
Index

- p -adics, 535–537, 539, 542–545
abc-conjecture, 223, 226, 414, 416
- Algebraic numbers and integers, 23, 29
Algebraic units, 23, 29
- Bernoulli numbers and polynomials, 11, 193, 286, 289
Binary quadratic forms, 340, 344, 345, 353, 380, 426, 443, 444, 446–452, 456, 458, 459, 465, 466, 468–470, 484, 506, 508
Binomial coefficients, 4, 9, 68, 99, 172, 233, 241, 285, 320, 321
- Carmichael λ -function, 261, 388
Carmichael numbers, 245, 250, 378, 387, 388
Catalan equation, 223, 417
Chinese Remainder Theorem, 92, 97, 104, 106, 132, 309, 366
Class group and composition, 456–461, 463–466
Class number, 448–451, 471–474, 513
Computation and running times, 52, 255, 256, 322, 366, 370, 372, 378, 382, 389, 390, 393, 394
Congruent number problem, 221, 229, 551–553, 557
Constructibility and pre-Galois theory, 17, 25, 30, 103
Continued fractions, 39, 47, 381, 423, 424, 426–429, 431, 434, 436, 437, 470
- Convolutions, 136, 141, 143
Covering systems, 280, 281
Cryptography, 366, 368, 370, 391, 392
Cyclotomic polynomials, 153, 248, 290
- Descent, 219, 223, 229, 360, 361, 410, 553, 554, 556, 561, 562
Diophantine problems, 215, 218, 220, 233, 249, 263, 309, 339, 360, 361, 406, 410, 413, 414, 444, 452, 501, 504, 508, 509, 514, 547, 558
Dirichlet L -functions, 140, 192, 330, 473, 497, 499, 512
Dirichlet characters, 321, 326, 327, 330, 511
Discrete logs, 260
Discriminants, 15, 28, 77, 121
Divisibility tests, 66, 246
Divisors (incl. gcds), 34, 85, 129, 147, 150, 490, 493
Dynamics, 48, 208, 360, 361, 364, 420, 482
- Egyptian fractions, 59, 124
Elliptic curves, 220, 504–506, 508, 514, 519, 547, 548, 550, 551, 553, 554, 556–559, 561–563
Euclidean algorithm, 33, 40, 41, 45, 47, 51, 75, 90, 118
Euclidean domains, 78
Euler’s ϕ -function, 128
Euler’s criterion, 298, 305
- Factoring methods, 373, 380, 382, 399

- Fermat numbers, 8, 96, 103, 156, 240, 249, 280, 303, 313, 372, 379
 Fermat quotients, 284, 289, 293, 543–545
 Fermat's Last Theorem, 96, 218, 221, 225, 249, 279
 Fermat's Little Theorem, 238, 254, 270, 288, 297
 Fermat-Catalan conjecture, 223, 228, 417
 Fibonacci numbers, 1, 14, 42, 47, 69, 96, 281, 333, 335, 427, 437
 Finite fields, 144, 273, 493, 501, 503–506, 508, 509, 514
 Frobenius postage stamp problem, 57, 123, 532
 Fundamental discriminants, 329, 444, 445, 448, 450, 451, 466, 467, 473, 474
 Fundamental Theorem of Algebra, 117
 Fundamental Theorem of Arithmetic, 81, 82, 112, 117
 Generating functions, 11, 14, 515, 518, 528, 542
 Groups, 19, 71, 74, 109, 269, 271, 326, 328, 361, 397, 398, 408, 454, 494, 550, 565
 Heuristics, xxvi, 187, 289, 336, 383
 Ideals, 37, 43, 47, 113, 115, 460, 465
 Irrational numbers, 24, 87, 97, 223, 404, 418, 429
 Jacobi symbol, 307, 311, 321, 327, 329
 Lattice points, 317, 338, 347–349, 351, 353, 356, 358, 404, 420, 455
 Legendre symbol, 296, 321, 326
 Lifting solutions mod p^k , 266, 310, 538–540
 Linear algebra, 35, 37, 49, 56, 90, 96, 104, 123, 226, 276, 360, 374, 443, 445
 Local-global principle, 92, 97, 342, 343, 345, 348, 350, 351, 353, 355, 447
 Lucas sequence, 2
 Magic squares, 54, 201, 559
 Mahler measure, 540
 Matrices and matrix groups, 20, 28, 45, 47, 49, 105, 180, 276, 361, 364, 424, 428, 445, 447, 454, 462, 470, 482–484
 Mersenne numbers, 8, 44, 69, 96, 130, 157, 240, 303, 336, 386
 Möbius function, 135, 177, 249
 Modularity, 519
 Multiplication table problem, 491, 494
 Orders (of elements), 73, 236, 240, 242, 246, 252, 259, 261, 263, 265, 269
 Pascal's triangle, 5, 99
 Pell's equation, 406, 408, 427, 428, 431, 434, 470
 Pell's equation; negative, 410, 428, 431, 432
 Perfect numbers, 129, 131
 Polynomial properties, 10, 13, 23, 66, 75, 87, 96, 117, 119, 120, 144, 153, 168, 200, 223, 225, 226, 240, 275, 288, 299, 311, 373, 381, 396, 399–401, 493
 Power residues, 235, 298
 Primality testing, 157, 371, 372, 375, 383, 395, 396
 Prime k -tuplets conjecture, 178, 190, 199, 485
 Prime factors: number of, 487, 488, 490, 492
 Primes in arithmetic progressions, 159, 163, 169, 179, 198, 248, 312, 331, 527
 Primes: infinitely many, 155, 156, 160, 182, 202, 203, 208, 562
 Primes: number of, 157, 160, 163, 171, 184, 185, 187, 194
 Primitive roots, 242, 243, 246, 258, 260, 263, 313, 371
 Pseudoprimes, 245, 250, 375–379
 Pythagorean triangle, 215, 221, 223, 229, 347, 551, 552, 557, 563
 Quadratic fields, 115, 357, 460, 461, 465
 Quadratic forms, 343, 355, 363, 479–482, 501, 503
 Quadratic reciprocity (Law of), 300, 301, 303, 305, 309, 313, 315, 323, 333, 341, 355, 503, 512
 Quadratic residues / non-residues, 296, 299
 Quadratic residues and non-residues; least, 297, 310, 319

- Residues (mod n), 61, 71, 89, 236, 238,
262, 295, 305, 315, 328, 405
- Resultants and discriminants, 77, 120
- Riemann zeta-function, 13, 141, 142,
182, 184, 186, 192
- Rings and fields, 22, 73, 109
- Roots of polynomials, 15, 117, 122, 265,
267, 275, 537, 540
- Second-order linear recurrence
sequences, 2, 7, 14, 44, 69, 96, 281,
290, 334, 385
- Square roots (mod n), 94, 267, 299,
309–311, 365, 376
- Sums of (more than two) squares, 471,
475, 476, 478, 479, 567
- Sums of powers of integers, 3, 9, 286,
287, 292
- Sums of two squares, 337, 339, 347, 356,
405, 436, 437, 456
- Sumsets, 519, 521–524, 530, 532
- Tiling, 41
- Transcendental numbers, 24, 411, 412,
416, 439, 440
- Unique factorization, 112, 113, 117, 120,
272
- Waring's problem, 224, 566
- Wilson's Theorem, 241, 270, 287