

Index

- $1/q$ -sequence, 265
 μ_N , *see* root of unity
 $\phi(N)$, *see* Euler totient function
 $\varphi_N(\mathbf{a})$, *see* N -adic complexity
 $\varphi(\mathbf{a})$, *see* complexity, π -adic
 $\Phi(f, g)$, *see* Weil height
 π -adic number, 98–471
 as inverse limit, 464
- Abelian group, 407
 fundamental theorem, 413
 action of a group, 410
 add with carry, 90
 additive character, 439
 adic topology, 470
 adjugate, 161
 AFSR, 96, 131, 250–263
 function field, 112
 memory, 108–114
 period, 114–115
 synthesis, 347–375
 algebra, over a ring, 425
 algebraic
 closure, 432
 curve, 452
 feedback shift register, *see* AFSR
 integer, 449
 model, 21, 45, 253
 number field, *see* number field
 algebraic element, 431
 algebraic immunity, 168
 algorithm
 Berlekamp–Massey, 296–304, 334, 347
 Euclidean, 338, 351, 420, 458
 complexity of, 421
 register synthesis, 295
 alphabet, 15
 annihilator, 414
 Antheil, George, 184
 aperiodic state, 20
- approximation lattice, 328, 335, 341, 479
 approximation, degree i , 298
 arithmetic code, 265, 335
 arithmetic correlation, 178–184
 arithmetic shift and add, 204–206, 265
 array, pseudo-noise, 212
 Artin’s conjecture, 265, 417
 Artin’s constant, 266
 associate elements, 418
 $\text{Aut}(S)$, 415
 autocorrelation, 168, 175, 192, 209, 230–240
 arithmetic, 178, 271
 Hamming, 185
 ideal, 175
 automorphism, 408, 415
 average
 correlation, 176–184
 average complexity, 376–388
 AWC, 90
- balanced, 168, 170, 269
 with respect to a character, 171
 Barrows code, 265
 basic irreducible polynomial, 245, 454
 basis, 424, 425
 bent function, 216, 314
 bent sequence, 216, 229, 314
 Berlekamp–Massey algorithm, 296–304, 334, 347
 Bézout coefficients, 421
 Blackburn’s theorem, 194
 Blahut’s theorem, 304–313
 block (in a sequence), 169, 267
 bound
 Deligne, 440
 singleton, 188
 sphere packing, 189
 Weil, 439–440
 Welch, 230
- carry, 71, 72
 delayed, 103

492

Cauchy sequence, 467
 CDMA, 7
 character, 214–226, 410
 additive, 439
 Dirichlet, 239
 multiplicative, 439
 quadratic, 239, 439, 443
 character sum, 218, 439
 characteristic (of a ring), 416
 characteristic polynomial, 27–28
 Chinese remainder theorem, 423
 class number, 450
 clock-controlled generator, 317
 cascaded, 317
 self-clocking, 318
 closed
 algebraically, 432
 integrally, 450
 translationally, 188
 code
 arithmetic, 265, 335
 Barrows–Mandelbaum, 265
 Reed–Muller, 209, 244
 coefficient
 Bézout, 421
 of N -adic integer, 72
 of a power series, 32
 collision, 6, 185
 combiner, 315
 summation, 316
 companion matrix, 28
 complete
 metric space, 467
 set of representatives, 96, 100
 valued field, 468
 completion, 467–471
 complexity
 average, 376–388
 linear, *see* linear complexity
 N -adic, *see* N -adic complexity
 π -adic, 349
 conjugacy class, 410
 connection
 element, 70, 98, 134
 integer, 71, 155
 polynomial, 27, 70, 152
 continued fraction, 472–479
 and Berlekamp–Massey, 302–304, 334
 convergent, 473
 expansion, 473, 476
 Laurent series, 475
 periodic, 475
 convergent, of a continued fraction, 473, 476
 convex set, 426
 convolution, 412
 coordinates, 463
 coprime, 101, 418, 457
 correlation, 175–178, 230–240

Index

 and Fourier transform, 215
 arithmetic, 178–184
 attack, 9, 316
 auto, *see* autocorrelation
 cross, *see* cross-correlation
 expectation values, 176–184
 Hamming, 6, 185
 correlation immunity, 168
 coset, 409
 cyclotomic, *see* cyclotomic coset
 cross-correlation, 7, 175, 217–226, 230–240
 arithmetic, 178, 271
 Hamming, 185, 241
 cryptography, 167
 curve
 algebraic, 452
 elliptic, 226
 cuspidal cubic, 263
 cyclic group, 408, 416
 cyclotomic coset, 116, 205, 380, 437
 $C_u(\pi)$, 116
 cyclotomic field, 437

