

# Index of notation

Entries are listed in order of appearance.

- $\infty$ : arithmetic with infinity, xiv
- log: natural logarithm, xiv
- exp: exponential function, xiv
- $\emptyset$ : the empty set, xiv
- $A \cup B$ : union of two sets, xiv
- $A \cap B$ : intersection of two sets, xiv
- $A \setminus B$ : difference of two sets, xiv
- $S_1 \times \cdots \times S_n$ : Cartesian product, xv
- $S^{\times n}$ :  $n$ -wise Cartesian product, xv
- $f(S)$ : image of a set, xv
- $f^{-1}(S)$ : pre-image of a set, xv
- $f \circ g$ : function composition, xvi
- $\mathbb{Z}$ : the integers, 1
- $b \mid a$ :  $b$  divides  $a$ , 1
- $\lfloor x \rfloor$ : floor of  $x$ , 3
- $a \bmod b$ : integer remainder, 3
- $\lceil x \rceil$ : ceiling of  $x$ , 3
- $a\mathbb{Z}$ : ideal generated by  $a$ , 4
- $a_1\mathbb{Z} + \cdots + a_k\mathbb{Z}$ : ideal generated by  $a_1, \dots, a_k$ , 5
- gcd: greatest common divisor, 6
- $\nu_p(n)$ : largest power to which  $p$  divides  $n$ , 8
- lcm: least common multiple, 9
- $\mathbb{Q}$ : the rational numbers, 9
- $a \equiv b \pmod{n}$ :  $a$  congruent to  $b$  modulo  $n$ , 13
- $b/a \bmod n$ : integer remainder, 17
- $a^{-1} \bmod n$ : integer modular inverse, 17
- $\mathbb{Z}_n$ : residue classes modulo  $n$ , 21
- $\phi$ : Euler's phi function, 24
- $\mu$ : Möbius function, 29
- $O, \Omega, \Theta, o, \sim$ : asymptotic notation, 33
- len: length (in bits) of an integer, 46
- rep( $\alpha$ ): canonical representative of  $\alpha \in \mathbb{Z}_n$ , 48
- $\pi(x)$ : number of primes up to  $x$ , 74
- $\vartheta$ : Chebyshev's theta function, 76
- li: logarithmic integral, 87
- $\zeta$ : Riemann's zeta function, 88
- P: probability function, 96
- $P[A \mid \mathcal{B}]$ : conditional probability of  $\mathcal{A}$  given  $\mathcal{B}$ , 100
- $E[X]$ : expected value of  $X$ , 111
- $\text{Var}[X]$ : variance of  $X$ , 113
- $E[X \mid \mathcal{B}]$ : conditional expectation of  $X$  given  $\mathcal{B}$ , 114
- $\Delta[X; Y]$ : statistical distance, 131
- $mG$ :  $\{ma : a \in G\}$ , 185
- $G\{m\}$ :  $\{a \in G : ma = 0_G\}$ , 186
- $G^m$ :  $\{a^m : a \in G\}$ , 186
- $H_1 + H_2$ :  $\{h_1 + h_2 : h_1 \in H_1, h_2 \in H_2\}$ , 189
- $H_1 \cdot H_2$ :  $\{h_1 h_2 : h_1 \in H_1, h_2 \in H_2\}$ , 189
- $a \equiv b \pmod{H}$ :  $a - b \in H$ , 190
- $a + H$ : coset of  $H$  containing  $a$ , 190
- $aH$ : coset of  $H$  containing  $a$  (multiplicative notation), 190
- $G/H$ : quotient group, 191
- $[G : H]$ : index, 191
- $\ker(\rho)$ : kernel, 194
- $\text{img}(\rho)$ : image, 194
- $G \cong G'$ : isomorphic groups, 197
- $\langle a \rangle$ : subgroup generated by  $a$ , 202
- $\langle a_1, \dots, a_k \rangle$ : subgroup generated by  $a_1, \dots, a_k$ , 202
- $\mathbb{R}$ : real numbers, 212
- $\mathbb{C}$ : complex numbers, 212
- $\bar{\alpha}$ : complex conjugate of  $\alpha$ , 212
- $N(\alpha)$ : norm of  $\alpha \in \mathbb{C}$ , 213
- $b \mid a$ :  $b$  divides  $a$ , 214
- $R^*$ : multiplicative group of units of  $R$ , 214
- $\mathbb{Z}[i]$ : Gaussian integers, 219
- $\mathbb{Q}^{(m)}$ :  $\{a/b : \gcd(b, m) = 1\}$ , 219
- $R[X]$ : ring of polynomials, 220
- deg( $a$ ): degree of a polynomial, 223
- lc( $a$ ): leading coefficient of a polynomial, 223
- $a \bmod b$ : polynomial remainder, 224
- $D(a)$ : formal derivative of  $a$ , 227

