INDEX

absolute value, 41
Adleman, 186
affine
  chart, 417
  curve, 418
  line, 415
  plane, 417, 418
Agrawal, 185
arithmetic progression, 70
Artin, 208, 209
  conjecture, 208
axioms, 29

Baker's bound, 441
bases and digits, 102, 103, 225
Bateman–Horn conjecture, 74, 75
Bellaso, 112
Bertrand's postulate, 67, 69
Bezout, 44
  algorithm, 44
  identity, 43, 44, 46–49, 51, 91–93, 161, 271
Bhaskara, 58, 395
bijection, 130, 181–183, 201, 215, 217, 222, 223, 254, 256, 260–262, 312, 338, 356, 415
binary operation, 124
binomial theorem, 57, 115, 185, 212
Brouncker, 395
brute force, 91, 274, 313, 349, 356, 455

canonical height, 455, 456
Carmichael number, 184, 190, 298, 301
Cartwright, 54, 55
change of variables
  linear, 248, 251
Chebyshev, 67
check digit, 106, 107
Chinese remainder theorem, 95, 98–101, 115, 116, 175, 181, 182, 187, 188, 221, 271, 273–275, 289, 291, 300, 304, 305, 315, 316, 356
  statement, 98
cipher
  Caesar, 111, 117
  shift, 111
  substitution, 111
  Vigenère, 111, 112, 117
Cipolla, 296
  algorithm, 296
complete residue system, 85, 86, 89, 91, 111, 113, 119, 120, 173, 174, 179, 189, 200, 201, 210, 213
complex numbers, 3, 24, 30, 78, 130, 131, 139, 140, 149, 239, 272, 350, 357
  complex conjugation, 140
composite number, 31, 37, 61
congruence, 84
  cancellation, 89, 121
  class, 84, 88, 119
  compatible family, 314
  index, 214–216
  invertible, 125
  linear, 90
  multiplicative inverse, 125
  multiplicative order, 195, 196, 229, 230
  of polynomials, 141, 156
  primitive root, 200–206, 208, 210, 214–216, 218, 220, 222, 223, 225, 277, 278, 280, 306, 307
  quadratic, 101, 271
  system of linear, 94, 95, 98
  unit, 132
  unit group, 132
  universal exponent, 203–205
conic section, 7, 89, 238, 248, 252
  parametrization, 255
  reduced form, 248, 251
constellation, 74, 75
  admissible, 74

continued fraction, xi, 55, 238, 323, 361–363, 395, 397, 398, 400, 401, 403, 409
  convergent, 366–369, 371, 386, 396, 397
  finite, 363
  infinite, 370
  period, 376, 399, 401
  periodic, 375–377, 380, 381
  purely periodic, 376, 382
  simple, 363
Cramer's rule, 243
cryptography, 110, 186
  Caesar cipher, 111
  Diffie–Hellman key exchange, 224, 233, 301, 471
  elliptic curve Diffie–Hellman, 471, 478
  Goldwasser–Micali, 301, 303, 308
  RSA, 186, 187, 301, 303
  substitution cipher, 110, 111
  Vigenère cipher, 111, 112, 225
cusp, 451

Davis, 22
decimal expansion, 225, 227
  period, 225, 227
  periodic, 227
Dedekind, 137
degree, 141
descent, 459
determinant, 129, 132
Diffie, 224
Diffie–Hellman key exchange, 224, 233
diophantine equation, 16, 17, 21, 25, 122, 123, 217, 269, 309, 343, 344, 347, 358
Diophantus, xi, 14, 15, 17, 18, 20, 25
Dirichlet, 68, 70, 75
  theorem, 71, 113, 136, 286, 304
discrete logarithm problem, 225, 233
  elliptic curve, 472, 477
discriminant, 147, 148, 153, 273–275, 310, 354, 355, 421, 450
divisibility test, 102, 103, 105, 106, 114
divisible, 31
  polynomials, 141
division theorem, 38, 39, 194, 197, 227
  for polynomials, 143
divisor, 31, 40, 41, 46

ellipse, 15, 24, 123, 238, 248, 251, 252, 265, 266, 268, 269, 334, 337, 348–350, 353, 356, 393, 403, 419, 424
elliptic curve, 11, 13, 15, 16, 21, 421, 437, 438
  conjecture of the rank, 447
  Diffie–Hellman key exchange, 471, 478
  discriminant, 421, 450
  free part, 445
  group structure, 441
  minimal discriminant, 451
  minimal model, 451
  Mordell–Weil group, 444
  over finite fields, 449
  rank, 445, 457, 467
  regulator, 458
  torsion subgroup, 445, 447
  Weierstrass equation, 439
elliptic height matrix, 458, 459
elliptic regulator, 458
equivalence relation, 88, 120, 128, 150, 415
Eratosthenes, 62
Erdös–Rényi graph, 303
Euclid, xi, 41–43, 63–65
  algorithm, 41–44, 46, 49, 57, 91–93, 109, 152, 271, 364
  theorem, 63
Euler, 4, 25, 54, 66, 67, 76, 167, 176, 177, 285, 338, 354, 375
  brick, 25
  criterion, 280–283, 288, 296–298
  phi function, 177, 178, 181, 189, 197
  theorem, 167, 176–178, 180, 183, 187, 196, 197, 203, 211, 213, 214, 222
  totient function, 177
even number, 40
exponential function, 215

