

Index of notation

Entries are listed in order of appearance.

- log: natural logarithm, xiv
- exp: exponential function, xiv
- $\emptyset, \in, \subseteq, \subsetneq, \cup, \cap, \setminus, | \cdot |$: set notation, xiv
- $S_1 \times \cdots \times S_n, S^{\times n}$: Cartesian product, xiv
- $\{x_i\}_{i \in I}$: family, xv
- $\{x_i\}_{i=m}^n, \{x_i\}_{i=m}^\infty$: sequence, xv
- \mathbb{Z} : the integers, xv
- \mathbb{Q} : the rationals, xv
- \mathbb{R} : the reals, xv
- \mathbb{C} : the complex numbers, xv
- ∞ : arithmetic with infinity, xvi
- $[a, b], (a, b)$, etc.: interval notation, xvi
- $f(S)$: image of a set, xvi
- f^{-1} : pre-image of a set/inverse function, xvi
- $f \circ g$: function composition, xvii
- $a | b$: a divides b , 1
- $\lfloor x \rfloor$: floor of x , 4
- $\lceil x \rceil$: ceiling of x , 4
- $a \bmod b$: integer remainder, 4
- $a\mathbb{Z}$: ideal generated by a , 5
- $I_1 + I_2$: sum of ideals, 6
- gcd: greatest common divisor, 7
- $v_p(n)$: largest power to which p divides n , 10
- lcm: least common multiple, 11
- $a \equiv b \pmod{n}$: a congruent to b modulo n , 16
- $b|a \bmod n$: integer remainder, 22
- $a^{-1} \bmod n$: integer modular inverse, 22
- $[a]_n, [a]$: residue class of a modulo n , 25
- \mathbb{Z}_n : residue classes modulo n , 25
- \mathbb{Z}_n^* : invertible residue classes, 28
- $\varphi(n)$: Euler's phi function, 31
- $(\mathbb{Z}_n^*)^m$: m th powers in \mathbb{Z}_n^* , 36
- $\mu(n)$: Möbius function, 46
- $O, \Omega, \Theta, o, \sim$: asymptotic notation, 50
- len(a): length (in bits) of an integer, 62
- rep(α): canonical representative of $\alpha \in \mathbb{Z}_n$, 65
- $\pi(x)$: number of primes up to x , 104
- ϑ : Chebyshev's theta function, 107
- li: logarithmic integral, 117
- $\zeta(s)$: Riemann's zeta function, 118
- Map(I, G): group of functions $f : I \rightarrow G$, 131
- mG : the subgroup $\{ma : a \in G\}$, 133
- $G\{m\}$: the subgroup $\{a \in G : ma = 0_G\}$, 133
- G^m : multiplicative subgroup $\{a^m : a \in G\}$, 133
- $H_1 + H_2$: sum of subgroups, 136
- $H_1 H_2$: product of subgroups, 136
- $a \equiv b \pmod{H}$: $a - b \in H$, 137
- $[a]_H$: coset of H containing a , 138
- G/H : quotient group, 140
- $[G : H]$: index, 140
- Ker ρ : kernel, 143
- Im ρ : image, 143
- $G \cong G'$: isomorphic groups, 146
- Hom(G, G'): group homomorphisms $G \rightarrow G'$, 151
- $\langle a \rangle$: subgroup generated by a , 153
- $\langle a_1, \dots, a_k \rangle$: subgroup generated by a_1, \dots, a_k , 153
- $\bar{\alpha}$: complex conjugate of α , 167
- $N(\alpha)$: norm of $\alpha \in \mathbb{C}$, 167
- Map(I, R): ring of functions $f : I \rightarrow R$, 168
- AB : ring-theoretic product, 169
- $a | b$: a divides b , 170
- R^* : multiplicative group of units of R , 170
- $\mathbb{Z}[i]$: Gaussian integers, 174
- $\mathbb{Q}^{(m)}$: $\{a/b : \gcd(b, m) = 1\}$, 174
- $R[X]$: ring of polynomials, 176
- deg(g): degree of a polynomial, 177
- lc(g): leading coefficient of a polynomial, 177
- $g \bmod h$: polynomial remainder, 178
- aR : ideal generated by a , 186
- (a_1, \dots, a_k) : ideal generated by a_1, \dots, a_k , 186
- R/I : quotient ring, 187
- $a \equiv b \pmod{d}$: $a - b \in dR$, 187
- $[a]_d$: the residue class $[a]_{dR}$, 187
- $R[\alpha]$: smallest subring containing R and α , 192
- $R[\alpha_1, \dots, \alpha_n]$: smallest subring containing R and $\alpha_1, \dots, \alpha_n$, 193

