Index

Note. Routine references to other textbooks are not indexed here. Some multi-author works are indexed only under the first author. See the list of references for more details. Boldface references are to definitions and theorems.

Abelson, H. 33, 123
abundant number 167
Adelman, L.M. 133
Alanen, J. 166
algorithm 13
al-Khowarizmi 13
amicable pairs 163
unitary 169
Anderson, J. 31
arithmetic, fundamental theorem of 1
arithmetic progression, primes in 81
Aurifeulle, A. 4
Beiler, A.H. 78
Berlekamp, E.R. 31
binomial coefficient 9, 27
Bombelli, R. 174
Boyd, D.W. 79
Brent, R.P. 3, 85, 167
brick, rectangular 10
Briggs, W.E. 67
Brillhart, J. 3, 4, 191
Broucker, J. 189
Bruce, J.W. 23, 172
Carmichael numbers 45, 100ff, 108, 109, 156
   infinitely many 101
   ceiling function 14
Ch'in Chiu-shao 79
Chinese remainder theorem 79
Churchhouse, R.F. 74
ciphers
   exponentiation 134ff
   RSA 133ff
Cipra, B. 3
Cohen, G.L. 167
coin tossing 145
Cole, F.N. 4
Colquitt, W. 171
composite(s) 1
   consecutive 5
   highly 161
   Sierpinski–Selfridge formula for 122
congruences 69ff
covering 73
   using primitive roots 148ff
   quadratic 217
solutions of linear 74ff, 119
   simultaneous 77, 79ff
\( x^2 \equiv 1 \ 76, 82 \)
Index

$z^2 \equiv z \ 77, 78$
$x^2 \equiv a \ 145, 151, 205, 217ff$
$x^d \equiv 1 \ 88$
$p^{a-1} \equiv 1 \ (mod \ p^2) \ 97, 148$
$x^2 \equiv y^2 \ 73, 175$
conjugate 187
continued fractions 174ff
  complete quotients 177, 182
  convergence 186
  convergents 176, 178
  partial quotients 177
for $\sqrt{\cdot} \ 180ff, 200$
and Pell's equation 189ff
recurrence 181

coprime 8
  random pairs 16
Costello, P. 166

cryptography 133ff
  cubes, sum of 33
Cunningham chain 125, 204
deciphering key 134
de la Vallee-Poussin 53
decimals, periods of 130ff
deficient number 167
Dickson, L.E. 167
diophantine equation 18, 72, 79
  linear 19ff, 74ff
  Pell's equation 189ff
  see also congruences
directed terrace 72
Dirichlet, G.L. 209
diSessa, A. 33, 123
divisor(s) 1
  common 7
  greatest common, see greatest
  common divisor
  number of 158ff
  sum of 158ff
  unitary 169
divisibility tests 71-2
Dixon, J. 23
Dodd, F. 27
Dressler, R.E. 118
Dubner, H. 101
Ehrlich, A. 74
Eisenstein, F.G. 207
Eldridge, K.E. 30
enciphering key 134
Eratosthenes, sieve of 55ff
Euclid 6
  Euclidean algorithm for gcd 12ff
  and continued fractions 175, 180
  modification 16
  minimal representation and 23
  number of steps 18, 23
  program for 14
Euler, L. 86, 174, 189, 147
  and Fermat numbers 3, 205
  and Mersenne numbers 4
  theorem on perfect numbers 167
  $\phi$ (totient) function, see
  phi-function
quadratic residue criterion 152, 201
  theorem 115, 119ff
exponent
  belonging to 120
  minimal universal 156
factor(s) 1
  highest common, see greatest
  common divisor
  number of prime 48
  primitive prime 48
  proper 73
factorial 26
factorization
  complete 3
  continued fraction method 191ff
  Fermat's method 138
  prime-power 2
  by trial division 44
Farey series 30
Fermat, P. de 3, 163, 170, 189, 191
  factorizing method 128
  last theorem 18, 72, 97, 121
  (little) theorem 86, 115
  numbers 3, 18, 46, 72, 85, 92, 97,
  115, 191, 199, 205
  primality test for 97, 202, 209
  quotients 87
Fibonacci
  nim 30
  numbers 35
  mod $m$ 74, 218
floor function 14
fourth powers, sum of 71
Fowler, D.H. 13
Gardiner, V. 67
Gardner, M. 31, 133
Gauss, C.F. 53, 69, 83, 147, 203, 206
   Lemma 206
gibberish 137
Goetghebuer, P. 27
Goldbach's conjecture 163
Graham, R. 24, 115
Granville, A. 101
greatest common divisor (gcd) 8
   algorithm for, see Euclid
   factorization related to 11, 47
   and least common multiple 11
   as linear combination of numbers
   17, 18, 20
   program 21
   of random pairs 15
   of three numbers 10
group 173
Gupta, H 202
INT 14
Hadamard, J. 53
Hagis, P. 169
hailstone (3N + 1) problem 32
Hayes, B. 32
Hawkins, D. 67
Head's algorithm 93ff
Heath-Brown, D.R. 160
Hellman, M.E. 133, 134
Hilbert prime 30
Hoehn, L. 29
Ibn al-Banna 163
inclusion-exclusion, principle of 10,
   59, 60
index 148
integer part 14, 24ff
inverse 22, 74, 119
Jacobi symbol 211
Jones, J.P. 35
Jordan, J.H. 30
Kaprekar constant 29
Keller, W. 4
Knuth, D.E. 115
Kraitchik, M. 4
Kummer, E.E. 27
Lagarias, J.C. 32
Lagrange, J.L. 102, 173
   four squares theorem 32
Lal, M. 128
Lambert, G.H. 147

