

---

# Index

- abundant number, 1, 140
- Adleman, Leonard, 99
- affine cipher, 93
  - frequency analysis, 94
  - using encryption key, 95
- algebraic integer, 148
  - irreducible, 149
  - prime, 149
  - see also* algebraic number
- algebraic number
  - algebraic integer, 148
  - characteristic polynomial, 144
  - degree, 144
  - fundamental unit, 203
  - Liouville's approximation theorem, 164
  - multiple factorizations, 146
  - norm, 146
  - Roth's approximation theorem, 166
  - unit, 149
- Algorithm, 3
  - Best Rational Approximation, 180
  - Chinese Remainder Theorem, 57
  - Continued Fraction Expansion, 170
  - Diffie–Hellman Key Exchange, 97
  - Digital Signature with Hash Function, 102
  - Digital Signature with RSA, 100
  - Divisibility test, 9
  - Division Algorithm, 9
  - Encryption with Affine Cipher, 94
  - Euclidean Algorithm, 16
  - Euler Factorization, 37
  - Extended Euclidean Algorithm, 18
  - Fermat Factorization, 36
  - Fundamental Solution to Pell's Equation, 207
  - Inverse from the Euclidean Algorithm, 46
  - Lucas–Lehmer Primality Test, 37
  - m*th Roots, 81
  - Pollard rho, 37
  - Rational Periodic Points by Good Reduction, 267
  - Rational Preperiodic Points by Good Reduction, 268
  - RSA Public Key, 99
  - Secret Sharing with Mignotte Sequences, 104
  - Sieve of Eratosthenes, 25
  - Torsion Subgroup, 236
  - Trial Division, 3, 36
- aliquot sequence, 140
- aliquot sum, 126, 140
  - abundant number, 140
  - deficient number, 140
  - perfect number, 128
- almost perfect number, 140
- almost prime, 35
- amicable pair, 139
- approximation, best, *see* best approximation
- arithmetic axioms, 5
- arithmetic function, 109
  - Euler totient function, 109–113
  - Möbius function, 113–117
  - number of distinct prime divisors, 122

- number of distinct prime factors, 128, 140
- partition function, 130–134
- sum of divisors function, 122–125
- Arithmetic Mean–Geometric Mean, 175
- arithmetic progression, 32
  - primes in, *see* Dirichlet’s theorem
- asymmetric cipher, 98
- asymptotic functions, 26
- bad reduction, 260
- Bang–Zsigmondy Theorem, 29
- best approximation
  - first kind, 159
  - first kind for  $\pi$ , 162
  - second kind, 171
  - second kind are convergents, 178
- Blum, Manuel, 107
- Brahmagupta, 202
- Brouncker, William, 202
- canonical height, 274
- Cantor, Georg, 144, 158
- Carmichael function, 60, 63, 88, 89
- Carmichael number, 1, 48, 58, 61, 62, 135
- Catalan equation, 214
- character frequency, 94, 96
- characteristic polynomial, 144
- Chaum, David, 103
- Chebyshev polynomials, 290
- check digit, 102
- Chinese Remainder Theorem, 54
  - solving Diophantine equations, 191
- cipher, 92
  - affine, 93
  - asymmetric, 98
  - Diffie–Hellman key exchange, 97
  - discrete log problem, 97, 228
  - NIST key size recommendations, 100
  - RSA public key, 99, 108
  - shared secret, 104, 108
  - symmetric, 96
  - Vigenère, 95
- complete systems of residues, 40
- composite number, 7
- congruent modulo  $n$ , 39
- congruent number, 218, 238
  - $t$ -congruent number, 246
  - generalizations, 246
- conjugation, 273
- continued fraction, 166, 167, 181
  - convergent, 171
  - finite, 170
  - for polynomials, 297
  - periodic, 185
  - solving quadratic equations, 186
- convergent, 171
  - as best approximations, 176
  - as solutions to Pell’s equation, 206, 297
  - error bound, 174
  - recursive formula for, 172
- counting function, 23, 160, 184
  - prime numbers, 24
- critical points, 273
- cubic reciprocity, 89
- CvHP hash function, 103
- cycle structure, 249
- cyclotomic polynomial, 117–121, 139, 144, 294
- Davis, Martin, 189
- decimal part of a number, 164, 168
- Dedekind, Julius, 150
- deficient number, 140
- degree
  - algebraic number, 144
  - polynomial, 275
  - rational function, 249
- density, 23
- descent, method of, 200
- Diffie, Whitfield, 97
- Diffie–Hellman key exchange, 97
  - with elliptic curves, 244
- digital signature, 100
- Diophantine approximation, 158–166
  - best rational approximation
    - algorithm, 179
  - by continued fractions, 171–181
  - Dirichlet’s theorem, 163, 175, 176, 204
  - Liouville number, 165
  - Liouville’s theorem, 164
  - Roth’s theorem, 166
  - simultaneous approximation, 185
- Diophantine equation
  - congruent numbers, 218
  - Fermat’s Last Theorem, *see* Fermat’s Last Theorem
  - Hasse principle, 190
  - Hensel’s Lemma, 193
  - method of descent, 200
  - modulo primes, 189–198
  - number of solutions mod  $p$ , 216