- $R \cong R'$: isomorphic rings, 195
 P : probability distribution, 207
 P_1, P_2, P_1^n : product distribution, 211
 $P[A | B]$: conditional probability of A given B , 214
 $E[X]$: expected value of X , 233
 $\text{Var}[X]$: variance of X , 235
 $E[X | B]$: conditional expectation of X given B , 237
 $\Delta[X; Y]$: statistical distance, 260
 $y \stackrel{\epsilon}{\leftarrow} \{0, 1\}$, $y \stackrel{\epsilon}{\leftarrow} \{0, 1\}^{\times \ell}$: assign random bit(s), 278
 $y \stackrel{\epsilon}{\leftarrow} T$: assign random element of T , 287
 $\log_y \alpha$: discrete logarithm, 327
 $(a | p)$: Legendre symbol, 342
 $(a | n)$: Jacobi symbol, 346
 J_n : Jacobi map, 347
 $\text{Map}(I, M)$: R -module of functions $f : I \rightarrow M$, 360
 cM : submodule $\{c\alpha : \alpha \in M\}$, 361
 $M\{c\}$: submodule $\{\alpha \in M : c\alpha = 0_M\}$, 361
 $R\alpha$: submodule $\{c\alpha : c \in R\}$, 361
 $\langle \alpha_1, \dots, \alpha_k \rangle_R$: submodule generated by $\alpha_1, \dots, \alpha_k$,
 361
 $R[X]_{< \ell}$: polynomials of degree less than ℓ , 361
 M/N : quotient module, 362
 $M \cong M'$: isomorphic modules, 365
 $\text{Hom}_R(M, M')$: R -linear maps $M \rightarrow M'$, 366
 $\dim_F(V)$: dimension, 372
 $A(i, j)$: (i, j) entry of A , 378
 $\text{Row}_i(A)$: i th row of A , 378
 $\text{Col}_j(A)$: j th column of A , 378
 $R^{m \times n}$: $m \times n$ matrices over R , 378
 $0_R^{m \times n}$: $m \times n$ zero matrix, 378
 A^T : transpose of A , 380
 $\text{Vec}_S(\alpha)$: coordinate vector, 382
 $\text{Mat}_{S, T}(\rho)$: matrix of linear map, 383
 $\Psi(y, x)$: number of y -smooth integers up to x , 399
 $\text{Map}(I, E)$: R -algebra of functions $f : I \rightarrow E$, 423
 $R[\alpha]$: subalgebra generated by α , 426
 gcd : greatest common divisor (polynomial), 432
 lcm : least common multiple (polynomial), 433
 $h/g \bmod f$: polynomial remainder, 435
 $g^{-1} \bmod f$: polynomial modular inverse, 435
 $(E : F)$: degree of an extension, 440
 $F(\alpha)$: smallest subfield containing F and α , 441
 $R[[X]]$: formal power series, 446
 $R((X))$: formal Laurent series, 447
 $R((X^{-1}))$: reversed Laurent series, 449
 $\deg(g)$: degree of $g \in R((X^{-1}))$, 449
 $\text{lc}(g)$: leading coefficient of $g \in R((X^{-1}))$, 449
 $\lfloor g \rfloor$: floor of $g \in R((X^{-1}))$, 449
 $\text{len}(g)$: length of a polynomial, 466
 $\text{rep}(\alpha)$: canonical representative of $\alpha \in R[X]/(f)$,
 466
 $D_F(V)$: dual space, 492
 $\mathcal{L}_F(V)$: space of linear transformations, 501
 $\mathbf{N}_{E/F}(\alpha)$: norm, 518
 $\mathbf{Tr}_{E/F}(\alpha)$: trace, 518