$a_1R + \cdots + a_kR$ : ideal generated by  
 $a_1, \dots, a_k$ , 231  
 $(a_1, \dots, a_k)$ : ideal generated by  $a_1, \dots, a_k$ , 231  
 $R/I$ : quotient ring, 232  
 $[a]_I$ : the coset  $a + I$ , 232  
 $[a]_d$ : the coset  $a + dR$ , 232  
 $R \cong R'$ : isomorphic rings, 237  
 $\log_\gamma \alpha$ : discrete logarithm, 268  
 $(a | p)$ : Legendre symbol, 285  
 $(a | n)$ : Jacobi symbol, 287  
 $J_n$ : Jacobi map, 289  
 $aM$ :  $\{a\alpha : \alpha \in M\}$ , 301  
 $M\{a\}$ :  $\{\alpha \in M : a\alpha = 0_M\}$ , 301  
 $\langle \alpha_1, \dots, \alpha_n \rangle_R$ : submodule spanned by  
 $\alpha_1, \dots, \alpha_n$ , 302  
 $R[X]_{<\ell}$ : polynomials of degree less than  $\ell$ , 302  
 $M/N$ : quotient module, 303  
 $M \cong M'$ : isomorphic modules, 304  
 $\dim_F(V)$ : dimension, 311  
 $A(i, j)$ :  $(i, j)$  entry of  $A$ , 317  
 $A(i)$ :  $i$ th row of  $A$ , 317  
 $A(\cdot, j)$ :  $j$ th column of  $A$ , 317  
 $R^{m \times n}$ :  $m \times n$  matrices over  $R$ , 317  
 $A^\top$ : transpose of  $A$ , 319  
 $\Psi(y, x)$ : number of  $y$ -smooth integers up to  $x$ ,  
336  
gcd: greatest common divisor (polynomial),  
368  
lcm: least common multiple (polynomial), 370  
 $b/a \bmod n$ : polynomial remainder, 371  
 $a^{-1} \bmod n$ : polynomial modular inverse, 371  
 $(E : F)$ : degree of an extension, 377  
 $R[[X]]$ : formal power series, 379  
 $R((X))$ : formal Laurent series, 380  
 $R((X^{-1}))$ : reversed formal Laurent series, 381  
 $\deg(a)$ : degree of  $a \in R((X^{-1}))$ , 381  
 $\text{lc}(a)$ : leading coefficient of  $a \in R((X^{-1}))$ , 381  
 $\lfloor a \rfloor$ : floor of  $a \in R((X^{-1}))$ , 382  
 $\text{len}$ : length of a polynomial, 399  
 $\text{rep}(\alpha)$ : canonical representative of  
 $\alpha \in R[X]/(n)$ , 400  
 $\mathcal{D}_F(V)$ : dual space, 429  
 $\mathcal{L}_F(V)$ : space of linear transformations, 440  
 $\mathbf{N}_{E/F}(\alpha)$ : norm, 458  
 $\mathbf{Tr}_{E/F}(\alpha)$ : trace, 458