- Pell's equation, *see* Pell's equation  
 Pell-like equations, 218  
 Pythagorean triple, *see* Pythagorean triple  
 solving using Chinese Remainder Theorem, 192  
 Waring problem, *see* Waring problem  
 Diophantus, 158, 187, 209, 223  
 Dirichlet's theorem  
   arithmetic progression, 32, 191  
   Diophantine approximation, 163, 175, 176, 204  
 Dirichlet, Johann, 163  
 discrete log problem, 97  
   for elliptic curves, 228  
 discriminant, 221, 270  
 divisibility  
   for algebraic integers, 148  
   for integers, 6–9  
   for polynomials, 278  
   test modulo  $n$ , 41  
 Division algorithm, 8, 39  
   for polynomials, 279  
 divisor, 6  
 dynamical system, 247  
   algorithm to compute all rational periodic points, 267  
   algorithm to compute all rational preperiodic points, 268  
   conjugation, 273  
   finitely many bad primes, 261  
   forward orbit, 248  
   good reduction, 260  
   Lagrange interpolation, 252  
    $n$ th iterate, 247  
   period bound via good reduction, 266  
   periodic point, 248  
   Poonen's conjecture, 253  
   post-critically finite, 272  
   preperiodic point, 248  
   wandering point, 248  
 dynatomic polynomial, 254–258  
  
 Eisenstein's criteria, 277  
   generalization, 295  
 elliptic curve, 221  
   addition of points, 224–228  
   algorithm to compute the torsion subgroup, 236  
   congruent numbers, 237, 240  
   Diffie–Hellman key exchange, 244  
   discriminant, 222, 242  
   doubling function, 250  
   for polynomials, 298  
   integer points, 230–244  
   Lattès map, 272  
   Lenstra factorization, 245  
   linearly independent points, 236  
   Mazur's theorem, 235, 253  
   Mordell curve, 223, 227, 230, 236, 241, 243  
   Mordell–Weil group, 237  
   Mordell–Weil Theorem, 237  
   Nagel–Lutz theorem, 234  
   order of a point, 229  
   over finite fields, 244  
   point at infinity, 224  
   point of finite order, 229  
   rank, 237  
   torsion point, 229–230  
   torsion subgroup, 235  
 encryption key, 95  
 Eratosthenes, 24  
 Erdős, Paul, 135  
 Euclid, 13, 22  
 Euclidean algorithm, 15  
   applied to continued fractions, 168  
   efficiency of, 18–20  
   extended, 17, 18  
   for polynomials, 280  
   *see also* extended Euclidean algorithm  
 Euler factorization, 37  
 Euler totient function, 49, 109–113  
   for polynomials, 284  
   formula for computing, 111  
   is multiplicative, 111  
 Euler's criterion, 67  
 Euler's formula, 49  
   for polynomials, 285  
 Euler, Leonhard, 71  
 Euler, Leonhard, 32, 130, 202, 223, 238  
 experimental mathematics, 4  
   development process, 2  
 extended Euclidean algorithm, 17  
   inverses from, 46  
  
 factorial, 47  
 factorization  
   Euler factorization, 37  
   Fermat factorization, 36  
   Lenstra elliptic curve, 245  
   multiple factorizations for algebraic numbers, 146