Fermat, 20, 21, 66, 167, 170, 338, 354, 395, 438, 477
  last theorem, 20, 21, 80, 347, 348, 358, 438, 477
  little theorem, 170, 173–176, 178, 180, 184, 186–189, 195, 196, 203, 205, 211, 213, 214, 277, 297, 298
  number, 66, 117
  primality test, 298, 301
  prime, 66
  two squares theorem, 338
  witness, 184
Fibonacci, 60

numbers, 59, 371
field, 138, 275
automorphism, 140, 166
characteristic, 163, 328, 421, 438
finite, 138, 155, 156, 160, 162
Frobenius, 166
homomorphism, 139, 152, 166
imaginary quadratic, 351
isomorphism, 139
norm, 350, 351, 359, 403
quadratic, 139, 350–352, 378, 403
real quadratic, 351
finite field, 449
Fourier, 54
frequency analysis, 111, 112, 117
Frobenius automorphism, 166, 191, 297
fundamental theorem of algebra, 3
fundamental theorem of arithmetic, xi, 10, 46, 51–54, 61, 64, 136, 205
statement, 51
fundamental unit, 407
Futurama, 413

Garfield, 358
Gauss, xi, 10, 66, 68, 84, 167, 271, 276, 285
Disquisitiones Arithmeticae, 285
Gauss–Wantzel theorem, 66
GCD (see greatest common divisor), 42
general linear group (GL), 124, 129, 130
genus, 15, 16, 21, 309
geometric locus, 238
Germain, 81, 238
prime, 75, 80, 116, 307
Giordano, 61
Goldbach, 76
conjecture, 76, 77, 81
ternary (or odd) conjecture, 77
Goldbach's conjecture, 77
golden ratio, 60, 371
Goldwasser, 302
greater than, 30
greatest common divisor, 41, 42, 46, 57, 92, 93, 109, 152, 344
group, 124
abelian or commutative, 124, 125, 131, 132, 134, 164, 441, 445, 447, 454
finitely generated, 444
homomorphism, 128, 151, 305
isomorphism, 130, 222, 305, 407
quotient, 150, 305
subgroup, 127

Hadamard, 68
Hardy, 72, 413, 414, 446
Hardy–Littlewood
k-tuple conjecture, 74
twin prime conjecture, 72
Hardy–Littlewood conjecture, 72
Hardy–Ramanujan, 446
Hardy–Ramanujan number, 413
Hasse, 315, 453
bound, 453
theorem, 453
Hasse–Minkowski theorem, 238, 255, 309, 313, 315, 321, 323, 330, 338
statement, 315–317
height, 455
Helfgott, 77
Hellman, 224
Hensel's lemma, 331, 471
trivial case, 332
Hermite, 54
Hilbert, 22, 79
10th problem, 22
homogeneous space, 467–470
homomorphism
of groups, 128
hyperbola, 7, 9, 15, 24, 84, 238, 248, 251–253, 255, 259, 265, 268, 323, 334, 352, 361, 393–395, 419
square, 393, 394, 409, 419
hyperelliptic curve, 14

imaginary number, 3
induction, 33–35, 38, 51, 56, 58, 88, 96, 103, 146, 222, 307, 319, 325, 367, 368, 372, 373, 379, 398
base case, 33
complete, 36, 37, 51, 52, 293, 294
hypothesis, 33
step, 33
inequality, 30
injective, 130, 151, 182, 217, 407, 408, 454
involution, 140
irrational number, 2, 10, 48, 53, 59, 238, 247, 363, 371–373, 375
approximation, 386
continued fraction, 373
e, 54
pi, 54
quadratic, 376–379, 381

quadratic reduced, 382
irreducible polynomial, 159
isomorphism of curves, 440

Jacobi, 290
symbol, 290, 303

Kayal, 185
Kovalevskaya, 193
Kronecker symbol, 291
Kummer, 137

Lagrange, 1, 127, 381
theorem, 127, 128, 150, 300
Lambert, 54
Lang's conjecture, 455
law of quadratic reciprocity, xi, 10, 276, 284, 285, 287, 289, 292–295, 298, 304, 308, 349
statement, 285
least common multiple, 58, 115, 203, 204, 311, 426
least non-negative residue, 85–88, 112
Legendre, 68, 279, 285
conjecture, 68
symbol, 279, 280, 284, 290–293, 295, 296, 298, 306, 332
less than, 30
linear independence, 458
Littlewood, 72
logarithm, 214
properties, 215
long division (see division theorem), 38, 39, 225

Matiyasevich, 22
Mazur's theorem (Ogg's conjecture), 447
Mersenne, 232
number, 232
prime, 232
Micali, 302
minimal discriminant, 451
minimal model, 451
Minkowski, 315
Mordell, 13, 14, 16, 444, 445
Mordell–Weil theorem, 13, 444, 447, 455, 459, 466, 467
weak, 445
Mullin, 65