# Index

- Abel's identity, 82
- abelian group, 180
- Adleman, L. M., 175, 179, 358, 488, 500
- Agrawal, M., 489, 500
- Alford, W., 267
- algebra, 359
- algebraic
  - element, 377
  - extension, 377
- Apostol, T. M., 95
- approximately computes, 155
- arithmetic function, 28
- Artin's conjecture, 72
- associate
  - elements of an integral domain, 383
  - polynomials, 366
- associative binary operation, xvi
- asymptotic notation, 33
- Atlantic City algorithm, 156
- automorphism
  - algebra, 360
  - group, 197
  - module, 304
  - ring, 237
  - vector space, 309
- baby step/giant step method, 271
- Bach, E., 73, 95, 179, 266, 281, 289, 298, 487
- basis, 306
- Bayes' theorem, 101
- Bellare, M., 358
- Ben-Or, M., 487
- Berlekamp subalgebra, 478
- Berlekamp's algorithm, 475
- Berlekamp, E. R., 447, 488
- Bernoulli trial, 96
- Bertrand's postulate, 78
- big-O, -Omega, -Theta, 33
- bijection, xv
- bijective, xv
- binary gcd algorithm, 57
- binary operation, xvi
- binary relation, xv
- binomial distribution, 110, 116
- binomial theorem, 214
- birthday paradox, 121
- bivariate polynomial, 228
- Blum, L., 73
- Blum, M., 73
- Boneh, D., 179, 282
- Bonferroni's inequalities, 99
- Boolean circuits, 53
- Brent, R. P., 421
- Brillhart, J., 356
- Buhler, J. P., 357
- Burgess, D. A., 298
- C, 212
- cancellation law
  - for integer congruences, 16
  - for polynomial congruences, 371
  - in an integral domain, 216
- Canfield, E., 357
- canonical representative
  - integer, 48
  - polynomial, 400
- Cantor, D. G., 488
- Cantor-Zassenhaus algorithm, 467
- Carmichael number, 248
- Carmichael, R. D., 267
- Carter, J. L., 147
- Cartesian product, xiv
- ceiling function, 3
- characteristic of a ring, 213
- characteristic polynomial, 458
- Chebyshev's inequality, 118
- Chebyshev's theorem, 74
- Chebyshev's theta function, 76
- Chernoff bound, 119
- Chinese remainder theorem
  - general, 242
  - integer, 18, 62
  - polynomial, 372, 406
- Chistov, A. L., 488
- classification of cyclic groups, 202
- collision probability, 137

- column null space, 331
- column rank, 331
- column space, 331
- column vector, 317
- common divisor
  - in an integral domain, 385
  - integer, 5
  - polynomial, 368
- common multiple
  - in an integral domain, 385
  - integer, 8
  - polynomial, 370
- commutative binary operation, xvi
- commutative ring with unity, 211
- companion matrix, 322
- complex conjugation, 212, 240
- composite, 2
- conditional distribution, 99, 105
- conditional expectation, 114
- conditional probability, 100
- congruence, 13, 190
- conjugacy class, 456
- conjugate, 456
- constant polynomial, 220
- constant term, 223
- continued fraction method, 356
- coordinate vector, 321
  - of a projection, 429
- Coppersmith, D., 357
- Cormen, T. H., 282
- coset, 190
- Crandall, R., 54, 95, 358
- cyclic, 202
  
- Damgård, I., 267, 397
- Davenport, J., 73
- decisional Diffie–Hellman problem, 279
- degree
  - of a polynomial, 223
  - of a reversed formal Laurent series, 381
  - of an element in an extension field, 377
  - of an extension, 377
- $\delta$ -uniform, 136
- Denny, T., 358
- derivative, 227
- deterministic poly-time equivalent, 277
- deterministic poly-time reducible, 277
- diagonal matrix, 319
- dictionary, 126
- Diffie, W., 282
- Diffie–Hellman key establishment protocol, 276
- Diffie–Hellman problem, 276
- dimension, 311
- direct product
  - of algebras, 359
  - of groups, 184
  - of modules, 300
  - of rings, 213
- Dirichlet inverse, 32
- Dirichlet product, 28
- Dirichlet series, 90
  
- Dirichlet’s theorem, 92
- Dirichlet, G., 95
- discrete logarithm, 268
  - algorithm for computing, 270, 337
- discrete probability distribution, 141
- discriminant, 226
- disjoint, xv
- distinct degree factorization, 467, 483
- divides, 1, 213
- divisible by, 1, 214
- division with remainder property
  - integer, 3
  - polynomial, 224, 367
- divisor, 1, 214
- Dixon, J., 356
- Dornstetter, J. L., 447
- dual space, 429
- Durfee, G., 179
  
- Eisenstein integers, 389
- Eisenstein’s criterion, 395
- elementary row operation, 325
- elliptic curve method, 357
- equal degree factorization, 469, 475
- equivalence class, xv
- equivalence relation, xv
- Eratosthenes
  - sieve of, 85
- Erdős, P., 357
- error correcting code, 69, 412
- error probability, 155
- Euclidean algorithm
  - extended
    - integer, 58
    - polynomial, 403
  - integer, 55
  - polynomial, 402
- Euclidean domain, 387
- Euler’s identity, 89
- Euler’s phi function, 24
  - and factoring, 263
- Euler’s theorem, 26
- Euler, L., 94
- event, 97
- execution path, 150
- exp, xiv
- expected polynomial time, 149
- expected running time, 149
- expected value, 111
- exponent, 206
  - module, 305
- extended Euclidean algorithm
  - integer, 58
  - polynomial, 403
- extended Gaussian elimination, 327
- extension field, 219, 376
- extension ring, 218
  
