

## Index

- Abramowitz, Milton, 179, 180, 190
- addition, 2, 91
  - carry bit, 10, 92
  - modular, 50
- addition chain, xiv, 69
  - weighted, 77
- Adleman, Leonard Max, 68
- AGM, *see* arithmetic-geometric mean
- Agrawal, Manindra, 45
- Aho, Alfred Vaino, 46, 78
- AKS primality test, 45
- algorithm
  - AGM (for log), 159, 162
  - Akiyama–Tanigawa, 181
  - ApproximateReciprocal, 103, 119
  - ApproximateRecSquareRoot, 113
  - BackwardFFT, 54
  - Barrett’s, 58, 78, 109, 111, 119
  - BarrettDivRem, 59
  - BasecaseDivRem, 15, 41, 42
  - BasecaseMultiply, 4, 40
  - BaseKExp, 71
  - BaseKExpOdd, 72
  - D. Bernstein’s, 122
  - R. Bernstein’s, 14
  - binary splitting, 163
  - BinaryDivide, 34
  - BinaryGcd, 31
  - bit-burst, 167, 178
  - Bluestein’s, 78
  - Brent–Salamin, 159, 184
  - cryptographic, 68, 78
  - DivideByWord, 24
  - DivideNewton, 107, 111, 119, 122
  - DoubleDigitGcd, 31
  - Erf, 149, 175
  - EuclidGcd, 30
  - ExactDivision, 22, 122
  - ExtendedGcd, 33, 43
  - FastIntegerInput, 39, 43
  - FastIntegerOutput, 39
  - FastREDC, 62
  - FFTMulMod, 56
  - ForwardFFT, 53
  - FPadd, 92
  - FPmultiply, 96
  - FPSqrt, 111, 119
  - Friedland’s, 182
  - Fürer’s, 57, 78
  - Gauss–Legendre, 159, 184
  - HalfBinaryGcd, 35, 43
  - HalfGcd, 43
  - IntegerAddition, 2
  - IntegerInput, 38
  - IntegerOutput, 38
  - IntegerToRNS, 73, 78

- IsPower, 29
- KaratsubaMultiply, 5, 40
- lazy, 2, 44
- LeftToRightBinaryExp, 70, 76
- LiftExp, 131
- McLaughlin's, 63–65, 77
- ModularAdd, 50, 76
- ModularInverse, 66
- Montgomery's, 60
- MontgomerySvoboda, 62
- Mulders', 96
- MultipleInversion, 67, 78
- MultMcLaughlin, 64
- OddEvenKaratsuba, 9, 41
- off-line, 2, 44
- on-line, 44
- parallel, 46, 49, 67, 76, 77, 175, 180
- Payne and Hanek, 101
- PrintFixed, 116, 120
- Rader's, 78
- RecursiveDivRem, 18, 42
- REDC, 60
- ReducedRatMod, 32, 46
- relaxed, 2, 44
- RightToLeftBinaryExp, 76
- RNSToInteger, 74
- RootInt, 27
- RoundingPossible, 89
- Sasaki–Kanada, 162, 181
- Schönhage–Strassen, 49, 55, 65, 78, 105, 122, 185
- SecantNumbers, 176, 177, 181
- SeriesExponential, 177
- ShortDivision, 108, 111, 121
- ShortProduct, 97, 121
- SinCos, 166
- SqrtInt, 27, 43, 45
- SqrtRem, 26, 45
- Strassen's, 36, 123
- SvobodaDivision, 17, 42
- systolic, 46
- TangentNumbers, 157, 176, 177, 181
- ToomCook3, 7
- UnbalancedDivision, 20, 42
- unrestricted, 121, 125
- zealous, 44
- Ziv's, 86
- aliasing, 179
- Andrews, George Eyre, 179, 180
- ANU, xi
- Apostol, Tom Mike, 180
- ARC, xi
- argument reduction, 101, 132–135
  - additive, 133
  - multiplicative, 133
- arithmetic-geometric mean, 158–163
  - advantages, 158
  - complex variant, 163
  - drawbacks, 162
  - error term, 160
  - for elliptic integrals, 158
  - for logarithms, 159–162
  - optimization of, 162, 182
  - Sasaki–Kanada algorithm, 162
  - scaling factor, 161
  - theta functions, 160
- Arndt, Jörg, xi, 181, 184
- ARPREC, 187
- Askey, Richard Allen, 179, 180
- asymptotic equality notation  $\sim$ , xv
- asymptotic expansions, 144, 180
- asymptotic series notation, xv
- Avizienis representation, 73
- Bach, (Carl) Eric, 46
- Bachmann, Paul Gustav Heinrich, 46
- Backeljauw, Franky, 180
- backward summation, 135, 138