 D_U , 425
 d -FCSR, 121, 133–150, 157, 283–292
 ℓ -sequence, 284
 norm, 137
 period, 140
 d -form sequence, 239
 de Bruijn sequence, 172, 193, 208, 256
 modified, 173
 pseudonoise, 173
 punctured, 173, 208
 decimation, 210, 217, 231, 272
 linear, 219
 quadratic, 220, 232
 Dedekind domain, 450
 degenerate state, 84
 $\deg_\pi(v)$, 113
 degree
 of a linear recurrence, 24, 71
 of an extension, 432
 of nilpotency, 455
 π -adic, 113
 delayed carry, 103
 Deligne bound, 440
 derivative
 formal, 306
 Hasse, 306, 380
 determinant
 of a lattice, 425
 DFT, 413
 Diaconis mind-reader, 226
 directed system, 427
 Dirichlet
 character, 239
 sequence, 239
 discrepancy, 298, 344, 347

- discrete Fourier transform, 413, 441–442
- discrete state machine, 20
- discrete valuation, 465
- distribution of blocks, 168, 170
- $\text{div } \pi$, 97, 101, 134
- $\text{div } N$, 70, 73
- divisibility, 420
 - in $R[x]$, 457
- division
 - of polynomials, 153, 429
- divisor, 418
- domain, 414
 - Dedekind, 450
 - Euclidean, 351, 419
 - integral, 414, 419, 466
 - principal ideal, 419
- dual vector space, 424
- element
 - connection, 70, 134
- elliptic curve, 226
- endomorphism, 408, 415
- entire ring, 414, 419, 466
- epimorphism, 408, 415
- equation, quadratic, 438
- equidistributed, 170, 172, 196, 208, 267
- Euclidean
 - algorithm, 338, 351, 420, 458
 - complexity of, 421
 - for rational approximation, 338
 - domain, 351, 419
 - ring, 351, 419
- Euler totient, 416
- eventually periodic, 15, 20, 34
- exact sequence, 409
 - split, 409
- expansion
 - power series, 33
- exponential representation, 21
- exponential sum, 439
- extension
 - Galois, 433, 435
 - of degree d , 460
 - of fields, 432
 - of rings, 415, 459
 - ramified, 459
 - unramified, 459
- \mathcal{F} -span, 295
- $F_{\geq 0}$, 466
- F^{∞} , 54
- factorization ring, 419, 450
- family of recurring sequences, 53, 60
- FCSR, 69–90, 98
 - d -, 133, 157
 - Galois mode, 154
 - synthesis, 322–346
- feed forward function, 312
- feedback function, 24
- feedback with carry shift register, *see* FCSR
- Fermat's congruence, 417
- FH, *see* frequency hopping
- Fibonacci
 - mode, 23
 - sequence, 16–18, 65, 67, 94, 163
- field, 414, 439
 - cyclotomic, 437
 - extension, 432
 - finite, 434–438
 - function, 36, 250–263
 - Galois, 435
 - global, 452
 - local, 451, 468
 - number, 109, 448
 - p -adic, 74, 451
 - residue, 415, 453, 466
 - valued, 466
- filter
 - nonlinear, 312
- finite field, 434–438
- finite local ring, 244, 453–463
 - units in, 454
- formal
 - derivative, 306
 - Laurent series, 33, 466
 - power series, 32–37, 466
- Fourier inversion formula, 412
- Fourier transform, 412, 413, 439
 - and linear span, 304
 - and m -sequences, 214–217
 - discrete, 413, 441–442
 - generalized, 307
- fraction field, 423
- fraction, continued, *see* continued fraction
- fractional linear transformation, 475
- fractions (localization), 422
- frequency hopping, *see* Hamming correlation
- full lattice, 425
- function
 - bent, 216, 314
 - feed forward, 312
 - generating, 39
 - rational, 33
- function field, 112, 250–263, 360
 - global, 36, 452
 - local, 451
 - rational, 111
 - sequence, 242
- Fundamental theorem
 - Abelian groups, 413
 - on AFSRs, 106
- Galois
 - conjugates, 199, 436
 - extension, 433, 435, 459
 - field, 434–438