- factoring
  - and Euler’s phi function, 263
- factoring algorithm

- integer, 344, 352
  - deterministic, 421
  - polynomial, 467, 475
    - deterministic, 483
- fast Fourier transform, 417
- Fermat's little theorem, 27
- FFT, 417
- field, 215
- field of fractions, 363
- finite dimensional, 311
- finite extension, 376
- finite fields
  - existence, 450
  - subfield structure, 454
  - uniqueness, 454
- finite probability distribution, 96
- finitely generated
  - abelian group, 202
  - module, 306
- fixed field, 455
- floor function, 3
  - reversed formal Laurent series, 382
- formal derivative, 227
- formal Laurent series, 380
- formal power series, 379
- Fouvry, E., 500
- Frandsen, G., 397
- Frobenius map, 451
- fundamental theorem of arithmetic, 2
- fundamental theorem of finite abelian groups, 208
- fundamental theorem of finite dimensional  $F[X]$ -modules, 445
- von zur Gathen, J., 422, 488
- Gauss' lemma, 285
- Gaussian elimination, 325
- Gaussian integers, 219, 240, 387, 390
- gcd
  - integer, 6
  - polynomial, 368
- generating polynomial, 424
- generator, 202
  - algorithm for finding, 268
- geometric distribution, 142, 145
- Gerhard, J., 422, 488
- Goldwasser, S., 298
- Gordon, D. M., 358
- Gordon, J., 488
- Granville, A., 267
- greatest common divisor
  - in an integral domain, 385
  - integer, 6
  - polynomial, 368
- group, 180
- guessing probability, 137
- Guy, M., 73
- Hadamard, J., 94
- Halberstam, H., 267
- Hardy, G. H., 94, 95
- hash function, 125
  - universal, 127
- hash table, 126
- Heath-Brown, D., 95
- Hellman, M., 282
- Hensel lifting, 294
- homomorphism
  - algebra, 360
  - group, 194
  - module, 303
  - ring, 236
  - vector space, 309
- Horner's rule, 400
- Huang, M.-D., 500
- hybrid argument, 135
- Hypothesis H, 93
- ideal, 4, 231
  - generated by, 4, 231
  - maximal, 234
  - prime, 234
  - principal, 4, 231
- identity element, 180
- identity matrix, 319
- image, xv
- image of a random variable, 104
- Impagliazzo, R., 147
- inclusion/exclusion principle, 99
- index, 191
- index calculus method, 358
- indicator variable, 105
- infinite extension, 377
- infinite order, 183
- injective, xv
- integral domain, 215
- inverse
  - multiplicative, 214
  - of a group element, 180
  - of a matrix, 323
- inverse function, xvi
- invertible matrix, 323
- irreducible element, 383
- irreducible polynomial, 366
  - algorithm for generating, 464
  - algorithm for testing, 462
  - number of, 453
- isomorphism
  - algebra, 360
  - group, 197
  - module, 304
  - ring, 236
  - vector space, 309
- Iwaniec, H., 281
- Jacobi map, 289
- Jacobi sum test, 500
- Jacobi symbol, 287
  - algorithm for computing, 290
- joint distribution, 105
- $k$ -wise independent, 105

- Kalai, A., 179
- Kaltofen, E., 488
- Karatsuba, A. A., 53
- Kayal, N., 489, 500
- kernel, 194
- kills, 206
- Kim, S. H., 267
- Knuth, D. E., 53, 54, 73
- von Koch, H., 94
- Kronecker substitution, 416
- Kung, H. T., 421
  
- Lagrange interpolation formula, 372
- Las Vegas algorithm, 157
- law of large numbers, 118
- law of quadratic reciprocity, 285
- lcm
  - integer, 9
  - polynomial, 370
- leading coefficient, 223
  - of a reversed formal Laurent series, 381
- least common multiple
  - in an integral domain, 385
  - integer, 9
  - polynomial, 370
- leftover hash lemma, 138
- Legendre symbol, 285
- Lehmann, D., 267
- Lehmer, D., 356
- Leiserson, C. E., 282
- len, 46, 399
- length
  - of a polynomial, 399
  - of an integer, 46
- Lenstra, Jr., H. W., 357, 488
- Levin, L., 147
- li, 87
- linear map, 303
- linear transformation, 440
- linearly dependent, 306
- linearly generated sequence, 423
  - minimal polynomial of, 424
  - of full rank, 429
- linearly independent, 306
- little-o, 33
- Littlewood, J. E., 95
- log, xiv
- logarithmic integral, 87
- lowest terms, 9
- Luby, M., 147, 179
  
