

---

# Index

- Abelian group, 177  
Additive function, 35  
Adleman, L. M., xi, 4, 104, 108, 234  
Agrawal, M., 69, 70, 73  
Alford, W., 65, 201  
Algebraic  
  factor, 50, 56, 57  
  number, 208  
  part, 50, 56  
Aliquot sequence, 99–101, 118, 134  
American Mathematical Society,  
  114, 115  
Amicable pairs, 100  
Amortize, 120, 125, 137, 140, 186,  
  197  
Aristotle, 101  
Arithmetic function, 33–36  
Arnold, V. I., 150  
Associative law, 177  
Atkin, A. O. L., 141, 142, 187, 188,  
  239  
Atkins, D., 5, 115, 201  
Aurifeuille, L. F. A., 77  
Aurifeuillian factorization, 76–82,  
  92, 99, 116, 117, 189, 216, 218  
  
Bach, E., 24, 46, 63  
Bai, S., 216  
Baillie, R., xiv, 68, 72, 140, 141  
Bang’s Theorem, 53, 82, 85  
  
Bang, A. S., 53  
Batalov, S., 218  
Bateman, P. T., 98  
Beach, B. D., 150  
Bell number, 98, 118  
Bell, E. T., 98, 114  
Bernoulli numbers, 101–104, 118,  
  216  
Bernoulli, J., 102  
Bernstein, D. J., 70  
Big O notation, 13  
Birthday problem, 135, 162  
Bliss, N., 49  
Block Lanczos, 202  
Block Weidemann, 202  
Blum, L., 109  
Blum, M., 109  
Boneh, D., 190, 250, 253, 261  
Brahmagupta, 169  
Brent, R. P., xiii, 78, 88, 97, 138,  
  140, 141, 186, 207, 244, 246,  
  262  
Brillhart, J., 58, 158, 159, 162, 207,  
  262  
Browne, M. W., 115  
Buell, D. A., 141, 163  
Buhler, J. P., 103, 212  
Burckhardt, J. C., 119  
Burt Laboratories, 224  
Butterfly net, 158

- Canfield, E., 43  
 Carissan, P., 222  
 Carmichael  
   lambda function, 35, 71  
   number, 64, 72, 113, 248, 249,  
   265, 267  
 Cataldi, P., 8, 119  
 Ceiling function, 13  
 CFRAC, 160  
 Chang, W.-L., 234  
 Characteristic polynomial, 94  
 Chebyshev, P., 132  
 Chen, J., xiv  
 Chernac, L., 119  
 Childers, G., xiii, 216, 217  
 Chinese Remainder Theorem,  
   26–28, 31, 33, 36, 64, 106, 107,  
   109, 110, 154, 253  
 Clausen, T., 262  
 Cocks, C., 5  
 Cohen, G. L., xiii, 87, 88  
 Cole, F. N., 98, 114  
 Complexity  
   of AKS primality test, 69  
   of BPSW primality test, 69  
   of Elliptic Curve Method, 184  
   of Euclidean Algorithm, 18  
   of Fermat's Method, 126  
   of Number Field Sieve, 213  
   of Pollard Rho, 137  
   of Quadratic Sieve, 197  
   of the CFRAC, 159  
   of the SQUFOF, 168  
 Composite number, 20  
 Congruence, 24–28  
 Continued fraction, 144, 158  
   algorithm, 144  
   periodic, 149–153  
 Continued Fraction Factoring  
   Algorithm, 158–163, 195, 230,  
   262, 263  
 Coppersmith, D., 202, 251, 260, 261  
 Coron, J.-S., 258  
 Crandall, R., 46, 67, 207, 213  
 Cray-1 computer, 115  
 Crelle, A. L., 119  
 Cryptography, public-key, 2–5  
 Cunningham Project, 7, 9–12, 49,  
   76  
 Cunningham table, 81, 82, 91–93,  
   117, 141  
 Cunningham, A. J. C., 9, 115  
 Davis, J., 115  
 Davis, L., 264  
 de Bruijn function, 43  
 Decimals, repeating, 6–8  
 de la Vallée Poussin, C., 23  
 Delay Line Sieve, 227  
 DES, 2  
 Deterministic algorithm, 15  
 Deuring, M., 181  
 deVogelaere, R., 93  
 Dickman, K., 43  
 Dickson, L. E., 8, 9, 101  
 Difference of Squares Factoring  
   Algorithm, 124  
 Diffie, W., 2, 4, 108  
 Digital signature, 4, 108–109  
 Discrete logarithm, 32–33, 108  
 Discriminant, 175, 178  
 Divisibility, 17–20  
 Divisibility sequence, 49–55, 71,  
   216  
 Dixon, J. D., 241  
 DNA computing, 234–236  
 Dodson, B., 186  
 Double Sieve, 202  
 DSH, factoring device, 237  
 Dubner, H., 92, 138, 232  
 Dubner, R., 232  
 Durfee, G., 261  
 ECM, 181  
 ECM, second stage of, 186  
 Elliptic curve  
   discrete logarithm problem, 189  
   method, 79, 181, 231, 232, 236,  
   241, 246, 247, 262, 263, 267  
   pairing, 189  
   point addition, 177  
   prime proving, 187  
   supersingular, 189  
 Ellis, J., 5  
 EPOC, factoring machine, 230

