

# 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 . . . . .	8
Hexadecimal Compact Prime Tables . . . . .	10
Difference Between Consecutive Primes . . . . .	10
The Number of Primes Below $x$ . . . . .	11
Meissel's Formula . . . . .	13
Evaluation of $P_k(x, a)$ . . . . .	14
Lehmer's Formula . . . . .	15
Computations . . . . .	16
A Computation Using Meissel's Formula . . . . .	20
A Computation Using Lehmer's Formula . . . . .	22
A Computer Program Using Lehmer's Formula . . . . .	24
Mapes' Method . . . . .	26
Deduction of Formulas . . . . .	26
A Worked Example . . . . .	29
Mapes' Algorithm . . . . .	33
Programming Mapes' Algorithm . . . . .	35
Recent Developments . . . . .	36
Results . . . . .	37
Comparison Between the Methods Discussed . . . . .	38
Bibliography . . . . .	39

## Chapter 2. The Primes Viewed at Large

Introduction . . . . .	40
No Polynomial Can Produce Only Primes . . . . .	40
Formulas Yielding All Primes . . . . .	42
The Distribution of Primes Viewed at Large. Euclid's Theorem . . . . .	44
The Formulas of Gauss and Legendre for $\pi(x)$ . The Prime Number Theorem . . . . .	44
The Riemann Zeta-function . . . . .	47
The Zeros of the Zeta-function . . . . .	52

Conversion From $f(x)$ Back to $\pi(x)$ . . . . .	53
The Riemann Prime Number Formula . . . . .	54
The Sign of $\text{li } x - \pi(x)$ . . . . .	57
The Influence of the Complex Zeros of $\zeta(s)$ on $\pi(x)$ . . . . .	57
The Remainder Term in the Prime Number Theorem . . . . .	60
Effective Inequalities for $\pi(x)$ and $p_n$ . . . . .	61
The Number of Primes in Arithmetic Progressions . . . . .	61
Bibliography . . . . .	62

**Chapter 3. Subtleties in the Distribution of Primes**

The Distribution of Primes in Short Intervals . . . . .	64
Twins and Some Other Constellations of Primes . . . . .	64
Admissible Constellations of Primes . . . . .	66
The Hardy-Littlewood Constants . . . . .	68
The Prime $k$ -Tuples Conjecture . . . . .	70
Theoretical Evidence in Favour of the Prime $k$ -Tuples Conjecture . . . . .	72
Numerical Evidence in Favour of the Prime $k$ -Tuples Conjecture . . . . .	73
The Second Hardy-Littlewood Conjecture . . . . .	73
The Midpoint Sieve . . . . .	75
Modification of the Midpoint Sieve . . . . .	76
Construction of Superdense Admissible Constellations . . . . .	76
Some Dense Clusters of Primes . . . . .	78
The Distribution of Primes Between the Two Series $4n + 1$ and $4n + 3$ . . . . .	79
Graph of the Function $\pi_{4,3}(x) - \pi_{4,1}(x)$ . . . . .	80
The Negative Regions . . . . .	81
The Negative Blocks . . . . .	83
Large Gaps Between Consecutive Primes . . . . .	84
The Cramér Conjecture . . . . .	85
Bibliography . . . . .	88

**Chapter 4. The Recognition of Primes**

Introduction . . . . .	90
Tests of Primality and of Compositeness . . . . .	90
Factorization Methods as Tests of Compositeness . . . . .	91
Fermat's Theorem as Compositeness Test . . . . .	91
Fermat's Theorem as Primality Test . . . . .	91
Pseudoprimes and Probable Primes . . . . .	92
A Computer Program for Fermat's Test . . . . .	93
The Labour Involved in a Fermat Test . . . . .	95
Carmichael Numbers . . . . .	95
Euler Pseudoprimes . . . . .	96
Strong Pseudoprimes and a Primality Test . . . . .	98
A Computer Program for Strong Pseudoprime Tests . . . . .	100
Pseudoprime Counts . . . . .	101