494

group, 432, 435
 of a finite local ring, 459
 mode, 151–157
 ring, 247, 453–463
 Galois mode
 FCSR, 154
 LFSR, 151
 Gauss sum, 439
 gcd, 418, 447
 gcd ring, 419
 GDFT, 307, 380
 Geffe generator, 315
 generating function, 39, 297
 generator
 clock-controlled, 317
 combiner, 316
 of a sequence, 20
 shrinking, 318
 step-once-twice, 317
 stop-and-go, 317
 threshold, 316
 geometric sequence, 235
 global field, 452
 global positioning system, 248
 GMW sequence, 237
 Gold sequence, 232
 golden mean, 66
 Golomb's randomness postulates, 167
 GPS, 248
 group, 407
 Abelian, 407
 structure of, 413
 action, 410
 character, 410
 cyclic, 408
 direct product of, 407, 413
 finite Abelian, 413
 Galois, 432, 435
 homomorphism, 408
 multiplicative, 416
 order, 407
 order of an element, 408
 quotient, 409
 torsion element of, 413
 torsion-free, 413
 Günther weight, 307, 380
 Günther-Blahut Theorem, 308
 Hadamard
 product, 312
 transform, 439
 Hamming correlation, 6, 185, 241, 247
 Hasse derivative, 306, 380
 Hasse matrix, 308
 height
 π -adic, 349
 Weil, 323, 335
 Hensel codes, 335

Index

Hensel's Lemma, 470
 $\text{Hom}_{\mathbb{F}}(V, W)$, 424
 homomorphism, 408
 of sequence generators, 20
 ring, 415
 hyperderivative, 306
 Hypothesis H1,H2,H3, 112, 361
 $I(\mathbf{a})$, 54
 ideal autocorrelation, 175
 ideal, principal, 415
 image (of a homomorphism), 408
 imbalance, 170, 178, 192, 215, 236, 269, 271
 index (of a subgroup), 409
 index function, 349
 inequality, triangle, 467
 integer
 algebraic, 449
 connection, 70, 71
 in a number field, 450
 N -adic, 72
 N -adic, *see* N -adic number
 integral domain, 414, 419, 466
 integral quotient, 101
 integrally closed, 450
 interleaving, 42, 140, 369
 and m -sequence, 211
 interpolation set, 350
 inverse limit, 36, 427, 464
 π -adic number as, 464
 N -adic integer as, 76
 power series as, 37
 inversion formula, 412
 invert (a multiplicative subset), 422
 irreducible element, 418
 isomorphism, 408
 isotropy subgroup, 410
 Kasami sequence, 233
 kernel, 408, 415
 kernel property, 197, 257
 key equation, 297
 keystream generator, 9
 Kloosterman sum, 226
 Kolmogorov complexity, 169
 Lamarr, Hedy, 184
 lattice, 335–337, 425
 approximation, 328, 335, 341, 479
 full, 425
 minimal basis, 336
 volume of, 425
 Laurent series, 33, 466, 475, 479
 reciprocal, 37
 lcm, 418
 least degree, 72
 of a power series, 32
 Legendre

- sequence, 239
- symbol, 239, 439
- Lemma, Hensel's, 470
- LFSR, 23–65, 98
 - definition of, 23
 - Galois mode, 151–157
 - synthesis problem, 298
- limit, inverse, 36, 427
- linear
 - complexity, 25, 168, 296
 - average, 377, 380
 - decimation, 219
 - feedback shift register, *see* LFSR
 - function, 424
 - recurrence, 24, 33
 - with carry, 71, 97
 - with delay, 134
 - register, 160, 311
 - span, *see* linear complexity
 - and Fourier transform, 304
- linearly recurrent sequence, *see* linear recurrence
- local field, 451, 468
- local ring, 419, 453–463, 466
- localization, 423
- ℓ -sequence, 69, 205, 256, 264–276, 284
 - and de Bruijn sequences, 267
 - arithmetic correlation, 271–275
 - distributional properties, 267–271
 - imbalance, 271
- Lucas sequence, 67

- M_U , 425
- m-sequence, 64, 70, 172, 175, 194, 196, 208–227, 246, 258
- machine state, 24
- Mandelbaum code, 265
- Maple, 266
- Marky, Hedy, 184
- matching, perfect, 67
- matrix, companion, 28
- maximal sequence, 244
- maximum order complexity, 329
- memory requirements
 - AFSR, 108
 - FCSR, 88
- metric space, 467
- minimal basis, 336
- minimal polynomial, 55, 431
- Minkowski's theorem, 426
- ML sequence, 247
- Möbius
 - function, 427
 - inversion, 426
- mod, 101
- mode
 - Fibonacci, 23
 - Galois, 151–157
- model, of a sequence generator, 21, 45, 253

- modular shift register, 151
- module, 424
- monic, 429
- monomorphism, 408, 415
- Monte Carlo, 167
- multiplicative
 - group, 416
 - order, 414
 - subset, 422
- multiply with carry, 71, 90–94
- MWC, *see* multiply with carry