- Equivalence relation, 24  
Eratosthenes, 119  
Erdős, P., 23, 63, 103, 139  
Estibals, N., 190  
Euclid, 8, 21, 83  
Euclidean Algorithm, 18–20, 145  
Euler  
  and perfect numbers, 83–86, 89  
  constant, 98  
  Criterion, 38, 45, 46, 63, 111  
  phi function, 31, 33  
  Theorem, 31, 36, 60, 105, 251  
Euler, L., 8, 31, 83, 84, 121, 132, 262  
Exponential time, 14  
Extended Euclidean Algorithm, 25, 26, 28, 36, 104, 179, 216, 246, 251  
  
Factor base, 159, 162, 202  
Factor chain method, 85  
Factors of  $b^m + 1$ , 55–56  
Factors of  $b^m - 1$ , 49–55  
Fast Exponentiation Algorithm, 29, 30, 46, 58, 64, 70, 97, 105, 109, 139, 179, 245, 251, 253, 265  
Fast Point Multiplication, 180, 185  
Feitsma, J., 68  
Fermat  
  Factoring Method, 106, 123–128, 130, 132, 141, 147, 221  
  Last Theorem, 104  
  Little Theorem, 28, 29, 31, 63, 64, 66, 123, 138, 227  
  number, 59, 62, 63, 140–142, 207, 231, 262  
  sum of two squares, 114  
Fermat, P., 28, 114, 123, 125, 128, 132, 142  
Fibonacci number, 18, 56–58, 68, 145, 216  
Filtering, 202  
Floor function, 13  
Floyd, R. W., 136  
Franke, J., 237  
Franklin, M., 190  
Full rank lattice, 255  
Fundamental solution, 169  
  
Fundamental Theorem of Arithmetic, 21  
  
Galois, E., 150  
Gardner, M., 4  
Gauss, C. F., ix, 7, 23, 121, 132  
Geiselmann, W., 237  
Generating function, 95  
Genetic algorithm, 264, 266  
Gérardin, A., 227  
Gilchrist, J., 68  
Goldwasser, S., 68, 187  
Golomb, S. W., 93, 97  
Goto, T., 89, 90  
Gower, J., 166, 168  
Graff, M., 5, 115, 201  
Gram-Schmidt process, 254  
Granville, A., 65, 78  
Greatest common divisor, 17  
Guy, R., 89, 101  
  
Hadamard, J., 23  
Hamming, R. W., 75  
Hardy, G. H., 13, 23  
Harmonic  
  mean, 88  
  number, 88–91  
Hart, W. B., 97, 127, 128, 142, 217  
Harvey, D., 103  
Hasse  
  interval, 181, 182, 184, 188, 241  
  Theorem, 180, 181, 187  
Hasse, H., 180  
Hellman, M., 2, 4, 33, 108  
Hensel's Lemma, 47, 195  
Hensel, K. W. S., 47  
Holdridge, D., 115  
Howgrave-Graham, N., 257  
  
Iamblichus, 100  
Index = discrete logarithm, 32  
Integer square root, 124  
Intrinsic factor, 50, 52, 53, 56, 57, 72, 80, 82, 141  
  
Jacobi  
  sum of four squares, 113  
  symbol, 38, 110, 246, 265, 267  
Jacobi, C. G. J., 113