Rigorous Primality Proofs . . . . .	102
Lehmer's Converse of Fermat's Theorem . . . . .	103
Formal Proof of Theorem 4.3 . . . . .	104
Ad Hoc Search for a Primitive Root . . . . .	105
The Use of Several Bases . . . . .	106
Fermat Numbers and Pepin's Theorem . . . . .	107
A Relaxed Converse of Fermat's Theorem . . . . .	109
Proth's Theorem . . . . .	110
Tests of Compositeness for Numbers of the form $N = h \cdot 2^n \pm k$ . . . . .	111
An Alternative Approach . . . . .	111
Primality Tests of Lucasian Type . . . . .	113
Lucas Sequences . . . . .	113
The Fibonacci Numbers . . . . .	114
Large Subscripts . . . . .	114
An Alternative Deduction . . . . .	117
Divisibility Properties of the Numbers $U_n$ . . . . .	119
Primality Proofs by Aid of Lucas Sequences . . . . .	121
Lucas Tests for Mersenne Numbers . . . . .	123
A Relaxation of Theorem 4.8 . . . . .	127
Pocklington's Theorem . . . . .	128
Lehmer-Pocklington's Theorem . . . . .	129
Pocklington-Type Theorems for Lucas Sequences . . . . .	130
Primality Tests for Integers of the form $N = h \cdot 2^n - 1$ , when $3 \nmid h$ . . . . .	131
Primality Tests for $N = h \cdot 2^n - 1$ , when $3 h$ . . . . .	132
Compositeness Tests With Lucas Sequences for $N = h \cdot 2^n \pm k$ . . . . .	136
The Combined $N - 1$ and $N + 1$ Test . . . . .	136
Lucas Pseudoprimes . . . . .	137
Recent Progress in General Primality Proofs . . . . .	138
A General Primality Testing Algorithm . . . . .	139
Three Lemmas . . . . .	139
Lenstra's Theorem . . . . .	142
The Sets $P$ and $Q$ . . . . .	143
The Running Time . . . . .	144
Bibliography . . . . .	145

## Chapter 5. Factorisation

Introduction . . . . .	146
When Do We Attempt Factorization and Which Method Should We Use? . . . . .	146
Trial Division . . . . .	147
A Computer Implementation of Trial Division . . . . .	149
Euclid's Algorithm as an Aid to Factorization . . . . .	151
Fermat's Factoring Method . . . . .	153
Legendre's Congruence . . . . .	156
Euler's Factoring Method . . . . .	146
Gauss' Factoring Method . . . . .	159

Legendre's Factoring Method . . . . .	163
The Number of Prime Factors of Large Numbers . . . . .	163
How Does a Typical Factorization Look? . . . . .	165
The Erdős-Kac Theorem . . . . .	166
The Distribution of Prime Factors of Various Sizes . . . . .	167
Dickman's Version of Theorem 5.4 . . . . .	168
A More Detailed Theory . . . . .	169
The Size of the $k^{\text{th}}$ Largest Prime Factor of $N$ . . . . .	170
Pollard's $(p - 1)$ -Method . . . . .	172
The $(p + 1)$ -Method . . . . .	174
Pollard's $\rho$ -Method . . . . .	174
A Computer Program for Pollard's $\rho$ -Method . . . . .	178
An Algebraic Description of Pollard's $\rho$ -Method . . . . .	180
Brent's Modification of Pollard's Method . . . . .	181
Searching for Factors of Certain forms . . . . .	184
Legendre's Theorem for the Factors of $N = a^n \pm b^n$ . . . . .	184
Adaptation to Search for Factors of the form $p = 2kn + 1$ . . . . .	188
Adaptation of Trial Division . . . . .	188
Adaptation of Fermat's Factoring Method . . . . .	189
Adaptation of Euclid's Algorithm as an Aid to Factorization . . . . .	190
Adaptation of the Pollard-Brent Method . . . . .	191
Shanks' Factoring Method SQUFOF . . . . .	191
A Computer Program for Shanks' Method . . . . .	195
Comparison Between Pollard's and Shanks' Methods . . . . .	199
Morrison and Brillhart's Continued Fraction Method . . . . .	199
The Factor Base . . . . .	200
An Example of a Factorization . . . . .	202
Further Details of the Method . . . . .	207
The Early Abort Strategy . . . . .	209
Results . . . . .	210
Running Time Analysis . . . . .	211
The Quadratic Sieve . . . . .	211
Smallest Solutions to $Q(x) \equiv 0 \pmod{p}$ . . . . .	212
Special Factors . . . . .	213
Results . . . . .	213
Running Time Analysis . . . . .	214
Schroeppel's Method . . . . .	214
The Schnorr-Lenstra Method . . . . .	215
Strategies in Factoring . . . . .	215
How Fast Can a Factorization Algorithm Be? . . . . .	218
Bibliography . . . . .	221