Index

- Abel's identity, 112
- abelian group, 126
- additive identity, 27
- additive inverse, 27
- additive subgroup, 169
- Adleman, L. M., 99, 103, 419, 420, 546, 559
- Agrawal, M., 548, 558
- Alford, W., 325
- algebra, 421
- algebraic
 - element, 441
 - extension, 441
- almost universal hash functions, 258
- Apostol, T. M., 125
- approximately computes, 302
- arithmetic function, 45
- arithmetic/geometric mean, 240
- Artin's conjecture, 99
- associate
 - elements of an integral domain, 451
 - polynomials, 430
- associative binary operation, xvii
- asymptotic notation, 50
- Atlantic City algorithm, 303
- automorphism
 - algebra, 424
 - group, 146
 - module, 365
 - ring, 195
 - vector space, 370
- baby step/giant step method, 330
- Bach, E., 125, 305, 325, 340, 357, 546
- basis, 367
- Bateman, P., 125
- Bayes' theorem, 215
- Bellare, M., 420
- Ben-Or, M., 546
- Berlekamp subalgebra, 538
- Berlekamp's algorithm, 538
- Berlekamp, E. R., 508, 546
- Bernoulli trial, 208
- Bernstein approximation, 240
- Bertrand's postulate, 109
- big-O, -Omega, -Theta, 50
- bijection, xvi
- bijjective, xvi
- binary gcd algorithm, 77
- binary operation, xvii
- binomial coefficient, 561
- binomial distribution, 223
- binomial expansion, 562
- binomial theorem, 169, 562
- birthday paradox, 248
- bivariate polynomial, 183
- Blum, L., 103
- Blum, M., 103
- Boneh, D., 103, 341
- Bonferroni's inequalities, 213
- Boole's equality, 210
- Boole's inequality, 210
- Boolean circuits, 72
- Brent, R. P., 485
- Brillhart, J., 418
- Buhler, J. P., 419
- Burgess, D. A., 357
- \mathbb{C} , xv
- cancellation law, 2, 21, 28, 129, 171, 435
- Canfield, E., 418
- canonical representative
 - integer, 65
 - polynomial, 466
- Cantor, D. G., 546
- Cantor-Zassenhaus algorithm, 530
- cardinality, xiv
- Carmichael number, 308
- Carmichael, R. D., 325
- Carter, J. L., 275
- Cartesian product, xiv
- ceiling, 4
- characteristic of a ring, 169
- characteristic polynomial, 518
- Chebyshev's inequality, 241
- Chebyshev's theorem, 105
- Chebyshev's theta function, 107

- Chernoff bound, 242
- Chinese remainder theorem
 - general, 202
 - integer, 23, 82
 - polynomial, 435, 473
- Chistov, A. L., 546
- classification of cyclic groups, 156
- closed under, xvii
- column null space, 395
- column rank, 394
- column space, 394
- column vector, 378
- common divisor
 - in an integral domain, 452
 - integer, 6
 - polynomial, 431
- common multiple
 - in an integral domain, 452
 - integer, 11
 - polynomial, 433
- commutative binary operation, xvii
- commutative ring with unity, 166
- companion matrix, 385
- complex conjugation, 167, 198
- composite, 2
- composition, xvi
- conditional distribution, 213, 224
- conditional expectation, 237
- conditional probability, 214
- congruence, 16, 137
- conjugacy class, 516
- conjugate, 516
- constant polynomial, 176
- constant term, 177
- continued fraction method, 418
- continued fractions, 103
- convex function, 564
- coordinate vector, 382
 - of a projection, 492
- Coppersmith, D., 419
- Cormen, T. H., 340
- coset, 138
- countable, 562
- countably infinite, 562
- covariance, 240
- Crandall, R., 73, 125, 420
- cyclic, 153