- Markov's inequality, 117
- Massey, J., 447
- matrix, 316
- Maurer, U., 267
- maximal ideal, 234
- memory cells, 36
- Menezes, A., 73, 179
- Mertens' theorem, 83
- message authentication scheme, 128
- Micali, S., 298
  
- Miller, G. L., 266, 267
- Miller–Rabin test, 247
- Mills, W., 421, 447
- min entropy, 137
- minimal polynomial, 374
  - algorithm for computing, 401, 438, 466
  - of a linear transformation, 441
  - of a linearly generated sequence, 424
  - of a vector under a linear transformation, 442
- Möbius function ( $\mu$ ), 29
- Möbius inversion formula, 30
- mod, 3, 13, 17, 224, 371
- modular square root, 283
  - algorithm for computing, 292
- module, 299
- modulus, 13
- monic associate, 366
- monic polynomial, 223
- monomial, 227, 229, 230
- Monte Carlo algorithm, 156
- Morrison, K., 447
- Morrison, M., 356
- multi-variate polynomial, 230
- multiple root, 226
- multiplication map, 194, 212, 305
- multiplicative function, 28
- multiplicative group of units, 214
- multiplicative inverse, 23
  - in a ring, 214
  - modulo integers, 15
  - modulo polynomials, 371
- multiplicative order, 26, 202
- multiplicative order modulo  $n$ , 26
- multiplicity, 226
- mutually independent
  - events, 100
  - random variables, 105
  
- natural map, 197
- Newton interpolation, 406
- Newton's identities, 383
- Niven, I., 289
- non-constant polynomial, 220
- non-trivial ring, 213
- norm, 213, 458
- normal basis, 461
- number field sieve, 357
  
- Oesterlé, J., 95
- one-sided error, 157
- van Oorschot, P., 73, 179, 282
- order
  - in a module, 305
  - of a group element, 202
  - of an abelian group, 183
- ordered basis, 321
  
- pairwise disjoint, xv
- pairwise independent
  - events, 100

- hash function, 125
- random variables, 105
- pairwise relatively prime
  - integer, 9
  - polynomial, 370
- partition, xv
- Penk, M., 73
- perfect power, 261
- period, 71
- periodic sequence, 71
- phi function of Euler, 24
- PID, 388
- pivot element, 326
- pivot sequence, 324
- Pohlig, S., 282
- Pollard, J. M., 282, 357
- polynomial
  - associate, 366
  - irreducible, 366
  - monic, 223
  - primitive, 392
  - reducible, 366
- polynomial evaluation map, 238, 361
- polynomial time, 38
  - expected, 149
  - strict, 149
- Pomerance, C., 54, 95, 267, 357, 358, 500
- de la Vallée Poussin, C.-J., 94, 95
- power map, 194
- pre-image, xv
- pre-period, 71
- prefix free, 150
- primality test
  - deterministic, 489
  - probabilistic, 244
- prime
  - ideal, 234
  - in an integral domain, 386
  - number, 2
- prime number theorem, 86
  - irreducible polynomials over a finite field, 453
- primitive polynomial, 392
- principal ideal, 4, 231
- principal ideal domain, 388
- probabilistic algorithm, 148
- probability distribution
  - conditional, 99
  - discrete, 141
  - finite, 96
- probability function, 96
- product distribution, 98
- program, 36
- projection, 429
- public key cryptography, 282
- purely periodic, 71
- $\mathbb{Q}$ , 9
- quadratic formula, 226
- quadratic reciprocity, 285
- quadratic residue, 283
- quadratic residuosity
  - algorithm for testing, 291
  - assumption, 297
- quadratic sieve, 353
- quantum computer, 358
- quotient algebra, 359
- quotient group, 191
- quotient module, 303
- quotient ring, 232
- quotient space, 309
- $\mathbb{R}$ , 212
- Rabin, M. O., 266
- Rackoff, C., 357
- RAM, 36
- random access machine, 36
- random self-reduction, 178
- random variable, 104
  - conditional distribution of, 105
  - conditional expectation, 114
  - distribution of, 105
  - expected value, 111
  - image, 104
  - independent, 105
  - joint distribution, 105
  - $k$ -wise independent, 105
  - mutually independent, 105
  - pairwise independent, 105
  - real, 104
  - variance, 113
- randomized algorithm, 148
- rank, 331
- rational function field, 366
- rational function reconstruction, 410
- rational reconstruction, 66
- real random variable, 104
- recursion tree, 282
- Redmond, D., 95
- reduced row echelon form, 324
- reducible polynomial, 366
- Reed, I., 421
- Reed–Solomon code, 69, 412
- relatively prime
  - in an integral domain, 385
  - integers, 6
  - polynomials, 368
- Renyi entropy, 137
- rep, 48, 400
- repeated-squaring algorithm, 49
- representation, 278
- representative
  - of a coset, 190
  - of a residue class, 21
  - of an equivalence class, xv
- residue class, 20, 232
- residue class ring, 232
- reversed formal Laurent series, 381
- Richert, H., 267
- Riemann hypothesis, 88, 90, 92, 94, 266, 267, 281, 298, 419, 488
- Riemann's zeta function, 88