**Chapter 6. Prime Numbers and Cryptography**

Practical Secrecy . . . . .	223
Keys in Cryptography . . . . .	223

Arithmetical Formulation . . . . .	225
RSA Cryptosystems . . . . .	226
How to Find the Recovery Exponent . . . . .	226
A Worked Example . . . . .	228
Selecting Keys . . . . .	231
Finding Primes . . . . .	232
The Fixed Points of an RSA System . . . . .	233
How Safe is an RSA Cryptosystem? . . . . .	235
Superior Factorization . . . . .	235
Bibliography . . . . .	236

**Appendix 1. Basic Concepts in Higher Algebra**

Introduction . . . . .	237
Modules . . . . .	237
Euclid's Algorithm . . . . .	238
The Labour Involved in Euclid's Algorithm . . . . .	240
A Definition Taken from the Theory of Algorithms . . . . .	241
A Computer Program for Euclid's Algorithm . . . . .	242
Reducing the Labour . . . . .	243
Binary Form of Euclid's Algorithm . . . . .	243
The Diophantine Equation $ax + by = c$ . . . . .	245
Groups . . . . .	245
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 . . . . .	260
Homomorphisms and Group Characters . . . . .	261
Bibliography . . . . .	261

**Appendix 2. Basic Concepts in Higher Arithmetic**

Divisors. Common Divisors . . . . .	262
The Fundamental Theorem of Arithmetic . . . . .	262
Congruences . . . . .	263
Linear Congruences . . . . .	265
Linear Congruences and Euclid's Algorithm . . . . .	266
Systems of Linear Congruences . . . . .	268
The Residue Classes (mod $p$ ) Constitute a Field . . . . .	269
The Primitive Residue Classes (mod $p$ ) . . . . .	270

The Structure of the Group $M_n$ . . . . .	272
Homomorphisms of $M_q$ when $q$ is a Prime . . . . .	274
Carmichael's Function . . . . .	275
Carmichael's Theorem . . . . .	276
Bibliography . . . . .	277

**Appendix 3. Quadratic Residues**

Legendre's Symbol . . . . .	278
Arithmetic Rules for Residues and Non-Residues . . . . .	278
Euler's Criterion for the Computation of $(a/p)$ . . . . .	280
The Law of Quadratic Reciprocity . . . . .	281
Jacobi's Symbol . . . . .	284
A PASCAL Function for Computing $(a/n)$ . . . . .	285
The Quadratic Congruence $x^2 \equiv c \pmod{p}$ . . . . .	287
The Case $p = 4k + 1$ . . . . .	287
Bibliography . . . . .	288

**Appendix 4. The Arithmetic of Quadratic Fields**

Integers of $K(\sqrt{D})$ . . . . .	289
Units of $K(\sqrt{D})$ . . . . .	292
Associated Numbers in $K(\sqrt{D})$ . . . . .	293
Divisibility in $K(\sqrt{D})$ . . . . .	294
Fermat's Theorem in $K(\sqrt{D})$ . . . . .	295
Primes in $K(\sqrt{D})$ . . . . .	297
Factorization of Integers in $K(\sqrt{D})$ . . . . .	298
Bibliography . . . . .	299

**Appendix 5. Continued Fractions**

Introduction . . . . .	300
What Is a Continued Fraction? . . . . .	300
Regular Continued Fractions. Expansions . . . . .	301
Evaluating a Continued Fraction . . . . .	303
Continued Fractions as Approximations . . . . .	306
Euclid's Algorithm and Continued Fractions . . . . .	307
Linear Diophantine Equations and Continued Fractions . . . . .	308
A Computer Program . . . . .	309
Continued Fraction Expansions of Square Roots . . . . .	311
Proof of Periodicity . . . . .	312
The Maximal Period-Length . . . . .	314
Short Periods . . . . .	315
Continued Fractions and Quadratic Residues . . . . .	315
Bibliography . . . . .	317

**Appendix 6. Algebraic Factors**

Introduction . . . . .	318
Factorization of Polynomials . . . . .	318
The Cyclotomic Polynomials . . . . .	319
The Polynomial $x^n + y^n$ . . . . .	322
The Polynomial $x^n + ay^n$ . . . . .	323
Aurifeuillian Factorizations . . . . .	323
Factorization Formulas . . . . .	325
The Algebraic Structure of Aurifeuillian Numbers . . . . .	328
A formula by Gauss for $x^n - y^n$ . . . . .	330
Bibliography . . . . .	331