- Damgård, I., 325, 464
- Davenport, J., 103
- De Morgan's law, 208
- decisional Diffie–Hellman problem, 338
- degree
 - of a polynomial, 177
 - of a reversed Laurent series, 449
 - of an element in an extension field, 441
 - of an extension, 440
- Denny, T., 420
- derivative, 444
- deterministic algorithm, 278
- deterministic poly-time equivalent, 336
- deterministic poly-time reducible, 336
- Dickson, L. E., 125
- Diffie, W., 341
- Diffie–Hellman key establishment protocol, 334
- Diffie–Hellman problem, 335
- dimension, 372
- direct product
 - of algebras, 422
 - of groups, 130
 - of modules, 360
 - of rings, 168
- Dirichlet inverse, 49
- Dirichlet product, 45
- Dirichlet series, 120
- Dirichlet's theorem, 121
- Dirichlet, G., 125
- discrete logarithm, 327
 - algorithm for computing, 329, 400
- discrete probability distribution, 270
- discriminant, 182
- disjoint, xv
- distinct degree factorization, 530, 543
- distributive law
 - Boolean, 208
- divides, 1, 170
- divisible by, 1, 170
- division with remainder property
 - integer, 3
 - polynomial, 178
- divisor, 1, 170
- Dixon, J., 418
- Dornstetter, J. L., 508
- dual space, 492
- Durfee, G., 103

- Eisenstein integers, 456
- Eisenstein's criterion, 462
- elementary row operation, 389
- elliptic curve method, 419
- equal degree factorization, 532, 537
- equivalence class, 15
- equivalence relation, 15
- Eratosthenes
 - sieve of, 115
- Erdős, P., 418
- error correcting code, 97, 477
- error probability, 302
- essentially equal
 - probability distributions, 212
- Euclidean algorithm
 - extended
 - integer, 78
 - polynomial, 470
 - integer, 74
 - polynomial, 469
- Euclidean domain, 454
- Euler's criterion, 38, 165, 205
- Euler's identity, 118
- Euler's phi function, 31
 - and factoring, 320
- Euler's summation formula, 114

- Euler's theorem, 34, 157
- Euler's totient function, 31
- Euler, L., 125
- event, 208
- eventually positive, 50
- exp, xiv
- expectation, 233
- expected polynomial time, 283
- expected running time, 283
- expected value, 233
- exponent, 160
 - module, 363
- extended Euclidean algorithm
 - integer, 78
 - polynomial, 470
- extended Gaussian elimination, 391
- extension, xvi
- extension field, 175, 440
- extension ring, 174

- factoring
 - and Euler's phi function, 320
- factoring algorithm
 - integer, 407, 414
 - deterministic, 484
 - polynomial, 530, 538
 - deterministic, 544
- family, xv
- fast Fourier transform, 480
- Fermat's little theorem, 34, 35
- FFT, 480
- field, 170
- field of fractions, 427
- finite dimensional, 372
- finite expectation, 272
- finite extension, 440
- finite fields
 - existence, 511
 - subfield structure, 515
 - uniqueness, 515
- finitely generated
 - abelian group, 153
 - module, 361
- floor, 4
 - of reversed Laurent series, 449
- formal derivative, 444
- formal Laurent series, 447
- formal power series, 446
- Fouvry, E., 559
- Frandsen, G., 464
- Frobenius map, 512
- fundamental theorem
 - of arithmetic, 2
 - of finite abelian groups, 163
 - of finite dimensional $F[X]$ -modules, 506
- Fürer, M., 72

- von zur Gathen, J., 485, 546, 547
- Gauss' lemma, 344
- Gaussian elimination, 389
- Gaussian integers, 174, 199, 454, 457

- gcd
 - integer, 7
 - polynomial, 432
- generating polynomial, 487
- generator, 153
 - algorithm for finding, 327
- geometric distribution, 271, 274
- Gerhard, J., 485, 546
- Goldwasser, S., 357
- Gordon, D. M., 420
- Gordon, J., 546
- Granville, A., 325
- greatest common divisor
 - in an integral domain, 452
 - integer, 6
 - polynomial, 431
- group, 126
- Guy, M., 103