- Bailey, David Harold, 184, 187  
 balanced ternary, 119  
 Barrett's algorithm, 58–60, 62, 77, 78, 109, 119  
 Barrett, Paul, 58, 59  
 base, xiv, 1, 80  
   conversion, 37, 190  
 Batut, Christian, 189  
 Becuwe, Stefan, 180  
 Beeler, Michael, 181  
 Belabas, Karim, 189  
 Bellard, Fabrice, 184  
 Bernardi, Dominique, 189  
 Bernoulli numbers, xiii, 147, 154, 156, 169, 176  
   Akiyama–Tanigawa algorithm, 181  
   complexity of evaluation, 177  
   denominators of, 156  
   fast evaluation, 177  
   Harvey's algorithm, 181  
   scaled, xiii  
   space required for, 169, 176  
   stable computation, 155, 176, 180  
   via tangent numbers, 156  
 Bernstein, Daniel Julius, 43, 45, 77, 78, 122, 123, 181  
 Bernstein, Joseph Naumovich, 183  
 Bernstein, Robert, 14  
 Berry, Michael Victor, 183  
 Bertot, Yves, 45  
 Bessel functions, 153  
   first kind,  $J_\nu(x)$ , 153  
   in computation of  $\gamma$ , 146, 184  
   Miller's algorithm, 154  
   second kind,  $Y_\nu(x)$ , 153  
 Bessel's differential equation, 153  
 Bessel, Friedrich Wilhelm, 152  
 Bézout coefficients, 32  
 Bézout, Étienne, 32  
 Big  $O$  notation, xv  
 binary coded decimal (BCD), 81  
 binary exponentiation, 69, 70  
 binary number, notation for, xvi  
 binary representation, 1  
   conversion to decimal, 37  
 binary splitting, 163–166, 178, 185  
   CLN library, 182  
   for  $1/\pi, \zeta(3)$ , 184  
   for sin/cos, 166  
 binary-integer decimal (BID), 81  
 binary64, 81, 83, 120  
 BinaryDivide, 34  
 binomial coefficient, xiii, 43  
 bipartite modular multiplication, 77  
 bit reversal, 53, 54  
 bit-burst algorithm, 166–169, 178  
 Bluestein, Leo Isaac, 78  
 Bodrato, Marco, xi, 44, 119  
 Boldo, Sylvie, 118  
 Bonan-Hamada, Catherine, 180  
 Booth representation, 73, 78  
 Bornemann, Folkmar, 184  
 Borodin, Allan Bertram, 45, 78  
 Borwein, Jonathan Michael, 159–161, 181–184, 190  
 Borwein, Peter Benjamin, 159–161, 181–184, 190  
 Bostan, Alin, 122  
 branch prediction, 16  
 Brent, Erin Margaret, xi  
 Brent, Richard Peirce, 45, 121, 166, 182, 184  
 Brent–McMillan algorithm, 146, 184  
 Brent–Salamin algorithm, 159, 184  
 Briggs, Keith Martin, 45  
 Bruijn, *see* de Bruijn  
 Bulirsch, Roland Zdeněk, 184  
 Bürgisser, Peter, 41, 123  
 Burnikel, Christoph, 45

- butterfly operation, 53
- C, 66, 186–189
- C++, 185, 187, 189
- cancellation, 138
- Cannon, John Joseph, 188
- carry bit, 10, 40, 92
- catastrophic cancellation, 138
- Cauchy principal value, xvi, 144
- Cauchy's theorem, 170
- Cayley, 188
- ceiling function  $\lceil x \rceil$ , xv
- Chen, Kwang-Wu, 181
- Cheng, Howard, 184
- Chinese remainder representation,  
*see* modular representation
- Chinese remainder theorem (CRT),  
 73–75, 78  
 explicit, 49  
 reconstruction, 74, 78
- Chiu Chang Suan Shu, 45
- Chudnovsky, David Volfovich, 166,  
 183, 184
- Chudnovsky, Gregory Volfovich,  
 166, 183, 184
- Chung, Jaewook, 45
- classical splitting, 142
- Clausen, Michael Hermann, 41, 123
- Clausen, Thomas, 156, 181
- Clenshaw, Charles William, 120, 180,  
 184
- Clenshaw–Curtis quadrature, 184
- Clinger, William Douglas, 123
- CLN, 182, 185
- Cohen, Henri, 45, 189
- Collins, George Edwin, 121
- complementary error function, *see*  
 $\operatorname{erfc}(x)$
- complex  
 AGM, 163
- arithmetic, 187  
 multiplication, 163  
 square root, 182  
 squaring, 163
- complexity  
 arithmetic, 3, 4  
 asymptotic, 8  
 bit, 4
- concatenation, notation for, xvi, 38
- continued fraction  
 approximant, 151  
 backward recurrence, 151, 175  
 error bound, 152, 175  
 fast evaluation, 175, 180  
 for  $E_1$ , 150  
 for  $\operatorname{erfc}$ , 150  
 forward recurrence, 151, 175  
 notation for, xvi, 150  
 regular, 30
- contour integration, 169, 184
- convolution, xiv, 78  
 convolution theorem, 50  
 cyclic, xiv, 76, 98  
 via FFT, 64, 99
- Cook, Stephen Arthur, 44
- Cornea-Hasegan, Marius Adrian,  
 122, 123
- correct rounding  $\circ_n$ , 85
- $\cosh(x)$ , 136
- Cowlshaw, Mike, 123, 190
- Crandall, Richard Eugene, 44, 122
- Crary, Fred D., 183
- CRT, *see* Chinese remainder theorem
- cryptographic algorithm, 68, 78
- Curtis, Alan R., 184
- Cuyt, Annie, 180
- D-finite, *see* holonomic
- DBNS, 78
- DDMF, 190