- N_R^S , *see* norm
- N -adic complexity, 168, 322–329
 - average, 384
 - of an m-sequence, 327
 - profile, 328
 - symmetric, 329–333
- N -adic number, 72–75, 79
 - as inverse limit, 76
 - coefficient, 72
 - periodic, 73
 - reduction modulo N , 73
- N -adic span, *see* N -adic complexity
- N -ary sequence, 15
- Nakayama's lemma, 454
- negative pair, 335
- Newton interpolation, 344
- nilpotent element, 454, 457
- Noetherian ring, 419
- nonlinear combiner, 315
- nonlinear filter, 312
- nonlinear span, 174
- nonlinearity, 168
- norm, 137, 433, 438, 449, 450
 - of rings, 460
- number
 - N -adic, *see* N -adic number
 - p -adic, *see* p -adic number
 - Fibonacci, *see* Fibonacci
- number field, 109, 448
 - order in, 109, 449

- occurrence (of a block), 169, 172, 208, 267
- orbit, 410
- ord, 417
- order
 - in a number field, 109, 449
 - multiplicative, 414, 417
 - of a group, 407
 - of a polynomial, 28, 430
 - of an element, 408
- orthogonality (of characters), 412

- p -adic field, 74, 451
- p -adic number, *see* N -adic number
- parallelepiped
 - closed –, 141

496

face of $-$, 144
 half open $-$, 141
 open $-$, 286
 Pari, 266
 Parseval's formula, 413
 perfect matching, 67
 period, 15, 168
 periodic, 15
 continued fraction, 475
 eventually, 15, 34
 state, 20, 88
 phase shift, 66
 phase taps, 66, 248
 PID, *see* principal ideal domain
 Pollard's algorithm, 344
 polynomial
 basic irreducible, 245, 454
 characteristic, 27–28
 connection, 24, 27, 70, 152
 minimal, 55
 primitive, 208, 436, 461
 reciprocal, 27, 37
 regular, 454
 ring, 419, 428
 positive pair, 335
 power series, 32–37
 as inverse limit, 37
 expansion, 33
 primary
 element, 418
 ideal, 415, 458
 prime
 element, 418
 ideal, 415
 in a finite local ring, 457
 relatively, 101, 418
 primitive
 element, 64, 436
 polynomial, 208, 436, 461
 root, 264–266, 417
 principal ideal, 415
 principal ideal domain, 419
 product, Hadamard, 312
 \mathbb{Q}_p , *see* p -adic field
 quadratic
 character, 239, 439, 443
 decimation, 220, 232
 equation, 438
 form, 438, 442
 residue (sequence), 239
 span, 25
 quotient
 group, 409
 in $R[x]$, 429
 in a ring, 419
 $R_0(x)$, 33

Index

R_π , 99
 $R((x))$, *see* Laurent series
 $R[[x]]$, *see* power series
 $R[x]$, *see* polynomial ring
 radar, 167
 ramified extension, 459
 random number, 167
 randomness postulates, Golomb's, 167
 rank, 424
 of a quadratic form, 443
 rational
 function, 33, 36
 representation, 113
 rational approximation, 334–345, 347
 Euclidean algorithm, 338
 in function fields, 360
 in quadratic extensions, 363–369
 in ramified extensions, 362
 in \mathbb{Z} , 352–353
 reciprocal
 Laurent series, 37
 polynomial, 27, 37
 recurrence
 inhomogeneous linear, 67
 linear, 24, 33
 family of, 53, 60
 with carry, 71, 97
 second order linear homogeneous, 22, 67
 reduction (modulo p), 101
 Reed–Muller code, 209, 244
 register synthesis, 295
 algorithm, 295–304
 register, linear, 160, 311
 regular
 element, 457
 polynomial, 454
 relatively prime, 101, 418
 remainder
 in $R[x]$, 429
 in a ring, 419
 representatives, complete set of, 96, 100
 residue, 416
 residue field, 415, 453, 466
 resilience, 168
 reversal
 of a polynomial, 329
 of a sequence, 329
 of an integer, 330
 Riemann hypothesis, 265
 ring, 21, 414
 commutative, 414
 discrete valuation, 465
 entire, 414, 419, 466
 Euclidean, 351, 419
 extension, 459
 factorial, 419
 factorization, 419, 450
 finite local, 244, 453–463