- Pollard rho factorization, 37
- trial division algorithm, 36
- unique for integers, 21
- unique for polynomials, 281
- Fermat equation, *see* Fermat's Last Theorem
- Fermat factorization, 36
- Fermat near miss, 213, 218
- Fermat number, 3, 33, 271
- Fermat pseudoprime, 48, 58, 62
  - see also* Carmichael number
- Fermat's Last Theorem, 1, 187, 200–202, 215
  - for polynomials, 289
  - generalized, 296
  - $n = 4$ , 200
  - near miss, 218
- Fermat's Little Theorem, 46
  - Fermat pseudoprime, 58, 62
  - for polynomials, 286
  - primality test, 48, 61
- Fermat, Pierre de, 1, 200, 202, 223, 238
- Fibonacci numbers, 1, 18, 31, 58
  - convergents of the golden ratio, 181
  - in terms of the golden ratio, 31
  - prime divisors of, 61
  - worst-case for Euclidean algorithm, 18–20
- floor function, 168
- Ford, Kevin, 136
- formal periodic point, 257
- forward orbit, *see* orbit
- Fundamental Theorem of Algebra, 51, 54, 276
- fundamental unit, 203
- Gauss' Lemma, 276
- Gauss, Carl Frederick, 71, 190, 210
- Germain, Sophie, 2
- Goldbach conjecture, 135
- Goldbach partitions, 141
- Goldbach, Christian, 135
- golden ratio, 19, 31, 180
- good reduction, 260
- greatest common divisor, 11
  - as linear combination, 12, 280
  - computing, 13
  - polynomial, 280
- hash function, 101
  - check digit, 102
  - CvHP, 103
  - ISBN, 103
  - MD5, 101
  - SHA-1,SHA-2,SHA-3, 102
  - UPC, 102
- Hasse principle, 190
- Hasse, Helmut, 190
- height, 159
  - canonical, 274
  - logarithmic, 274
  - of a rational number, 159
  - points of bounded height, 184
- Hellman, Martin, 97
- Hensel lifting, *see* Hensel's Lemma
- Hensel's Lemma, 193, 194
- Heron triangle, 246
- Heron of Alexandria, 246
- Hilbert's 10th problem, 3
- Hilbert's 10th problem, 189
- Hilbert's number, 182
- Hilbert, David, 3, 189, 209
  - 10th problem, 4, 189
- integers
  - abundant number, 140
  - almost perfect, 140
  - almost prime, 35
  - composite, 7
  - deficient number, 140
  - density, 23
  - divisibility, 6–9
  - Division algorithm, 8
  - factorial, 47
  - Fermat number, *see* Fermat number
  - greatest common divisor, 11
  - least common multiple, 11
  - linear combination, 11
  - Mersenne prime, 34
  - partitions, 130–134
  - perfect number, 125–128
  - prime, 7
  - prime gap, 33
  - Prime Number Theorem, 28
  - relatively prime, 11
  - smooth number, 35
  - unique factorization, 21
  - well ordering property, 5
- International Standard Book Number (ISBN), 103
- inverse, 44
  - modulo  $n$ , 45
- irrational number, 157
- irreducible
  - algebraic integer, 149