- de Bruijn, Nicolaas Govert (Dick), 180
- decimal arithmetic, 81
- decimal representation, 2  
   conversion to binary, 37
- decimal64, 120
- deg, xv
- determinant, notation for, xvi
- Detrey, Jérémie, xi
- DFT, *see* Discrete Fourier transform
- differentiably finite, *see* holonomic
- Diffie, Bailey Whitfield, 68
- Diffie–Hellman key exchange, 68
- Dimitrov, Vassil S., 78
- Discrete Fourier transform, 50, 64  
   notation for, xv
- div notation, xiv
- divide and conquer  
   for conversion, 38  
   for GCD, 33  
   for multiplication, 5
- division, 14–25, 49  
   by a single word, 23, 42  
   classical *versus* Hensel, 24  
   divide and conquer, 18  
   Euclidean, 49  
   exact, 14, 21, 42  
   full, 14  
   Goldschmidt’s iteration, 123  
   modular, 65  
   notation for, xiv  
   paper and pencil, 25  
   SRT algorithm, 126, 128, 179  
   time for,  $D(n)$ , xiv, 102  
   unbalanced, 19, 42
- divisor  
   implicitly invariant, 60, 78  
   notation for, xiv  
   preconditioning, 17, 61
- Dixon, Brandon, 44
- DLMF, 190
- double rounding, 90
- double-base number system, 78
- doubling formula, 133–136, 171, 172  
   for exp, 133  
   for sin, 133  
   for sinh, 136  
   versus tripling, 136, 179
- Dupont, Régis, 181
- $e$ , *see* Euler’s constant  $e$
- ECM, *see* elliptic curve method
- Ehrhardt, Wolfgang, xi
- $\text{Ein}(x)$ , 173
- elementary function, 125–144
- El Gamal, Taher, 68
- El Gamal cryptosystem, 68
- elliptic curve cryptography, 65
- elliptic curve method, 77
- elliptic integral, 158  
   first kind, 158  
   modulus, 159  
   nome, 161  
   second kind, 158
- email addresses, x
- Enge, Andreas, 45, 119, 187
- entire function, 140
- Ercegovac, Milòs Dragutin, 123
- $\text{erf}(x)$ , 138, 148, 173
- $\text{erfc}(x)$ , 139, 148, 150
- error correction, 75
- error function, *see*  $\text{erf}(x)$
- ESF, 190
- Estrin, Gerald, 180
- Euclid, 29
- Euclidean algorithm, *see* GCD
- Euler’s constant  $e$ , 184
- Euler’s constant  $\gamma$ , 184  
   Brent–McMillan algorithm, 146, 184

- Euler–Maclaurin approx., 146
- Euler’s totient function, xiv
- Euler–Maclaurin formula, 146, 180
  - for computation of  $\gamma$ , 146
- $\exp(x)$ , *see* exponential
- exponent, 79, 81, 83
- exponential
  - addition formula, 133
  - binary splitting for, 182
  - `expm1`, 135, 172
  - notations for, xv
- exponential integral, 144, 150, 173, 175
- exponentiation
  - binary, 70
  - modular, 68–73
- extended complex numbers  $\widehat{\mathbb{C}}$ , 151
- fast Fourier transform (FFT), 8, 50, 65, 86, 122
  - Bluestein’s algorithm, 78
  - complex, 99
  - in place algorithm, 53
  - over finite ring, 99
  - padding, 58, 98
  - Rader’s algorithm, 78
  - rounding errors in, 99
  - use for multiplication, 58, 98
- Féjer, Leopold, 184
- Fermat, Pierre de
  - little theorem, 69, 156
- FFT, *see* fast Fourier transform
- field, finite, 77, 78
  - representation, 49
- Figures
  - Figure 1.1, 12
  - Figure 1.2, 13
  - Figure 1.3, 20
  - Figure 1.4, 21
  - Figure 1.5, 24
- Figure 2.1, 68
- Figure 3.1, 95
- Figure 3.2, 97
- Figure 3.3, 100
- Figure 3.4, 101
- Figure 3.5, 110
- finite field, *see* field
- floating-point
  - addition, 91, 92, 121
  - binary64, 81
  - choice of radix, 121
  - comparison, 91
  - conversion, 114, 123
  - decimal, 114
  - division, 101
  - double precision, 81
  - encoding, 83
  - expansions, 86, 121
  - guard digits, 135
  - input, 117
  - level-index representation, 120
  - loss of precision, 134
  - multiplication, 95
  - output, 115
  - reciprocal, 101, 102, 122
  - reciprocal square root, 112
  - redundant representations, 120
  - representation, 79
  - sign-magnitude, 84
  - special values, 82
  - square root, 111
  - subtraction, 91, 93
  - via integer arithmetic, 86
- floor function  $[x]$ , xv
- `fmaa` instruction, 40
- folding, 63
- Fortran, 187
- forward summation, 135, 138
- Fourier transform, *see* DFT
- fraction, *see* significand