- Hadamard, J., 124
- Halberstam, H., 325
- Hardy, G. H., 103, 124, 125
- hash function, 252
- Heath-Brown, D., 125
- Hellman, M., 340, 341
- Hensel lifting, 351
- homomorphism
 - algebra, 424
 - group, 142
 - module, 363
 - ring, 192
 - vector space, 370
- Horn, R., 125
- Horner's rule, 467
- Huang, M.-D., 559
- hybrid argument, 264

- ideal, 5, 185
 - generated by, 5, 186
 - maximal, 190
 - prime, 189
 - principal, 5, 186
- identity element, 126
- identity map, xvi
- identity matrix, 379
- image, xvi
- image of a random variable, 221
- Impagliazzo, R., 276
- inclusion map, xvi
- inclusion/exclusion principle, 210
- independent, 214, 224
 - k -wise, 218, 225
 - mutually, 218, 225
- indeterminate, 176
- index, 140
- index calculus method, 420
- index set, xv
- indicator variable, 222
- infinite extension, 440
- infinite order, 130
- injective, xvi

- integral domain, 171
- internal direct product, 148
- inverse
 - multiplicative, 170
 - of a group element, 126
 - of a matrix, 386
- inverse function, xvi
- invertible matrix, 386
- irreducible element, 451
- irreducible polynomial, 430
 - algorithm for generating, 523
 - algorithm for testing, 522
 - number of, 514
- isomorphism
 - algebra, 424
 - group, 146
 - module, 365
 - ring, 195
 - vector space, 370
- Iwaniec, H., 340

- Jacobi map, 347
- Jacobi sum test, 559
- Jacobi symbol, 346
 - algorithm for computing, 348
- Jensen's inequality, 239, 275

- Kalai, A., 305
- Kaltofen, E., 547
- Karatsuba, A. A., 71
- Kayal, N., 548, 558
- Kedlaya, K., 485
- kernel, 143
- kills, 160
- Kim, S. H., 325
- Knuth, D. E., 72, 73, 103
- von Koch, H., 125
- Kronecker substitution, 479
- Krovetz, T., 276
- Kung, H. T., 485

- Lagrange interpolation formula, 436
- Las Vegas algorithm, 303
- Latin square, 131
- law of large numbers, 242
- law of quadratic reciprocity, 343
- law of total expectation, 237
- law of total probability, 215
- lcm
 - integer, 11
 - polynomial, 433
- leading coefficient, 177
 - of a reversed Laurent series, 449
- least common multiple
 - in an integral domain, 452
 - integer, 11
 - polynomial, 433
- leftover hash lemma, 267
- Legendre symbol, 342
- Lehmann, D., 325
- Lehmer, D., 418

- Leiserson, C. E., 340
- len, 62, 466
- length
 - of a polynomial, 466
 - of an integer, 62
- Lenstra, Jr., H. W., 419, 546, 559
- Levin, L., 276
- li, 117
- linear combination, 361
- linear map, 363
- linear transformation, 501
- linearly dependent, 367
- linearly generated sequence, 486
 - minimal polynomial of, 487
 - of full rank, 492
- linearly independent, 367
- little-o, 50
- Littlewood, J. E., 125
- log, xiv
- logarithmic integral, 117
- lowest terms, 12
- Luby, M., 276, 305

- map, xvi
- Markov's inequality, 241
- Massey, J., 508
- matrix, 377
- matrix of a linear map, 383
- Maurer, U., 325
- maximal ideal, 190
- memory cells, 53
- Menezes, A., 103
- Mertens' theorem, 113
- Micali, S., 357
- Miller, G. L., 324, 325
- Miller–Rabin test, 307
- Mills, W., 484, 508
- min entropy, 266
- minimal polynomial, 438
 - algorithm for computing, 468, 500, 525
 - of a linear transformation, 503
 - of a linearly generated sequence, 487
 - of an element under a linear transformation, 504
- Möbius function (μ), 46
- Möbius inversion formula, 47
- mod, 4, 16, 22, 178, 435
- modular composition, 467, 485
- modular square root
 - algorithm for computing, 350
- module, 358
- modulus, 16
- monic associate, 430
- monic polynomial, 177
- monomial, 183
- Monte Carlo algorithm, 303
- Morrison, K., 508
- Morrison, M., 418
- multi-variate polynomial, 184
- multiple, 1, 170
- multiple root, 182
- multiplication map, 143, 166, 363

