

Index of Terms

- p -adic distance, 190
- p -adic norm, 190
- absolute value
 - of a complex number, 102
 - of a polynomial, 142
- abundant, 71
- acceleration
 - of a quadratic progression, 290
- algebraic, 83
- aliquot parts, 67
- ambiguous
 - binary quadratic form, 257, 288
 - river segment, 289
- amicable, 73
- associate
 - quadratic form, 256
- authentication, 166
- automorphism
 - composite, 241
 - inverse, 241
 - of the domain topograph, 240
- basis, 230
 - home, 232
 - lax, 232
 - lax, adjacent, 233
- bijection, 1
- binary quadratic form, 244
- bits, 11
- Carmichael number, 162
- ceiling, 10
- cell, 237
- Chebyshev's bias, 116
- choose, 8
- cipher, 166
- ciphertext
 - RSA, 187
- class
 - of binary quadratic forms, 252
- class number, 252
 - definite form, 271
 - for square discriminants, 282
 - indefinite form, 294
- commensurable, 82
- common divisor, 31
- common multiple, 35
- complementary angle, 79
- complex conjugate, 103
- composite, 48
- congruent, 130
 - integers, 127
- constructible number, 79
- coprime, 62
- cycle diagram
 - of a permutation, 204
- cycle length
 - mod p , 164
- cycle number
 - mod p , 164
- deficient, 71
- definite
 - negative, 262
 - positive, 262

- degree
 - of a polynomial, 140
- deprecated, 32
- descent
 - of congruences, 182
- determinant, 227
- Diffie-Hellman protocol, 166
- Diophantine approximation, 92
- Diophantine equation, 33
- discrete logarithm problem, 167
- discriminant, 250
 - cell, 251
 - fundamental, 272
 - triad, 250
- divides, 14
- divisor-sum function, 64

- Eisenstein integer, 105
- equivalence
 - of binary quadratic forms, 249
 - proper, 249
- Euclidean algorithm, 26
- Euclidean domain, 99

- factor, 12
- factorial, 72
- factoring, 48
- Fermat prime, 85
- Fermat's Last Theorem, 95
- Fermat's Little Theorem, 158
- floor, 10
- Ford circle, 87
- fraction, 76

- Gaussian integer, 104
- golden ratio, 97
- greatest common divisor, 31

- Hadwiger-Finsler inequality, 264
- Hasse diagram, 14
- home triad, 239
- homogeneous, 36
- hyperbolic plane, 247

- identity permutation, 204
- inaccessible, 230
- indefinite, 281
- inert, 113, 116, 117
- infinity-gon, 237
- integer, 10
- inversion
 - of a permutation, 208
- irreducible
 - polynomials mod p , 145
- isometry
 - improper, 288
 - of a binary quadratic form, 253

- Jacobi symbol, 221

- kissing fractions, 87

- lake, 274, 281
- lax superbasis, 237
- least common multiple, 35
- Legendre symbol, 202
- lies above, 115
- lies below, 114
- lifting
 - of congruences, 182
- lonely, 194
- loop
 - simple, 263

- Markov invariant, 296
- Markov number, 297
- Markov spectrum
 - integer, 296
- Markov triple, 297
- max, 61
- measures, 12
- mediant, 86
- Mersenne prime, 51
- Miller-Rabin primality test, 162
- min, 61
- modulus, 130
- monic, 146
- multiple, 12

- multiplicative, 64
- natural number, 1
- neighbor
 - binary quadratic forms, 257
- opposite
 - quadratic form, 256
- orientation
 - of a superbasis, 239
- pair, 8
- part
 - imaginary, 100
 - real, 100
- partner
 - a , 196
- path
 - simple, 263
- Pell's equation, 281
- perfect, 67
- permutation, 204
- pigeonhole principle, 175
- Pingala's algorithm, 161
- polynomial
 - constant, 140
 - linear, 140
 - mod p , 140
- price, 92
- primagon, 112
- prime
 - Gaussian or Eisenstein integer, 110
 - integer, 110
- prime decomposition, 56
- prime gaps, 54
- prime number, 48
- prime number theorem, 71
- primitive
 - binary quadratic form, 270
- primitive root
 - mod p , 165
- primitive vector, 231
- principal
 - binary quadratic form, 250
- private key
 - RSA, 186
- proper divisors, 67
- public key
 - RSA, 186
- Pythagorean triple, 81
- quadratic reciprocity, 215
- quadratic residue, 193
- ramified, 113, 116, 117
- rational numbers, 75
- reduced, 76
 - definite binary quadratic form, 278
 - Gauss, 277
 - indefinite binary quadratic form, 303
 - Lagrange, 276
- reduction operator
 - for indefinite quadratic forms, 303
- regular polygon, 85
- relatively prime, 62
- represent
 - by a quadratic form, 244
- representatives
 - mod n , 128
- Riemann hypothesis, 53
- river, 281
- riverbend number, 294
- root
 - mod p , 140
- RSA cryptosystem, 186
- semiotics, 76
- Sieve of Eratosthenes, 47
- sign
 - of a cycle, 207
 - of a permutation, 207
- simplify
 - mod n , 128
- Sophie Germain prime, 171, 220
- special orthogonal group, 253
- split, 113, 116, 117
- square numbers, 4
- square root

- mod n , 184
- square-free, 261
- square-scaling, 261
- squares
 - mod p , 193
- subset, 8
- superbasis
 - lax, 238
 - strict, 238
- topograph
 - domain, 232
 - range, 244
- totient, 156
- transcendental, 83
- transposition, 204
 - adjacent, 209
- tree, 263
- triad, 237
- triangular number, 5

- unit, 48
 - Eisenstein, 105
 - Gaussian, 104
 - polynomial mod p , 143

- vector
 - lax, 232

- walking home, 234

- water, 281

- well, 262

- double, 262

- single, 262

- witness

- perceptive, 162

- primality, 160

- zero polynomial, 140