- free format, 123  
 Friedland, Paul, 182  
 function, D-finite, *see* holonomic  
 function, elementary, *see* elementary  
 function, holonomic, *see* holonomic  
 function, special, *see* special  
 functional inverse, 125  
 Fürer, Martin, 78
- Gabcke sequence, 183  
 Gabcke, Wolfgang, 183  
 Galbraith, Steven Douglas, xi, 43  
 $\gamma$ , *see* Euler's constant  $\gamma$   
 Gamma function  $\Gamma(x)$ , 134, 137, 138,  
 147–150, 173, 174, 177, 183,  
 184  
   on imaginary axis, 174  
 Gathen, *see* von zur Gathen  
 Gaubatz, Gunnar, 77  
 Gaudry, Pierrick, 186  
 Gaunt, John Arthur, 184  
 Gauss, Johann Carl Friedrich, 46, 158  
 Gauss–Kuz'min theorem, 45  
 Gauss–Legendre algorithm, 159, 184  
 Gaussian quadrature, 184  
 Gautschi, Walter, 180  
 Gay, David M., 123  
 GCD, 29  
   algorithms for, 29  
   Bézout coefficients, 32  
   binary, 30, 49  
   cofactors, 32  
   continued fraction from, 30  
   divide and conquer, 33  
   double digit, 30, 33  
   Euclidean, 29, 45, 49  
   extended, 29, 32, 43, 65  
   half binary, 33  
   Lehmer's algorithm, 29  
   multipliers, 32  
   notation for, xiv  
   plain, 29  
   Sorenson's algorithm, 29  
   subquadratic, 33–37, 43  
   subtraction-only algorithms, 29
- Gerhard, Jürgen, 77  
 Girgensohn, Roland, 184  
 GMP, xi, 185, 188, 189  
 gnuplot, xi  
 Goldberg, David Marc, 121  
 Goldschmidt's iteration, 123  
 Golliver, Roger Allen, 122  
 Goodwin, Charles E. T., 180  
 Gopal, Vinodh, 77  
 Gosper, Ralph William, Jr., 181  
 Gourdon, Xavier Richard, 183, 184  
 GP, 189  
 GPL, 185  
 Graham, Ronald Lewis, 181  
 Granlund, Torbjörn, xi, 42, 78, 185  
 greatest common divisor, *see* GCD  
 Grotefeld, Andreas Friedrich Wilhelm, 122, 182  
 group operation  
   cost of, 77  
   notation for, 73  
 guard digits, 96, 118, 135  
   for AGM, 162  
   for Bernoulli numbers, 155, 170  
   for catastrophic cancellation, 138  
   for *exp*, 171  
   for subtraction, 94  
   for summation, 138  
   negative, 162
- Haenel, Christoph, 184  
 Haible, Bruno, 182, 185  
 HAKMEM, 181  
 HalfBezout, 30  
 HalfBinaryGcd, 34, 65

- HalfGcd, 43  
 Hanek, Robert N., 101, 122  
 Hankerson, Darrel Richard, 78  
 Hanrot, Guillaume, xi, 40, 41, 45, 122, 184  
 harmonic number, xiii, 173  
 Hars, Laszlo, 77  
 Harvey, David, 39–41, 44, 45, 122, 123, 177, 178, 181, 182  
 Hasan, Mohammed Anwarul, 45  
 Hasenplaugh, William, 77  
 Håstad, Johan Torkel, 41  
 Hellman, Martin Edward, 68  
 Hennessy, John LeRoy, 121  
 Hensel  
   division, 24–25, 45, 49, 58–61, 66  
   lifting, 21, 22, 32, 45, 49, 65  
 Hensel, Kurt Wilhelm Sebastian, 49  
 Heron of Alexandria, 129  
 Higham, Nicholas John, 121, 179  
 Hille, Einar Carl, 170  
 Hoeven, *see* van der Hoeven  
 holonomic function, 139, 167, 178, 183  
 Hopcroft, John Edward, 46, 78  
 Horner's rule, 137, 142, 143  
   forward, 171  
 Horner, William George, 137  
 Householder, Alston Scott, 179  
 Hull, Thomas Edward, 121  
 Hurwitz zeta-function, 183  
 Hurwitz, Adolf, 183  
 hypergeometric function, 139, 159, 167  
 idempotent conversion, 123  
 IEEE 754 standard, 79, 121  
   extension of, 187  
 IEEE 854 standard, 121  
 iff, xiv  
 infinity,  $\infty$ ,  $\pm\infty$ , 82  
 INRIA, xi  
 integer  
   notation for, xv  
 integer division  
   notation for, xiv  
 integer sequences, 190  
 interval arithmetic, 188, 190  
 inversion  
   batch, 78  
   modular, 32, 65–68, 76  
 Iordache, Cristina S., 121  
 ISC, 190  
 Ispiryan, Karen R., 40  
 Jacobi symbol, 43, 46  
   notation for, xiv  
   subquadratic algorithm, 43, 46  
 Jacobi, Carl Gustav Jacob, 43  
 Jebelean, Tudor, 45, 46  
 Johnson, Jeremy Russell, 121  
 Jones, William B., 180  
 Jullien, Graham A., 78  
 Kahan, William Morton, 123  
 Kaihara, Marcelo Emilio, 77  
 Kanada, Yasumasa, 162, 181  
 Kaneko, Masanobu, 181  
 Karatsuba's algorithm, 5–6, 40, 41, 44, 62, 163  
   in-place version, 40  
   threshold for, 40  
 Karatsuba, Anatolii Alekseevich, 41, 44, 62, 96  
 Karp, Alan Hersh, 22, 45, 122, 179  
 Karp–Markstein trick, 22, 45, 122, 179  
 Kayal, Neeraj, 45  
 Khachatryan, Gurgen H., 40, 45