- Jeopardy!*, ix, xiv
- Kac, M., 23
- Kanold, H.-J., 90
- Kayal, N., 69, 70, 73
- Kida, Y., 49
- Kilian, J., 68, 187
- Kleijung, T., 217, 237
- Knuth, D. E., 29, 43, 48, 159, 244
- Kobayashi, M., 49
- Koblitz, N., 173, 184
- Kolata, G., 115
- Korselt's Theorem, 65, 72, 249, 267
- Korselt, A., 65
- Kraitchik, M., 143, 162, 196
- Kruppa, A., 97, 140
- Lamé, G., 18
- Landry, F., 76, 77, 262
- Las Vegas algorithm, 15, 59, 240
- Lattice, 255
- Law of Quadratic Reciprocity, 38, 62, 121, 122
- Lawrence, F. W., 128, 129, 142, 222
- Least common multiple, 17, 95
- Legendre symbol, 37, 66, 111, 180, 196, 197, 229
- Legendre, A. M., 37, 132, 153
- Lehman, R. S., 129–131, 141, 142, 240
- Lehmer, D. H., 11, 60, 63, 101, 126, 133–135, 155, 158, 162, 223–228, 246
- Lehmer, D. N., 119, 135, 191, 224, 226
- Lehmer, E., 133, 134
- Lehmers' Factoring Method, 132–135, 169, 228
- Lenstra, A. K., xiv, 5, 115, 201, 207, 232, 237, 253, 256, 262
- Lenstra, H. W., Jr., 1, 173, 181, 182, 207, 212, 242, 256
- Levesque, W. J., 150
- Leyland, P. C., 5, 115, 201
- Linear feedback shift register, 93–97, 117
- Linear recurrence relation, 57
- Lipton, R. J., 234
- Loeff, W., 9
- Lovász, L., 256
- Lucas number, 57, 72, 145
- Lucas, É., 63, 77, 78, 98
- Lucas-Lehmer Test, 63, 98
- $L(x)$ , 159, 184, 185, 197, 241, 242
- Macaulay, T. B., 226
- Manasse, M., 115, 207, 232, 262
- Mathews, G. B., 133
- May, A., 251, 258, 261
- Mazur, B., 216
- McKee, J., 132, 147–149
- Menezes, A. J., 189
- Mersenne  
     number, 59, 63, 123, 126, 216  
     prime, 9, 12, 89, 97, 98
- Mersenne, M., 8, 98, 115, 132
- Miller, G. L., 67
- Miller, V., 173
- Mod Squad, 230
- Modulus of a congruence, 24
- Möbius  
     function, 34  
     inversion formula, 35, 48
- Monier, L. M. G., 67
- Monte Carlo algorithm, 15, 67, 136
- Montgomery, H. L., 13
- Montgomery, P. L., 58, 186, 202, 210, 212, 245
- Morain, F., 187, 188
- Morimoto, M., 49
- Morrison, M. A., 158, 159, 162, 207, 262
- Morton, P., 227
- Multiplicative function, 33
- Murphy, B., 212
- Nagell, T., 50
- New York Times*, 115
- Newton's method, 47, 124, 153
- Nielsen, P. P., 9, 88
- Niven, I., 13
- $\mathcal{NP}$  complete, 14
- $\mathcal{NP}$  complexity class, 14
- Number Field Sieve, 33, 105, 207–217, 232, 236, 237, 247, 262, 263, 267

- Ochem, P., 9, 88  
 Okamoto, T., 189  
 Okeya, K., 89, 90  
 One-way function, 3  
 Ore, O., 89
- Paar, C., 237  
 Paper strips as sieve, 222  
 Partial fraction decomposition, 95  
 Pell's equation, 169  
 Pell, J., 169  
 Pelzl, J., 237  
 Pepin, T., 62, 72  
 Perfect number, 8–9, 83–88  
 Pleasants, P., 78  
 Pocklington Theorem, 61, 68, 92, 187, 247  
 Pocklington, H. C., 61  
 Pohlig, S., 33  
 Pollard Rho Method, 135–138, 142, 207, 231, 232, 247, 262, 263  
 Pollard, J. M., xii, 135, 138, 207, 240, 262  
 Pollard  $p - 1$  Method, 106, 138–142, 173, 181, 186, 231, 263  
 Polynomial  
   cyclotomic, 47–49, 71  
   irreducible, 47, 96  
   primitive, 95–97  
   self-reciprocal, 71  
   time, 14, 33, 110, 154, 234, 243, 250, 262, 267  
 Pomerance, C., xiii, 46, 60, 64, 65, 67, 68, 72, 159, 192, 197, 201, 207, 212, 213, 231, 242  
 Powers, R. E., 155, 158, 162  
 $p + 1$  Method, 141  
 Pratt, V. R., 61  
 Primality testing, 59–71  
 Prime  
   factor, primitive, 6  
   irregular, 103  
   number, 20  
   Number Theorem, 23, 148, 185  
   proving, 60–62, 91–93  
   regular, 103  
 Primitive  
   part, 50, 53, 55, 56, 72, 77, 81  
   polynomial, 93, 96, 97  
   prime factor, 6, 7, 10, 11, 50, 53, 56, 57, 82, 85, 123  
   root, 32, 33, 38, 60, 61, 63  
   root of unity, 48  
 Priplata, C., 237  
 Probabilistic algorithm, 15  
 Probable prime, 63, 188  
 Probable prime, strong, 66  
 Pseudocode, 15  
 Pseudoprime, 63, 72, 248, 265, 266, 268  
 Pseudoprime, strong, 66, 72, 80, 248, 265, 266, 268  
 Pseudosquare, 64, 229  
 Public-key cipher, 3, 4, 104–108
- Quadratic  
   congruence, 36  
   form, 132, 134, 163, 170, 240, 242  
   formula, 36  
   nonresidue, 37, 45, 46, 62, 63, 71, 110, 190  
   polynomial, 136, 149, 174, 196  
   residue, 37, 44–46, 106, 107, 110, 121–123, 143, 151, 154, 159, 180, 221  
   Sieve, 33, 115, 195–202, 207, 231, 232, 236, 247, 263  
   surd, 149  
 Quantum computing, 232–234, 257
- Rabin, M. O., 67, 106, 108  
 Rahn, J. H., 169  
 Ramanujan, S., 23  
 Ramaswami, V., 43  
 Random number generation, 109–111  
 Rao, M., 9, 88  
 Relation  
   full, 198  
   partial, 198  
 Repunit, 5–6, 12, 71, 92  
 Reuschle, K. G., 9  
 Rickert, N., 141  
 Riemann Hypothesis, Extended, 46, 67, 240