- multiplicative function, 46
 - multiplicative group of units, 170
 - multiplicative identity, 27
 - multiplicative inverse
 - in a ring, 170
 - modulo integers, 21
 - modulo polynomials, 435
 - multiplicative order, 33, 153
 - multiplicative order modulo n , 33
 - multiplicity, 182
 - mutually independent, 218, 225

- natural map, 143, 192
- Newton interpolation, 474
- Newton's identities, 450
- Niven, I., 357
- norm, 167, 518
- normal basis, 521
- number field sieve, 419

- Oesterlé, J., 125
- one-sided error, 304
- one-time pad, 229
- one-to-one correspondence, xvi
- van Oorschot, P., 103, 341
- order
 - in a module, 364
 - of a group element, 153
 - of an abelian group, 130

- pairwise disjoint, xv
- pairwise independent
 - events, 218
 - hash functions, 252
 - random variables, 225
- pairwise relatively prime
 - integers, 11
 - polynomials, 434
- parity check matrix, 385
- partition, xv
- Pascal's identity, 562
- Penk, M., 103
- perfect power, 64
- period, 98
- periodic sequence, 98
- PID, 455
- pivot element, 389
- pivot sequence, 388
- Pohlig, S., 340
- Pollard, J. M., 340, 419
- polynomial
 - associate, 430
 - irreducible, 430
 - monic, 177
 - primitive, 459
 - reducible, 430
- polynomial evaluation map, 192, 426
- polynomial time, 55
 - expected, 283
 - strict, 283
- Pomerance, C., 73, 125, 325, 418–420, 559

- de la Vallée Poussin, C.-J., 124, 125
- power map, 143
- pre-image, xvi
- pre-period, 98
- primality test
 - deterministic, 548
 - probabilistic, 306
- prime
 - ideal, 189
 - number, 2
- prime number theorem, 116
 - irreducible polynomials over a finite field, 514
- primitive polynomial, 459
- principal ideal, 5, 186
- principal ideal domain, 455
- probabilistic algorithm, 278
- probability distribution
 - conditional, 213
 - discrete, 270
 - finite, 207
- product distribution, 211
- program, 53
- projection, 492
- public key cryptography, 341
- public key cryptosystem, 99
- purely periodic, 98

- \mathbb{Q} , xv
- quadratic formula, 182
- quadratic reciprocity, 343
- quadratic residue, 36
- quadratic residuosity
 - algorithm for testing, 349
 - assumption, 355
- quadratic sieve, 415
- quantum computer, 420
- quotient algebra, 423
- quotient group, 140
- quotient module, 362
- quotient ring, 187
- quotient space, 370

- \mathbb{R} , xv
- Rabin, M. O., 324
- Rackoff, C., 418
- RAM, 53
- random access machine, 53
- random self-reduction, 337
- random variable, 221
 - conditional distribution of, 224
 - conditional expectation, 237
 - distribution of, 222
 - expected value, 233
 - image, 221
 - independent, 224
 - real valued, 221
 - variance, 235
- random walk, 244
- randomized algorithm, 278
- rank, 395
- rational function field, 429