- Khinchin, Aleksandr Yakovlevich, 45, 180  
 Kidder, Jeffrey Nelson, 118  
 Knuth, Donald Ervin, xi, 45, 46, 121, 122, 181  
 Koornwinder, Tom Hendrik, 183  
 Krandick, Werner, 45, 121  
 Kreckel, Richard Bernd, 185  
 Kronecker, Leopold, 44  
 Kronecker–Schönhage trick, 3, 39, 42, 44, 49, 77  
 Kulisch, Ulrich Walter Heinz, 123  
 Kung, Hsiang Tsung, 46, 179  
 Kuregian, Melsik K., 40  
 Kuz'min, Rodion Osievich, 45
- Lagrange interpolation, 6, 74  
 Lagrange, Joseph Louis, 6  
 Landen transformations, 163, 181  
 Landen, John, 163  
 Lang, Tomas, 122  
 Laurie, Dirk, 184  
 lazy algorithm, 2, 44  
 leading zero detection, 94  
 Lecerf, Grégoire, 122  
 Lefèvre, Vincent, 45, 120, 121  
 Legendre, Adrien-Marie, 158, 184  
 Lehmer, Derrick Henry, 30, 45, 183  
 Lehmer–Gabcke sequence, 183  
 Lenstra, Arjen Klaas, 44  
 Lenstra, Hendrik Willem, Jr., 45  
 level-index arithmetic, 120  
 lg, *see* logarithm  
 LGPL, 186, 187  
 Lickteig, Thomas Michael, 123  
 lists versus arrays, 84  
 little *o* notation, xv  
 ln, *see* logarithm  
 Loan, *see* Van Loan  
 log, *see* logarithm
- log<sub>1p</sub>, *see* logarithm  
 Logan, Benjamin Franklin “Tex”, Jr., 181  
 logarithm  
   addition formula, 133  
   computation via AGM, 159  
   lg(*x*), ln(*x*), log(*x*), xv  
   log<sub>1p</sub>, 140, 172  
   notations for, xv  
   Sasaki–Kanada algorithm, 162  
 logical operations, xv  
 LSB, 22, 24, 25, 29, 49  
 Luschny, Peter, 43  
 Lyness, James N., 184
- machine precision, xiv  
 Maeder, Roman Erich, 40  
 Magaud, Nicolas, 45  
 Magma, 188  
 mailing lists, 189  
 mantissa, *see* significand  
 Maple, 183, 188  
 Markstein, Peter, 22, 45, 122, 123, 179  
 Martin, David W., 180  
 MasPar, 44  
 Massey, James Lee, 40  
 Mathematica, 188  
 Mathematics Genealogy Project, xi  
 matrix multiplication, 41, 123  
 matrix notation, xv  
 Matula, David William, 121  
 Maze, Gérard, 45  
 MCA, 77  
 McLaughlin’s algorithm, 57, 58, 63–65, 77  
   polynomial version, 77  
 McLaughlin, Philip Burtis, Jr., 40, 63, 77  
 McMillan, Edwin Mattison, 184