Landry, F. 3
   painful story 4
least common multiple (lcm) 11, 47
   of three numbers 12
   of orders 122
Lee, E.J. 163
Legendre, A.M. 58
   sieve 58ff
   symbol 200
Lehmer, D.H. 58, 125, 128, 171, 191
Lehning, H. 36
Lenstra, A. 3
Lindemann, F.A. 2
Lines, M.E. 30, 31
Liouville, J. 161
logarithmic integral 53, 65
Lucas, E. 171
   factorizations 5
   primality test (“n − 1 over q test”) 125
lucky numbers 67
Madachy, J.S. 163
magic squares 83
Manasse, M. 3
McDaniel, W.L. 99
mediant 30
Meissel, E.D.F. 58
Mersenne numbers 4, 5, 98, 167, 170
   factor of 171, 204
   Lucas–Lehmer test 171, 210
Miller's test 104ff
modulus 69
Morain, F. 12
Morrison, M.A. 3, 191
   multiple, least common, see least
   common multiple
   multiplicative function 113, 159,
   162
nim, Fibonacci 30
non-totient 114, 118
order 105, 120ff
   lcm of 122
Paganini, B.N.I. 166
palindromes 31, 185
Peelle, R. 27
Pell's equation 189ff
Pepin's test 97, 202, 209
   perfect numbers 158, 160ff
   k- 167
Index

odd 168
unitary 169
periods of decimals 130ff
phi-function 112ff, 136ff
average 116
and combinatorics 115
iterated 117
Pohlig, S. 134
Pollard, J.M. 3, 84, 85
p − 1 method 93
ρ method 84
polygons 123
Potter, A. 5, 41
power algorithm 80ff
Powers, R.E. 191
prime(s) 1
in arithmetic progression 81
Cunningham chain of 125, 204
by division 38ff
eight 11
number of prime factors 48
gaps between 5, 40, 41
Hilbert 30
infinitely many 6
listing 37ff
Mersenne, see Mersenne
by multiplication 50ff
mutually, see coprime
number ≤ x (π(x)) 40, 44, 52ff, 55ff
power dividing n! 26
probable 109
product of two 6
relatively, see coprime
as sum of two squares 79
triples 41
twin 41, 102, 127
twins 4
4r − 1 6, 48, 151
4r + 1 48, 79, 151, 201
8r + 1 151
8r + 5 151, 202
8r − 1 204
8r + 3 204
5r + 4 209
n^6 + 1091 203
primality tests 89, 105, 110, 124ff
trial division 54
“n − 1 over q test” 125