- polynomial, 276
- Jacobi symbol, 75
- Jacobi, Carl, 75
- Julius Caesar, 91
- key exchange, Diffie–Hellman, 97
- Kummer, Ernst, 2, 150
- Lagrange interpolation, 252
- Lagrange polynomial, 252
- Lagrange’s Theorem, 84, 88
- Lagrange, Joseph Louis, 209
- Lamé’s Theorem, 19
- Lambert, Johann, 158
- Lattès map, 272
- lattice points, 184
- least common multiple, 11
- Legendre sieve, 128, 129
- Legendre symbol, 67
  - is multiplicative, 68
- Legendre, Adrien-Marie, 67, 71, 128, 210
- Lehmer, Derrick, 113
- Lenstra, Hendrik, 245
- Lind, Carl-Erik, 190
- Lindemann, Carl, 145
- linear combination, 11
  - greatest common divisor as, 12, 280
- linear congruence
  - multivariable, 62
  - solving in general, 52
  - solving with inverses, 50
  - system of, 54
  - see also* Chinese Remainder Theorem
- linear fractional transformation, 273
- Liouville function, 138, 141
- Liouville number, 145, 165
- Liouville’s theorem, 164
- Liouville, Joseph, 138, 141, 145
- logarithmic height, 274
- Lucas–Lehmer primality test, 37
- $m$ th power residue, 76
- $m$ th root modulo  $n$ , 76
- Mahler measure, 296
- Mandelbrot set, 250
- Matiyasevich, Yuri, 189
- Mazur’s theorem, 235, 253
- Mazur, Barry, 230
- MD5, 101
- Mersenne prime, 34, 127
  - relation with perfect numbers, 127
- Mersenne, Marin, 34
- Mignotte secret sharing, 104
- Mignotte sequence, 104
- Mignotte, Maurice, 104
- minimal period, 249
- Möbius function, 113–117, 255
  - is multiplicative, 114
- Möbius inversion formula, 116
- modular arithmetic, 41
  - for polynomials, 282
- modulus, 39
- monic polynomial, 148, 275
- Mordell curve, *see* elliptic curve
- Mordell, Louis, 227, 237
- Morton, Richard Patrick, 253
- Morton–Silverman uniform boundedness conjecture, 253, 273
- multiplicative function, 110
- multiplicative order, 76
  - for polynomials, 286
- multiplier, 263
- $n$ th iterate, 247
- Nagel–Lutz theorem, 234
- National Institute of Standards and Technology, 100, 102
- National Security Agency, 102
- Natural numbers, 5
- Newton map, 271
- nonlinear congruence, 62
- nototient, 136
- norm, 146
- number field, *see* quadratic number field
- one-way function, 101
- orbit, 248
- $p$ -adic number, 194, 198, 216
- parity problem, 130
- partition, 130–134
  - as power series coefficients, 131
  - Goldbach, 141
  - part, 130
  - prime partition, 141
  - Young diagram, 132
- Pell’s equation, 187, 202–208
  - for polynomials, 290
  - fundamental solution, 205
  - Pell-like equations, 218
  - solving with continued fractions, 206–208, 297
- Pell, John, 202

- perfect number, 1, 125–128  
 relation with Mersenne primes, 127
- periodic point, 248  
 determining by good reduction, 267  
 existence of, 272  
 formal periodic point, 257  
 minimal period, 249  
 multiplier, 263  
 period modulo  $p$ , 264  
*see also* dynatomic polynomial
- Pfitzmann, Birgit, 103
- pigeonhole principle, 163
- point at infinity, 224
- Polignac's Conjecture, 33
- Pollard rho factorization, 37
- polynomial, 275  
 content, 276  
 continued fraction, 297  
 degree, 275  
 Diophantine equations, 293  
 Diophantine equations, 288  
 Division algorithm, 279  
 Eisenstein's criteria, 277  
 Euclidean algorithm, 280  
 Euler totient function, 284  
 Euler's formula, 285  
 Fermat's Last Theorem, 289  
 Fermat's Little Theorem, 286  
 Fundamental Theorem of Algebra, 276  
 irreducible, 276  
 Mahler measure, 296  
 modular arithmetic for polynomials, 282  
 modulo irreducible polynomials, 288  
 monic, 148, 275  
 multiplicative order, 286  
 number of monic irreducible, 288  
 Pell's equation, 290  
 prime generating, 32  
 primitive, 276  
 Pythagorean triple, 289  
 Quadratic Reciprocity, 296  
 reducible, 276  
 root, 117, 275  
 unique factorization, 281  
 value, 282  
 Waring problem, 292, 298
- post-critically finite, 272
- preimage, 268
- preperiodic point, 248  
 cycle structure, 249  
 determining by good reduction, 268  
 MS uniform boundedness conjecture, 253, 273  
 tail, 249
- primality test, 24, 60  
 AKS, 61  
 Fermat's Little Theorem, 48, 61  
 Lucas, 61  
 Lucas–Lehmer, 37  
 Miller–Rabin, 61  
 pseudoprime, 61  
 Sieve of Eratosthenes, 24  
 trial division, 61  
 Wilson's theorem, 61
- prime gap, 33  
 Polignac's Conjecture, 33  
 Twin prime conjecture, 33
- prime number, 1, 7  
 algebraic integer, 149  
 consecutive primes, 33  
 generated by polynomials, 32  
 in arithmetic progression, 32  
 infinitely many, 22  
 Mersenne prime, 34  
 prime gap, 33  
 Sieve of Eratosthenes, 24, 128  
 twin primes, 33
- Prime Number Theorem, 28
- prime partition, 141
- prime splitting, *see* quadratic number field
- primitive polynomial, 276
- primitive prime divisor, 31, 32
- primitive root, 77  
 existence of, 85
- proper divisor, 126
- pseudoprime, 61  
 Fermat, 58, 62  
*see also* Carmichael number
- PSQL algorithm, 4
- Putnam, Hilary, 189
- pyramidal number, 243
- Pythagorean triple, 160, 187, 198–200  
 congruent number, 238  
 for polynomials, 289
- quadratic number field  
 basis, 145, 156  
 fundamental unit, 205  
 imaginary, 145  
 prime splitting, 151, 156  
 real, 145