- Menezes, Alfred John, 78  
 Ménissier-Morain, Valérie, 120  
 Mezzarobba, Marc, xi, 178  
 Microsoft, 186  
 middle product, 22, 41, 99  
 Mihailescu, Preda V., 77  
 Mikami, Yoshio, 45  
 Miller's algorithm, 154, 175, 180  
 Miller, Jeffrey Charles Percy, 154, 180  
 Miller, William C., 78  
 mod notation, xiv  
 modular  
   addition, 50  
   division, 65  
   exponentiation, 68–73, 78  
     base  $2^k$ , 70  
   inversion, 32, 65–68, 76  
   multiplication, 58–65  
   splitting, 142  
   subtraction, 50  
 modular arithmetic  
   notation for, xiv  
   special moduli, 65, 78  
 modular representation, 73  
   comparison problem, 75  
   conversion to/from, 73  
   redundant, 75  
   sign detection problem, 75  
 Moenck, Robert Thomas, 45, 78  
 Moler, Cleve Barry, 184  
 Möller, Niels, 42, 43, 46, 78  
 Montgomery's algorithm, 58  
 Montgomery's form, 48, 60  
 Montgomery multiplication, 60–63  
   subquadratic, 62  
 Montgomery reduction, 25, 49  
 Montgomery, Peter Lawrence, 42, 48, 77, 78  
 Montgomery–Svoboda algorithm, 49, 61–63, 76, 77  
 Mori, Masatake, 184  
 MP, 179–181, 187  
 MPC, 187, 188  
 MPFI, 188  
 MPFQ, 186  
 MPFR, 187, 188  
 MPIR, 186  
 MSB, 21, 22, 24, 25, 29, 49  
 Mulders, Thom, 96, 119, 121  
 Muller, Jean-Michel, xi, 121–123, 179  
 multiplication  
   by a constant, 13  
   carry bit, 40  
   complex, 163  
   FFT range, 8  
   Fürer's algorithm, 78  
   Karatsuba's algorithm, 163  
   modular, 58–65  
   of integers, 3–45  
   of large integers, 58  
   Schönhage–Strassen, 49  
   schoolbook, 5  
   short product, 95  
   time for,  $M(n)$ , xiv  
   unbalanced, 8–11, 41  
     complexity of, 11  
   via complex FFT, 98  
 multiplication chain, 69  
   weighted, 77  
 Munro, (James) Ian, 78  
 NaN, 82  
   quiet, 82  
   signaling, 82  
 nbits, xv  
 nearest integer function  $\lfloor x \rfloor$ , xv  
 Neumann, Carl Gottfried, 153

- Newton's method, 21, 25, 26, 49, 66, 102, 114, 125–132, 179  
   for functional inverse, 130, 139  
   for inverse roots, 127  
   for power series, 129  
   for reciprocal, 128  
   for reciprocal square root, 129  
   higher-order variants, 131  
   Karp–Marstein trick, 179  
    $p$ -adic (Hensel lifting), 22  
 Newton, Isaac, 21, 49, 102, 125  
 Nicely, Thomas R., 128  
 NIST, 78  
 NIST Digital Library, 190  
 normalized divisor, 14  
 Not a Number (NaN), 82  
 Nowka, Kevin John, 121  
 NTL, 189  
 numerical differentiation, 184  
 numerical instability  
   in summation, 138  
   recurrence relations, 155  
 numerical quadrature, *see* quadrature  
 Nussbaumer, Henri Jean, 78  
  
 odd zeta-function, 157  
 odd–even scheme, 9, 45, 142, 171  
 Odlyzko, Andrew Michael, 183  
 Odlyzko–Schönhage algorithm, 183  
 OEIS, 190  
 off-line algorithm, 2, 44  
 Olivier, Michel, 189  
 Olver, Frank William John, 120, 180  
 Omega notation  $\Omega$ , xv  
 on-line algorithm, 44  
 Oorschot, *see* van Oorschot  
 ord, xv  
 Osborn, Judy-anne Heather, xi  
  
 Paar, Christof, 41  
  
 $p$ -adic, 49  
 Pan, Victor Yakovlevich, 122  
 Papanikolaou, Thomas, 182, 184  
 PARI/GP, 189  
 Patashnik, Oren, 181  
 Paterson, Michael Stewart, 180  
 Patterson, David Andrew, 121  
 Payne and Hanek  
   argument reduction, 101, 122  
 Payne, Mary H., 101, 122  
 Pentium bug, 128, 179  
 Percival, Colin Andrew, 78, 119, 122  
 Pétermann, Yves-François Sap-  
   phorain, 183  
 Petersen, Vigdis Brevik, 180  
 phi function  $\phi$ , xiv  
 $\pi$ , 184  
   Brent–Salamin algorithm, 159, 181  
   Chudnovsky series, 184  
   Gauss–Legendre algorithm, 159  
   record computation, 184  
 Pila, Jonathan S., 45  
 Plouffe, Simon, 190  
 Pollard, John Michael, 77, 78  
 polylogarithm, 183  
 polynomial evaluation, 141  
 Pomerance, Carl, 44  
 power  
   computation of, 69  
   detection of, 28, 45  
 power series  
   argument reduction, 140  
   assumptions re coefficients, 139  
   backward summation, 135, 137, 138  
   direct evaluation, 140  
   forward summation, 135, 137, 138  
   radius of convergence, 139  
 precision, xiv  
   local/global, 84