**Appendix 7. Multiple-Precision Arithmetic**

Introduction . . . . .	332
Various Objectives for a Multiple-Precision Package . . . . .	332
How to Store Multi-Precise Integers . . . . .	333
Addition and Subtraction of Multi-Precise Integers . . . . .	334
Reduction in Length of Multi-Precise Integers . . . . .	335
Multiplication of Multi-Precise Integers . . . . .	335
Division of Multi-Precise Integers . . . . .	337
Input and Output of Multi-Precise Integers . . . . .	338
A Complete Package for Multiple-Precision Arithmetic . . . . .	339
A Computer Program for Pollard's $\rho$ -Method . . . . .	345

**Appendix 8. Fast Multiplication of Large Integers**

The Ordinary Multiplication Algorithm . . . . .	348
Double Length Multiplication . . . . .	349
Recursive Use of Double Length Multiplication Formula . . . . .	351
A Recursive Procedure for Squaring Large Integers . . . . .	352
Fractal Structure of Recursive Squaring . . . . .	356
Large Mersenne Primes . . . . .	356
Bibliography . . . . .	357

**Appendix 9. The Stieltjes Integral**

Introduction . . . . .	358
Functions With Jump Discontinuities . . . . .	358
The Riemann Integral . . . . .	359
Definition of the Stieltjes Integral . . . . .	361
Rules of Integration for Stieltjes Integrals . . . . .	363
Integration by Parts of Stieltjes Integrals . . . . .	363
The Mean Value Theorem . . . . .	365
Applications . . . . .	366

**Tables**

Table 1. The Primes Below 12553 . . . . .	369
Table 2. The Primes Between $10^n$ and $10^n + 1000$ . . . . .	372
Table 3. $\pi(x)$ and the Errors in $\text{li } x$ and $R(x)$ . . . . .	374
Table 4. Factors of Fermat Numbers . . . . .	377
Table 5. Primes of the Form $h \cdot 2^n + 1$ . . . . .	381
Table 6. Primes of the Form $h \cdot 2^n - 1$ . . . . .	384
Table 7. Factors of Mersenne Numbers . . . . .	388
Table 8. Factors of $2^n + 1$ . . . . .	392
Table 9. Factors of $10^n - 1$ . . . . .	398
Table 10. Factors of $10^n + 1$ . . . . .	400
Table 11. Factors of $3^n \pm 2^n$ . . . . .	404
Table 12. Factors of $4^n \pm 3^n$ . . . . .	407
Table 13. Factors of $5^n \pm 2^n$ . . . . .	409
Table 14. Factors of $5^n \pm 3^n$ . . . . .	410
Table 15. Factors of $5^n \pm 4^n$ . . . . .	412
Table 16. Factors of $6^n \pm 5^n$ . . . . .	413
Table 17. Factors of $7^n \pm 2^n$ . . . . .	415
Table 18. Factors of $7^n \pm 3^n$ . . . . .	416
Table 19. Factors of $7^n \pm 4^n$ . . . . .	418
Table 20. Factors of $7^n \pm 5^n$ . . . . .	419
Table 21. Factors of $7^n \pm 6^n$ . . . . .	421
Table 22. Factors of $8^n \pm 3^n$ . . . . .	422
Table 23. Factors of $8^n \pm 5^n$ . . . . .	424
Table 24. Factors of $8^n \pm 7^n$ . . . . .	425
Table 25. Factors of $9^n \pm 2^n$ . . . . .	427
Table 26. Factors of $9^n \pm 5^n$ . . . . .	428
Table 27. Factors of $9^n \pm 7^n$ . . . . .	430
Table 28. Factors of $9^n \pm 8^n$ . . . . .	431
Table 29. Factors of $10^n \pm 3^n$ . . . . .	433
Table 30. Factors of $10^n \pm 7^n$ . . . . .	434
Table 31. Factors of $10^n \pm 9^n$ . . . . .	436
Table 32. Quadratic Residues . . . . .	438
Table 33. Gauss' formulas for Cyclotomic Polynomials . . . . .	445
Table 34. Lucas' formulas for Cyclotomic Polynomials . . . . .	452

**Index**