- Quadratic Reciprocity, 69–74  
   for polynomials, 296  
   Supplemental Law, 69  
 quadratic residue, 66  
 quotient, 9
- Rabin coin flipping, 107  
 Rabin, Michael, 107  
 rational approximation, *see*  
   Diophantine approximation  
 rational function, 249  
   bad reduction, 260  
   canonical height, 274  
   conjugation, 273  
   critical points, 273  
   degree, 249  
   dynatomic polynomial, 254–258  
   forward orbit, 248  
   good reduction, 260  
   Lattès map, 272  
   modulo  $p$ , 258  
   MS uniform boundedness conjecture,  
     253, 273  
   multiplier, 263  
    $n$ th iterate, 247  
   Newton map, 271  
   post-critically finite, 272  
   preimage, 268  
   resultant, 259  
 rational numbers, 143, 157  
 Reichardt, Hans, 190  
 relatively prime, 11  
 remainder, 9  
 remainder after division, 39  
 residue class, 40  
 resultant, 258  
   rational function, 259  
 Rivest, Ronald, 99  
 Robinson, Julia, 189  
 root of unity, 69, 83  
   modulo  $n$ , 89  
   primitive, 117  
   *see also* cyclotomic polynomial  
 Roth's theorem, 166, 182  
 Roth, Klaus, 166  
 RSA public key, 99, 108
- Selmer, Ernst, 190  
 Shamir, Adi, 99  
 shared secret, 93, 108  
 shift cipher, *see* affine cipher  
 Siegel, Carl, 235  
 Sieve of Eratosthenes, 24, 128  
 sieve theory, 128  
 Silverman, Joseph H., 253  
 smooth number, 35  
 sociable numbers, 140  
 squarefree, 113  
 sum of divisors function, 122–125, 139  
   as power series coefficients, 124  
   formula for computing, 123  
   is multiplicative, 123  
   sum of two squares, 143, 152–153  
 symmetric cipher, 96
- tail of a preperiodic point, 249  
 Taylor, Richard, 200  
 Thue, Axel, 223  
 torsion point, 229  
 torsion subgroup, 235  
 totient function, *see* Euler totient  
   function  
 transcendental number, 144  
   Liouville number, 165  
 Triangle Inequality, 176  
 triangular number, 1, 215  
 twin primes, 33
- unique factorization  
   integers, 21  
   polynomials, 281  
 unit, 149  
 Universal Product Code (UPC), 102
- van Heijst, Eugène, 103  
 Vigenère cipher, 95
- wandering point, 248  
 Waring problem  
   for integers, 208–212, 219  
   for polynomials, 292, 298  
   generalized four square problem, 216  
   modulo primes, 219  
   sum of four squares, 212  
   sum of four squares, 209  
 Waring, Edward, 208  
 Weil, André, 237  
 well ordering property, 5, 8, 200, 205  
 Wiles, Andrew, 2, 200  
 Wilson's Theorem  
   for polynomials, 295  
   integer, 60  
   primality test, 61
- Young diagram, 132  
 Young, Alfred, 132