- machine, 137
- operand/operation, 84, 121
- reduced, 162
- working, 90, 137
- Priest, Douglas M., 86, 121
- product tree, 67
- pseudo-Mersenne prime, 65, 78
- $PV\int$ , *see* Cauchy principal value
- Python, 189
- quadrature
  - Clenshaw–Curtis, 184
  - contour integration, 169
  - Gaussian, 184
  - numerical, 184
  - Romberg, 184
  - tanh-sinh, 184
- Quercia, Michel, 40, 41, 122
- Quisquater, Jean-Jacques, 77
- quotient selection, 16, 18, 61
- Rader, Charles M., 78
- radix, xiv, 79–81
  - choice of, 80
  - mixed, 83
  - radix ten, 114
- rational reconstruction, 37
- reciprocal square root, 112, 129
- rectangular series splitting, 141–144, 180
- recurrence relations, 152
- REDC, 60, 77
- redundant representation
  - for error detection/correction, 75
  - for exponentiation, 73
  - for modular addition, 48
- Reinsch, Christian, 180
- relaxed algorithm, 2, 44
- relaxed multiplication, 76
- remainder tree, 43, 67
- Rémy, Jean-Luc, 183
- residue class representation, 47
- residue number system, 48, 73, 77
- Reyna, Juan Arias de, 183
- Richardson extrapolation, 184
- Richardson, Lewis Fry, 184
- Riemann Hypothesis
  - computational verification, 183
- Riemann zeta-function, 147, 184
  - at equally spaced points, 183
  - at even integers, 157
  - Bernoulli numbers, 157
  - Borwein’s algorithm, 183
  - error analysis, 183
  - Euler–Maclaurin expansion, 147, 183
  - odd zeta-function, 157
  - Odlyzko–Schönhage algorithm, 183
  - Riemann–Siegel formula, 183
- Riemann, Georg Friedrich Bernhard, 147
- Rivest, Ronald Linn, 68
- Rix, Anne, xi
- RNS, *see* residue number system
- Robertson, James Evans, 179
- Roche, Daniel Steven, 40
- Roegel, Denis, xi
- Romberg quadrature, 184
- Romberg, Werner, 184
- root
  - $k$ th, 27
  - Goldschmidt’s iteration, 123
  - inverse, 127
  - principal, 50
  - square, 25–26, 111
    - complex, 123, 182
    - paper and pencil, 25
    - wrap-around trick, 114
- Rosser, John Barkley, 183

- rounding
  - away from zero, 87
  - boundary, 86
  - correct, 85, 137
  - double, 90
  - mode, 87, 121
  - notation for, xiv
  - probabilistic, 87
  - round bit, 88, 92
  - sticky bit, 88, 92, 121
  - stochastic, 87
  - strategies for, 90
  - to nearest, 82, 87–90
    - balanced ternary, 119
  - to odd, 118
  - towards zero, 87, 118
  - Von Neumann, 118
- rounding mode  $\circ$ , 85–91
- Roy, Ranjan, 179, 180
- RSA cryptosystem, 68
- runs of zeros/ones, 121
- Ryde, Kevin, 40
  
- Sage, 189
- Salamin, Eugene, 181, 184
- Salvy, Bruno, 178
- Sasaki, Tateaki, 162, 181
- Saxena, Nitin, 45
- Schmid, Wolfgang Alexander, xi
- Schmookler, Martin S., 121
- Schönhage, Arnold, xi, 43, 44, 46, 122, 171, 180, 182, 183
- Schönhage–Strassen algorithm, 49, 55, 65, 78, 105, 122, 185
- Schost, Éric, 122, 171
- Schroeppel, Richard Crabtree, 181
- Sebah, Pascal, 184
- secant numbers, 157, 177
- Sedjelmaci, Sidi Mohamed, xi
- Sedoglavic, Alexandre, 42
- segmentation, *see* Kronecker–Schönhage trick
- Sergeev, Igor S., 182
- Shallit, Jeffrey Outlaw, 46
- Shamir, Adi, 68
- Shand, Mark Alexander, 45
- Shokrollahi, Mohammad Amin, 41, 123
- short division, 121
- short product, 62, 95–98, 121
- Shoup, Victor John, 43, 189
- Sieveking, Malte, 179
- sign, xv
- sign-magnitude, 2, 47, 84, 91
- significant, 79, 83
- $\sin(x)$ , 133
- $\sinh(x)$ , 136
- sliding window algorithm, 72
- Sloane, Neil James Alexander, 190
- Smith’s method, *see* rectangular series splitting
- Smith, David Michael, 180
- software tools, 185
- Sorenson, Jonathan Paul, 31, 46, 77, 78
- special function, 125–184, 190
- special moduli, 65, 78
- splitting
  - classical, 142
  - modular, 142
- square root, *see* root
- squaring, 11, 41
  - complex, 163
- SRT division, 126, 128, 179
- Staudt, Karl Georg Christian von, 156, 181
- Steel, Allan, 44
- Steele, Guy Lewis, Jr., 123
- Stegun, Irene Anne, 179, 180, 190
- Stehlé, Damien, 43, 46

