Bibliography | 303 |

Appendix 6. Algebraic Factors

| | |
|--|-----|
| Introduction | 304 |
| Factorization of Polynomials | 304 |
| The Cyclotomic Polynomials | 305 |
| The Polynomial $x^n + y^n$ | 308 |
| The Polynomial $x^n + ay^n$ | 308 |
| Aurifeuillian Factorizations | 309 |
| Factorization Formulas | 310 |
| The Algebraic Structure of Aurifeuillian Numbers | 314 |
| A formula by Gauss for $x^n - y^n$ | 315 |
| Bibliography | 316 |

Appendix 7. Elliptic Curves

| | |
|--|-----|
| Cubics | 317 |
| Rational Points on Rational Cubics | 319 |
| Homogeneous Coordinates | 319 |
| Elliptic Curves | 320 |
| Rational Points on Elliptic Curves | 321 |
| Bibliography | 326 |

Appendix 8. Continued Fractions

| | |
|--|-----|
| Introduction | 327 |
| What Is a Continued Fraction? | 327 |
| Regular Continued Fractions. Expansions | 328 |
| Evaluating a Continued Fraction | 329 |
| Continued Fractions as Approximations | 332 |
| Euclid's Algorithm and Continued Fractions | 334 |
| Linear Diophantine Equations and Continued Fractions | 334 |
| A Computer Program | 335 |

CONTENTS

| | |
|---|-----|
| Continued Fraction Expansions of Square Roots | 337 |
| Proof of Periodicity | 338 |
| The Maximal Period-Length | 340 |
| Short Periods | 341 |
| Continued Fractions and Quadratic Residues | 341 |
| Bibliography | 342 |

Appendix 9. Multiple-Precision Arithmetic

| | |
|--|-----|
| Introduction | 343 |
| Various Objectives for a Multiple-Precision Package | 343 |
| How to Store Multi-Precise Integers | 344 |
| Addition and Subtraction of Multi-Precise Integers | 345 |
| Reduction in Length of Multi-Precise Integers | 346 |
| Multiplication of Multi-Precise Integers | 346 |
| Division of Multi-Precise Integers | 348 |
| Input and Output of Multi-Precise Integers | 349 |
| A Complete Package for Multiple-Precision Arithmetic | 349 |
| A Computer Program for Pollard's rho Method | 355 |

Appendix 10. Fast Multiplication of Large Integers

| | |
|---|-----|
| The Ordinary Multiplication Algorithm | 357 |
| Double Length Multiplication | 358 |
| Recursive Use of Double Length Multiplication Formula | 360 |
| A Recursive Procedure for Squaring Large Integers | 361 |
| Fractal Structure of Recursive Squaring | 364 |
| Large Mersenne Primes | 364 |
| Bibliography | 364 |

Appendix 11. The Stieltjes Integral

| | |
|--|-----|
| Introduction | 365 |
| Functions With Jump Discontinuities | 365 |
| The Riemann Integral | 366 |
| Definition of the Stieltjes Integral | 367 |
| Rules of Integration for Stieltjes Integrals | 369 |
| Integration by Parts of Stieltjes Integrals | 370 |
| The Mean Value Theorem | 371 |
| Applications | 372 |

Tables. For Contents, see page 374

List of Textbooks, page 457

Index, page 458

<http://www.springer.com/978-0-8176-8297-2>

Prime Numbers and Computer Methods for
Factorization

Riesel, H.

2012, XVIII, 464 p. 20 illus., Softcover

ISBN: 978-0-8176-8297-2

A product of Birkhäuser Basel