Nagell–Lutz theorem, 448
Nagura's theorem, 67, 80
Néron–Tate pairing, 458
Newton's method, 324
Niven, 54, 55
node, 451
Noether, 137
non-singular, 7, 420–422, 424, 425, 427, 428, 438, 439, 452
norm, 351
normal vector, 240–243, 424, 428, 438

odd number, 40
Ogg's conjecture, 447

p-adic
integers, 328
numbers, 317, 328–331, 349, 470, 471
valuation, 331
parabola, xii, 238, 248, 250–254, 256, 257, 261–264, 268, 269, 271, 419
Pell, 395, 396
equation, 238, 313, 395, 397, 409
fundamental solution, 400
generalized equation, 401, 408
negative equation, 401
perpendicular, 268
pigeonhole principle, 38, 57, 114
Poincaré, 444
point at infinity, 439
Pollard's rho algorithm, 109
polynomial, 2, 47, 48, 140
cancellation, 142
congruence, 156
congruence classes, 158
degree, 141
discriminant, 147, 148, 153, 273–275, 354, 355
divisibility, 141
homogeneous, 418
irreducible, 153, 159–162, 165, 354
quadratic, 147
resultant, 148
root, 145
unit, 159
positive integral solution, 396
primality test
AKS test, 185
primality testing, 61, 62, 170, 184
Solovay–Strassen, 298
prime number, 31, 37, 51–53, 57, 59, 61, 155, 328
arithmetic progression, 70
constellation, 74, 75, 80

counting function, 68
safe, 116
sexy, 80
Sophie Germain, 116, 307
theorem, 68, 69, 72, 76, 108
twin primes, 72
primitive root (see congruence), 200
projective
line, 415
plane, 416, 418
points at infinity, 415, 416
projectivization, 418, 419
pseudoprime, 184, 189, 190
Putnam, 22
Pythagoras of Samos, 343
Pythagoras's theorem, 343, 357, 358
pythagorean triple, 25, 113, 310, 343–348, 358
parametrization, 345
primitive, 344, 345

quadratic
field (see field), 350
form (see quadratic form), 309
formula, 272
Legendre symbol (see Legendre), 279
non-residue, 162, 276
reciprocity (see law of), 285
residue, 276–283, 289, 291, 296, 297, 304–306, 320, 329, 332, 349, 354, 355, 452
residue symbol, 279
ring, 404
quadratic form, 309, 310
compatible system of solutions, 314
discriminant, 310
Gram matrix, 310
primitive solution, 311
regular, 310
quotient, 39

Rado (or random) graph, 303
Ramanujan, 413, 414, 446
rank, 445
rank conjecture, 447
rational numbers, 1
reduced form, 47
reduction of an elliptic curve, 452
additive, 452
good, 452
non-split multiplicative, 452
split multiplicative, 452
regulator of an elliptic curve, 458
remainder, 39
theorem, 144, 159
Riemann, 78
hypothesis, 78, 79
hypothesis (generalized), 210
Riemann–Roch theorem, 439
surface, 15
zeta function, 78
ring, 131
commutative, 131, 158, 329
fundamental quadratic unit, 407
homomorphism, 137, 138
ideal, 137, 151
isomorphism, 137
of polynomials, 140
quadratic, 404
unit, 132, 404
zero-divisor, 132, 133, 158, 168
Rivest, 186
Robinson, 22, 23
root, 145
multiplicity, 145
of unity, 351
theorem, 4, 145, 159, 160

Saxena, 185
sexy primes, 80
Shamir, 186
Siegel's theorem, 441
sieve of Eratosthenes, 62, 63, 65, 80
singular curve, 420, 450, 451, 474
cusp, 451
node, 451
smooth, 7
smooth curve, 420, 438, 450
Solovay–Strassen primality test, 298
special linear group (SL), 26, 57, 130, 149
special relativity, 333
stereographic projection, 255
subgroup, 127
sum of two squares, 318
surjective, 130, 135, 136, 151, 182, 217, 223, 407
Sylvester's theorem, 67
system of linear congruences, 94, 98
incompatible, 98, 101, 313

tangent line, 394
tangent vector, 240
taxicab number, 414, 420

torsion points, 445
trichotomy, 30
twin primes, 72, 73
  conjecture, 72, 75

Vallée-Poussin, 68
vector space, 164
Vigenère, 111

Wantzel, 66
Waring, 170
Weierstrass equation, 425, 428, 438, 439
Weierstrass form, 414, 425, 426, 431, 432
Weil, 13, 14, 444
well-defined, 11, 120, 130, 135, 151, 181, 182, 290, 335, 356, 394, 407, 416, 421, 422
well-ordering principle, 30, 33, 36, 40, 143, 347
WhatsApp, 472
Wiles, 20, 21
Wilson, 167, 170
  theorem, 167, 170, 175, 188, 231, 278

Zhang, 73
Zi
  Sun Zi Suanjing, 96