- Riesel, H., 78, 79, 122  
 Rivest, R., xi, 4, 104, 108  
 Root of unity, primitive, 48  
 Rosen, K. H., 67  
 RSA cipher, 4, 5, 104–106, 242,  
     250, 253, 268  
  
 Saito, M., 49  
 Sandia National Labs, 115  
 Sassoon, G., 201  
 Saxena, N., 69, 70, 73  
 Schinzel, A., 78, 80, 82  
 Schoof, R., 188  
 Schroepfel's Linear Sieve, 205–207  
 Schroepfel, R., xiv, 127, 159, 205,  
     265  
*Scientific American*, 115  
 Selfridge, J. L., 61, 68, 72, 101  
 Sequence, divisibility, 49–55, 71  
 Shallit, J., 46, 63  
 Shamir, A., xi, 4, 104, 108, 236,  
     242, 243, 265, 267  
 Shanks, D., 46, 163, 168, 240  
 Shark, factoring device, 237  
 Shor, P., 232, 257, 267  
 Shub, M., 109  
 Siegel, C. L., 104  
 Sieve devices, 126, 134, 219–230  
 Sieve of Eratosthenes, 139,  
     192–195, 217  
 Silverman, J. H., 174  
 Silverman, R. D., 58, 141, 186, 201  
 Simmons, G., 115  
 Size of an elliptic curve modulo  $p$ ,  
     180  
 Smith, J. W., 230, 231  
 Smooth integer, 43–44, 139, 158,  
     184, 203, 205, 213, 264  
 Sociable numbers, 100  
 Square root modulo  $p$ , 44–47, 110  
 Square-free integer, 34  
 SQUFOF, 163–168, 266  
 Stahlke, C., 237  
 Standard factorization, 21  
 Stars in Cunningham table, 50  
 Steinwandt, R., 237  
 Strassen, V., 240  
 Subexponential time, 14, 33  
  
 Sum of  
     divisors function, 33  
     four squares, 113  
     two squares, 114  
 Suyama, H., 141, 186, 231  
 Sylvester, J. J., 52  
  
 Tate, J., 174  
 Ten Most Wanted List, 141  
 Thomason Civil Engineering  
     College, 9  
 Thomé, E., 217  
*Time* magazine, 115  
 Tonelli, A., 45  
 Touchard, J., 99  
 Tower of Hanoi problem, 57  
 Trabb Pardo, L., 43  
 Trappe, W., 174, 190  
 Trebek, A., x, xiv  
 Trial Division, 42, 79, 120–123,  
     127, 135, 137, 141, 148, 151,  
     159, 196, 230, 231, 236, 240,  
     241, 247, 262, 263, 267  
 Tromer, E., 236  
 Truman, H., 2  
 Tuler, R., 231  
 Twinkle, factoring device, 236  
 TWIRL, factoring device, 236  
  
 van der Waerden, B. L., 48  
 Vandersypen, L. M. K., 234  
 Vang, M., 140  
 Vanstone, S. A., 189  
 von Staudt–Clausen Theorem, 103  
  
 Wagstaff, S. S., Jr., 18, 46, 72, 103,  
     166, 168, 186, 230, 231  
 Washington, L. C., 103, 174, 181,  
     190  
 Weaver, R., xiii  
 Weierstrass form, 174  
 Weil pairing, 190  
 Weintraub, S. H., 48  
 Wheel, 121  
 Wiener, M. J., 251, 262  
 Wiles, A., 104  
 Williams, G. T., 99  
 Williams, H. C., xiv, 57, 92, 106,  
     108, 126, 141, 150, 228, 229

- Woodall, H. J., 10, 115
- Wright, E. M., 13
- Wunderlich, M. C., 62, 187
  
- Xu, N., 234
  
- YASD, factoring device, 237
  
- Zero-knowledge proof, 111–113, 249
- Zimmermann, P., 97, 140, 186, 217,  
244, 246
- Zsigmondy, K., 50
- Zuckerman, H. S., 13