- Stein, Josef, 45  
 Stein, William Arthur, 189  
 Sterbenz's theorem, 94, 121  
 Sterbenz, Pat Holmes, 94, 121  
 sticky bit, 88, 121  
 Stirling numbers, 174, 181  
 Stirling's approximation  
   convergent form, 174  
   for  $\ln \Gamma(iy)$ , 174  
   for  $\ln \Gamma(x)$ , 149  
   for  $\ln \Gamma(z)$ , 147  
   for  $n!$  or  $\Gamma(z)$ , 134, 137, 138, 147,  
     177, 184  
   with error bounds, 146  
 Stirling, James, 134  
 Stockmeyer, Larry Joseph, 180  
 Stoer, Josef, 184  
 Strassen's algorithm, 36  
 Strassen, Volker, 36, 123  
 strings  
   concatenation, xvi, 38  
 subnormal numbers, 82  
   smallest, xiv  
 substitution, *see* Kronecker–  
   Schönhage trick  
 subtraction, 2, 91  
   guard digits, 94  
   leading zero detection, 94  
   modular, 50  
 summation  
   backward, 135, 138  
   forward, 135, 138  
 Svoboda's algorithm, 17, 23, 42, 45,  
   49, 61, 63, 77  
 Svoboda, Antonin, 45, 49  
 Swartzlander, Earl E., Jr., 78, 179  
 Sweeney, Dura Warren, 179
- Tables  
   Table 2.1, 49  
   Table 2.2, 63  
   Table 3.1, 89  
   Table 3.2, 93  
   Table 3.3, 100  
   Table 4.1, 164
- Takagi, Naofumi, 77  
 Takahasi, Hidetosi, 184  
 $\tan(x)$ , 133, 155  
 tangent numbers, xiii, 156, 176, 181  
   algorithm for, 156  
   complexity of evaluation, 177  
   space required for, 176  
 Tellegen's principle, 122  
 Temme, Nico M., 179, 183  
 tensor rank, 41, 123  
 ternary system, 119  
 theta functions, 160  
 Theta notation  $\Theta$ , xv  
 Théveny, Philippe, 187  
 Thomé, Emmanuel, xi, 40, 41, 184,  
   186  
 Tocher, Keith Douglas, 179  
 Toom, Andrei Leonovich, 44  
 Toom–Cook multiplication, 6–7, 41  
   time for, 7  
 totient function, xiv  
 Traub, Joseph Frederick, 179  
 Trefethen, (Lloyd) Nicholas, 184  
 tripling formula  
   for  $\sin$ , 133  
   for  $\sinh$ , 136  
   in FFT range, 136, 180
- Ullman, Jeffrey David, 46, 78  
 unbalanced multiplication, 8–11, 41  
 unit in the last place (ulp), xiv, 80, 87  
 unrestricted algorithm, 121, 125  
   for *exp*, 180
- Vallée, Brigitte, 46

- valuation, xiv  
 van der Hoeven, Joris, 44, 76, 122, 178, 182, 183  
 Van Loan, Charles Francis, 78  
 van Oorscot, Paul Cornelis, 78  
 Vandermonde matrix, 7  
 Vanstone, Scott Alexander, 78  
 vectors, notation for, xv  
 Vepštas, Linas, 183  
 Verdonk, Brigitte, 180  
 Vetter, Herbert Dieter Ekkehart, 122, 182  
 Vidunas, Raimundas, 183  
 Von Neumann, John (János Lajos), 118  
 Von Staudt–Clausen theorem, 156, 181  
 von zur Gathen, Joachim, 77  
 Vuillemin, Jean Étienne, 41, 45  
  
 Waadeland, Haakon, 180  
 Wagon, Stanley (Stan), 184  
 Waldvogel, Jörg, 184  
 Wall, Hubert Stanley, 180  
 Wang, Paul Shyh-Horng, 46  
 Watson, George Neville, 180  
 Weber functions,  $Y_\nu(x)$ , 153  
 Weber, Heinrich Friedrich, 153  
  
 Weber, Kenneth, 46  
 Weimerskirch, André, 41  
 Wezelenburg, Mark, xi  
 White, Jim, 172  
 White, Jon L., 123  
 Whittaker, Edmund Taylor, 180  
 Wilkinson, James Hardy, 121, 179, 180  
 Winograd, Shmuel, 78  
 Wolfram, Stephen, 188  
 Wong, Roderick, 180  
 wrap-around trick, 60, 105  
  
 Yap, Chee-Keng, 46  
  
 Zanoni, Alberto, 44  
 zealous algorithm, 44  
 Zeilberger, Doron, 183  
 zero,  $\pm 0$ , 82, 84  
 $\zeta(3)$ , 184  
 Ziegler, Joachim, 45  
 Zima, Eugene, 184  
 Zimmermann, Marie, xi  
 Zimmermann, Paul Vincent, 45, 46, 122, 184, 187  
 Ziv's algorithm, 86  
 Zuras, Dan, 41, 44