- rational function reconstruction, 474
- rational reconstruction problem, 90
- recursion tree, 332, 340
- Redmond, D., 125
- reduced row echelon form, 388
- reducible polynomial, 430
- Reed, I., 484
- Reed–Solomon code, 97, 477
- regular function, 223
- relatively prime
 - in an integral domain, 452
 - integers, 7
 - polynomials, 432
- Renyi entropy, 266
- rep, 65, 466
- repeated-squaring algorithm, 65
- representation, 337
- representative
 - of a coset, 138
 - of a residue class, 25
 - of an equivalence class, 16
- residue class, 25, 187
- residue class ring, 187
- restriction, xvi
- reversed Laurent series, 448
- Richert, H., 325
- Riemann hypothesis, 118, 120, 122, 125, 324, 326, 340, 357, 482, 546, 547
- Riemann's zeta function, 118
- Riemann, B., 125
- ring, 166
- ring of polynomials, 176
- ring-theoretic product, 169
- Rivest, R. L., 99, 103, 340
- Rogaway, P., 276, 420
- root of a polynomial, 179, 425
- Rosser, J., 124
- row echelon form, 397
- row null space, 393
- row rank, 394
- row space, 392
- row vector, 378
- RSA cryptosystem, 99
- Rumely, R. S., 559
- running time
 - expected, 283
- sample mean, 241
- sample space, 207
- Saxena, N., 548, 558
- scalar, 358
- scalar multiplication map, 358
- Schirokauer, O., 420
- Schoenfeld, L., 124
- Schönhage, A., 72, 102
- Scholtz, R., 508
- Schoof, R., 103
- secret sharing, 230
- Semaev, I. A., 546
- separating set, 544
- sequence, xv
 - Shallit, J., 125, 357, 546
 - Shamir, A., 71, 99, 103, 275
 - Shanks, D., 340
 - shift register sequence, 488
 - Shor, P., 420
 - Shoup, V., 340, 508, 546, 547
 - Shub, M., 103
 - sieve of Eratosthenes, 115
 - simple root, 182
 - smooth number, 399, 414
 - Solomon, G., 484
 - Solovay, R., 325, 357
 - Sophie Germain prime, 123
 - spans, 367
 - splitting field, 443
 - square root (modular)
 - algorithm for computing, 350
 - square-free
 - integer, 9
 - polynomial, 509
 - square-free decomposition, 527
 - square-free decomposition algorithm, 527
 - standard basis, 368
 - statistical distance, 260
 - Stein, C., 340
 - Stein, J., 103
 - Stinson, D. R., 276
 - Stirling's approximation, 114
 - Strassen, V., 72, 325, 357
 - strict polynomial time, 283
 - subalgebra, 423
 - fixed by, 425
 - generated by, 426
 - subfield, 175
 - subgroup, 132
 - generated by, 153
 - submodule, 360
 - subring, 173
 - subspace, 370
 - sufficiently large, 50
 - surjective, xvi
- theta function of Chebyshev, 107
- total degree, 183
- total expectation
 - law of, 237
- total probability
 - law of, 215
- trace, 518
- transcendental element, 441
- transpose, 380
- trial division, 306
- trivial
 - group, 130
 - module, 359
 - ring, 168
- twin primes conjecture, 124
- two-sided error, 304
- UFD, 451
- ultimately periodic sequence, 98

- Umans, C., 485
- union bound, 210
- unique factorization
 - in a Euclidean domain, 454
 - in a PID, 455
 - in $D[X]$, 459
 - in $F[X]$, 430
 - in \mathbb{Z} , 2
- unique factorization domain, 451
- unit, 170
- universal hash functions, 252

- Vandermonde matrix, 385
- Vanstone, S., 103
- variance, 235
- vector space, 370

- Walfisz, A., 124
- Wang, P., 103
- Wang, Y., 340
- Weber, D., 420
- Wegman, N. M., 275
- Weilert, A., 464
- Welch, L., 508
- well-behaved complexity function, 69
- Wiedemann, D., 508
- Wiener, M., 103, 341
- Wright, E. M., 103, 124, 125

- Yun, D. Y. Y., 546

- \mathbb{Z} , xv
- Zassenhaus, H., 546
- zero divisor, 171
- zero element, 129
- zero matrix, 378
- zero-sided error, 304
- zeta function of Riemann, 118
- Zuckerman, H., 357
- Zuckermann, D., 276