prime number theorem 53
primitive prime factor 48
primitive root 105, 121, 131, 147ff, 203, 219
extistence of 150ff
finding (Gauss's method) 154
least 210
number of 152
equal to 2, 204
probabilistic primality test 110
Proth's theorem 129
converse 209
pseudoprimes 98ff, 108
infinitely many 99
strong 106
public key cryptography 133ff
quadratic reciprocity 206ff
quadratic residue 151, 200ff
chain of 202
Euler's criterion for 152, 201
Jacobi symbol for 211
quotients, see continued fractions
Rabin's test 110
RANDOMIZE 16
Ratering, S. 161
repunit 5, 18, 45, 46, 119
residue 69
Ridenhour, J. 227
Riemann, B.
function 54, 65
hypothesis 110
Rivest, R.L. 133
Rosen, M.I. 172, 210
Rosencreantz and Guildenstern 136ff
RSA ciphers 133ff
Sacks, O. 4
Sagong, S. 30
Schnizel, A. 49
Schoenberg, I.J. 154
Selfridge, J.L. 4, 92, 123
Shamir, A. 133
Shapiro, H.N. 117
Shanks, D. 87, 217, 220, 222
sieve
of Eratosthenes 55ff
of Legendre 58ff
for lucky numbers 67
shunting 31
Thabit ibn Qurra 163
Index

Thue, A. 115
    lemma 78
tiling 23
totient function, see phi-function
trial division 38f, 44, 54
trinomial 27
Turner, S.M. 222
twin primes, see prime
twins, prime 4
unitary divisor, see divisor
verbal sequences 35
Wagon, S. 80
Wall, C.R. 169
Wall, D.D. 74, 218

Wallis, J. 174
Waring, E 81
    problem 25, 32, 71
weird numbers 168
Wells, D. 31, 163
Welsh, L. 171
Western, A.E. 92
Wieferich, A. 97, 121
Wilson’s theorem 102
Wong, W.J. 27
Young, J. 5, 41
zigzags 3 3
Zsigmondy, K. 48
Index of Listed Programs

P1.3.5 Euclid’s algorithm for the gcd
P1.3.16 Greatest common divisor as linear combination of the numbers
P2.1.3 Primes by trial division by odd numbers up to the square root
P2.1.4 Second program for primes by trial division
P2.1.10 A text file of primes
P2.1.11 Reading primes from a file
P2.1.13 Factorization by trial division
P2.1.15 Modified factorization by trial division
P2.1.17 Special factorization related to lcm and gcd
P2.1.21 File of primes as reals
P2.1.21A Extracting an entry from the previous file
P2.2.1 Primes by multiplication (elimination of composites)

P2.4.1 Sieve of Eratosthenes
P2.4.3 Alternative program for the sieve of Eratosthenes
P2.4.8 Legendre’s sieve
P2.4.12 Calculation of \( \phi(x, a) \)
P4.2.3 Power algorithm
Ch.4, 3.4 Procedure for Head’s algorithm
P4.3.4 Power rule using Head’s algorithm
P5.1.5 Miller’s test
P5.1.6 Miller’s test using Head’s algorithm
Ch.6, 3.5 Lucas’s primality test
P7.2.3 Public key cryptography
P9.1.3 Divisor function \( d(n) \)
P9.2.5 Sum of divisors, \( \sigma(n) \)
P10.2.6 Continued fraction of \( \sqrt{n} \)
P10.5.5 Factorization by continued fractions
P11.4.6 Quadratic residue evaluation
P11.5.5 Solving \( x^2 \equiv a (mod \ p) \)
Index of Notation

\[ d(n) \text{ number of divisors of } n \quad 158 \]
\[ F_n \text{ Fermat number } 3 \]
\[ \text{mod modulus } 69 \]
\[ \text{ord}_n a \text{ order of } a, \text{mod } n \quad 120 \]
\[ s(n) \sigma(n) = n \quad 165 \]
\[ a \mid b \text{ a divides } b \quad 1 \]
\[ [x] \text{ integer part of } x \quad 14 \]
\[ [a_0, \ldots, a_n] \text{ continued fraction } 176 \]
\[ c_k = \frac{p_k}{q_k} \text{ convergent of continued fraction } 178 \]
\[ P_k, Q_k \text{ from continued fraction of } \sqrt{n} \quad 182 \]
\[ Q_k^* = (-1)^k Q_k \quad 191 \]
\[ \equiv \text{ congruence } 69 \]
\[ \pi(x) \text{ number of primes } \leq x \quad 40 \]
\[ \phi(x, a) \text{ number of } n \leq x \text{ not divisible by any of the first } a \text{ primes } 66 \]
\[ \phi(n) \text{ Euler's totient function } 112 \]
\[ \sigma(n) \text{ sum of divisors of } n \quad 158 \]
\[ \sigma^*(n) \text{ sum of unitary divisors of } n \quad 169 \]
\[ \left( \frac{a}{p} \right) \text{ Legendre symbol } 200 \]
\[ \left( \frac{a}{k} \right) \text{ Jacobi symbol } 211 \]