- Riemann, B., 94
- ring, 211
- ring of polynomials, 220
- Rivest, R. L., 175, 179, 282
- Rogaway, P., 358
- root of a polynomial, 224
- Rosser, J., 94
- row echelon form, 333
- row null space, 329
- row rank, 331
- row space, 329
- row vector, 317
- RSA cryptosystem, 175
- Rumely, R. S., 500
  
- sample mean, 118
- sample space, 96
- Saxena, N., 489, 500
- scalar, 299
- scalar matrix, 319
- scalar multiplication, 299
- Schirokauer, O., 358
- Schoenfeld, L., 94
- Schönhage, A., 53, 54, 73
- Scholtz, R., 447
- secret sharing scheme, 407
- Semaev, I. A., 488
- separating set, 484
- Shallit, J., 95, 289, 487
- Shamir, A., 52, 175, 179, 421
- Shanks, D., 282
- shift register sequence, 425
- Shor, P., 358
- Shoup, V., 281, 447, 487, 488
- Shub, M., 73
- sieve of Eratosthenes, 85
- simple root, 226
- smooth number, 336, 352
- Solomon, G., 421
- Solovay, R., 266, 298
- solving linear congruences
  - integer, 17
  - polynomial, 371
- Sophie Germain prime, 93
- splitting field, 378
- square root (modular), 283
  - algorithm for computing, 292
- square-free
  - integer, 10
  - polynomial, 449
- square-free decomposition algorithm, 476, 485
- standard basis, 306
- statistical distance, 131
- Stein, C., 282
- Stein, J., 73
- Strassen, V., 54, 266, 298
- strict polynomial time, 149
- subalgebra, 360
- subfield, 219
- subgroup, 185
  - generated by, 202
- submodule, 301
  - generated (or spanned) by, 302
- subring, 218
- subspace, 309
- surjective, xv
  
- theta function of Chebyshev, 76
- total degree, 229, 230
- trace, 458
- transcendental element, 377
- transpose, 319
- trial division, 244
- trivial ring, 213
- twin primes conjecture, 94
- two-sided error, 157
  
- UFD, 384
- ultimately periodic sequence, 71
- unique factorization
  - in a Euclidean domain, 387
  - in a PID, 388
  - in  $D[\mathbf{x}]$ , 392
  - in  $F[\mathbf{x}]$ , 367
  - in  $\mathbb{Z}$ , 2
- unique factorization domain, 384
- unit, 214
- universal family of hash functions, 127
  
- Vandermonde matrix, 373
- Vanstone, S., 73, 179
- variance, 113
- vector, 299
- vector space, 309
  
- Walfisz, A., 94
- Wang, P., 73
- Wang, Y., 281
- Weber, D., 358
- Wegman, N. M., 147
- Weilert, A., 397
- Welch, L., 447
- well-behaved complexity function, 51
- Wiedemann, D., 447
- Wiener, M., 179, 282
- Wright, E. M., 94, 95
  
- Yun, D. Y. Y., 488
  
- $\mathbb{Z}$ , 1
- Zassenhaus, H., 488
- zero divisor, 215
- zero-sided error, 157
- zeta function of Riemann, 88
- Zuckerman, H., 289
- Zuckermann, D., 147