- unit, 454
- Galois, 247, 453–463
- GCD, 419
- integral domain, 414, 419, 466
- local, 419, 466
- Noetherian, 419
- of fractions, 423
- polynomial, 419, 428
- principal, 419
- valuation, 466
- ring homomorphism, 415
- ring LFSR, 161
- root
 - of a polynomial, 429
 - of unity, 436, 441
 - primitive, 264–266, 417
 - simple, 430
- run, 170
- run property, 172, 208
- Schönage–Strassen algorithm, 344
- second order linear homogeneous recurrence, 22
- security measures, 376
- self decimation generator, 318
- separable (ring), 471
- $\text{seq}(a)$, $\text{seq}_\pi(a)$, 32, 39, 99, 105, 347
- $\text{seq}_N(a)$, 73
- sequence, 15–21
 - d -form, 239
 - add with carry, 90
 - bent, 216, 229, 314
 - Cauchy, 467
 - de Bruijn, *see* de Bruijn sequence
 - Dirichlet, 239
 - eventually periodic, 15
 - exact, 409
 - Fibonacci, 65, 67, 94, 163
 - function field, 242
 - generator, 20, 295
 - homomorphism, 20
 - geometric, 235
 - GMW, 237
 - Gold, 232
 - Kasami, 233
 - ℓ -, 69, 256
 - Legendre, 239
 - linearly recurrent, *see* linear recurrence
 - Lucas, 67
 - m -, 64, 70, 172, 194, 196, 208–227, 258
 - maximal, 244
 - ML, 247
 - multiply with carry, 71, 90–94
 - periodic, 15
 - quadratic residue, 239
 - reversal, 329
 - shifted, 188
 - strictly periodic, 15
 - translated, 188, 241
 - window, 196
- shift
 - of a sequence, 18
 - phase, 66
- shift and add, 191–207
 - and autocorrelation, 192
 - and balance, 193
 - and punctured de Bruijn, 198
 - arithmetic, 204–206, 265
 - over a prime field, 194
 - with coefficients in a ring, 192
- shift and subtract, 192
- shift distinct, 18, 188, 198, 210, 232, 241, 259
- shift register, *see* LFSR, FCSR, AFSR
 - modular, 151
- shift-equivalent, 18
- shifted sequence, 188
- short exact sequence, 409, 415
- shrinking generator, 318
- signature, 6
- simple root, 430
- singleton bound, 188
- $\text{SL}(2, \mathbb{Z})$, 475
- space, metric, 467
- span, 295
 - linear, *see* linear complexity
 - N -adic, *see* N -adic complexity
 - nonlinear, 174
 - of a recurrence, 24, 71
- spectral test, 90
- sphere packing bound, 189
- split (exact sequence), 409
- spread spectrum, 6
- $S^{-1}R$ (localization), 422
- stabilizer, 410
- Stark–Heegner Theorem, 450
- state
 - aperiodic, 20
 - degenerate, 84
 - eventually periodic, 20
 - periodic, 20, 88
- states, set of
 - closed, 20
 - complete, 20
 - discrete, 20
- step-once-twice generator, 317
- stop-and-go generator, 317
 - cascaded, 318
- strictly periodic sequence, 15
- strong N -prime, 320
- subgroup, isotropy, 410
- successive minima, 335
- sum
 - character, 218, 439
 - exponential, 439
 - Gauss, 439
 - Kloosterman, 226
- summation combiner, 311, 316, 345–346

498

symbol, Legendre, 439

test, spectral, 90

threshold generator, 316

topology, adic, 470

torsion element, 413

torsion-free, 413

totient, Euler, 416

Tr_R^S , *see* trace

trace, 48, 433, 438, 449
 of rings, 460

transform
 Fourier, 412, 413, 439
 and m-sequences, 214–217
 discrete, 413, 441–442
 Hadamard, 439
 Walsh, 439

transitive action, 410

translated sequence, 188, 241

translationally closed, 188

transpose, 424

triangle inequality, 467

turning point, 299, 354

UFD, 419

unit, 414, 418, 457
 in a finite local ring, 454

unity, root of, 436, 441

unramified extension, 459

Index

valuation
 and metric space, 468
 discrete, 465
 on a ring, 465

valuation ring, 466

valued field, 466

vector space, 423
 dual, 424

volume (of a lattice), 425

V_q , 115

Walsh transform, 439

weight, Günther, 307, 380

Weil
 bound, 439–440
 height, 323, 335

Welch bound, 230

window sequence construction, 196

Xu's algorithm, 348–375

$\mathbb{Z}/(N)$, 416–418, 455

$\mathbb{Z}[\pi]$, 133

\mathbb{Z}_N , 72

$\mathbb{Z}_{N,0}$, 75

\mathbb{Z}_π , 137

zero divisor, 414, 457

zeta function, 265

Zierler, 53, 194