

Index

- algébriquement indépendants, 268
- algorithme
 - crible quadratique, 225
 - d'Euclide, 559
 - de Berlekamp, 294
 - de Fermat, 220
 - de Fibonacci, 24
 - de Golomb, 25
 - de Lenstra, 230
 - de Pollard, 221, 222, 533
 - de Shanks, 227
 - de Williams, 221, 533
- anneau
 - de Dedekind, 422
 - des entiers, 414
 - euclidien, 61
- arbre
 - de Calkin-Wilf, 120
 - de Stern-Brocot, 111
- axiome
 - de l'infini, 129
 - de Zermelo-Fraenkel, 126
- base
 - de transcendance, 268
- Bezout
 - relation, 9, 11, 12, 101, 111
- biais de Tchébychev, 254
- borne
 - inférieure, 86
 - supérieure, 86, 128
- caractère, 492
- cardinal, 130
- cercle
 - de Ford, 124
- clôture
 - algébrique, 273
 - galoisienne, 310
 - intégrale, 414
 - normale, 310
- code
 - AES, 527
 - authentification, 530
 - BCH, 557
 - borne du singleton, 553
 - capacité de correction, 552
 - CD, 561
 - César, 510
 - correcteur, 551
 - de Hamming, 554, 559
 - de Reed-Solomon, 560
 - distance de Hamming, 552
 - El Gamal, 534
 - Hill, 512, 564
 - linéaire, 553
 - cyclique, 555
 - matrice
 - de contrôle, 554
 - génératrice, 553
 - vérificatrice, 553
 - minitel, 560
 - parfait, 552
 - quadratique, 563
 - RSA, 529
 - Scytale, 509
 - signature, 530, 535, 539, 543
 - systematique, 554
 - taux d'information, 551
 - Vernam, 522
 - VIC, 514
 - Vigenère, 512
- complet, 85
- conducteur
 - d'un semi-groupe, 18
- congruence, 11
- conjecture
 - $P \neq NP$, 519
 - abc, 255
 - d'Artin, 16
 - de Cramer, 194
 - de Erdős-Straus, 28

- de Goldbach, 256
- de Hardy et Littlewood, 192
- de Hasse-Weil, 256
- de Polignac, 254
- de Vinogradov, 48
- de Wilf, 20
- corps
 - archimédien, 84
 - caractéristique, 265
 - cyclotomique, 323, 393, 461
 - de classes de Hilbert, 206, 456, 463
 - de décomposition, 272
 - de rupture, 270
 - discriminant, 415
 - extension
 - algébrique, 266
 - composée, 312
 - de Carlitz, 367
 - de type fini, 265
 - degré, 264
 - degré de transcendance, 269
 - galoisienne, 306
 - monogène, 265
 - normale, 305
 - norme, 411
 - norme absolue, 415
 - radicale, 319
 - résoluble, 319
 - séparable, 301, 302
 - trace, 411
 - trace absolue, 415
 - transcendante, 266
 - extensions, 264
 - fini, 286, 527
 - hilbertien, 382
 - niveau, 75
 - parfait, 304
 - plongement canonique, 304, 418, 426
 - plongement logarithmique, 419
 - plongements, 304
 - quadratique, 207, 435, 504
 - ordre, 435
 - régulateur, 421
 - signature, 304, 415
 - unités, 417
 - système fondamental, 418
- correspondance de Langlands, 461
- courbe
 - elliptique, 470, 479
- critère
 - d'Eisenstein, 37
 - d'Euler, 43, 368
 - de Dumas, 37
 - de Lucas-Lehmer, 210
 - de Pépin, 209
- cryptanalyse, 507
- cryptographie, 507
- développement décimal illimité, 28
- dense, 85
- densité, 5, 16
- Dirichlet
 - caractère de, 247
 - séries, 244
 - théorème de, 248
- discriminant, 412
- disque de Jensen, 356
- division euclidienne, 5
- écriture
 - hyperbinaire, 119
- ensemble
 - bien ordonné, 126, 145
 - dénombrable, 133
 - diophantien, 185
 - équipotents, 130
 - initial, 127
 - récuratif, 184
 - récurivement énumérable, 184
- entier
 - algébrique, 414
 - décadique, 161
- entiers
 - de Gauss, 61
- équation
 - d'Hurwitz, 68, 476
 - de Catalan, 487
 - de Fermat, 486, 488
 - de Pell-Fermat, 186, 472, 505
 - de Thue, 480
 - diophantienne, 56, 433, 465, 504

- Euclide
 - algorithme, 9
 - lemme, 7
 - théorème, 5
- Euler
 - fonction, 12
 - indicatrice, 12, 13, 123, 248
- Fermat
 - algorithme, 220
 - descente, 173, 197
 - petit théorème, 13
- fermeture intégrale, 414
- fonction
 - arithmétique, 244
 - de hachage, 539
 - de Möbius, 16
 - zêta, 396, 499
- forme
 - de Pfister, 73
 - hyperbolique, 74
 - isotrope, 73
 - multiplicative, 74
 - universelle, 73
- forme bilinéaire symétrique, 73
- forme quadratique, 73, 226, 437, 438
 - ambiguë, 228
 - arithmétiquement équivalentes, 199
 - classes d'équivalence, 440
 - composition, 205, 440, 442
 - de même genre, 203
 - géométriquement équivalentes, 199
 - opposée, 440
 - primitive, 199
 - principale, 201
 - réduction, 446
 - réduite, 201, 445
- formule
 - de Legendre, 172
- fraction
 - continuée, 87, 113
 - égyptienne, 24
 - médiane, 108
- fractions continuées, 87, 113
- Frobenius
 - morphisme, 395
- Gauss
 - lemme, 8, 34
 - somme de, 58
 - sommes de, 491
- groupe
 - abélien, 392
 - de décomposition, 337
 - de Galois, 306
 - des classes d'idéaux, 424, 428, 440, 456
 - formel, 460
 - produit
 - semi-direct, 328
 - symétrique, 332
- Hasse
 - principe de, 480
- hauteur, 284
- hypothèse du continu, 133
- idéal
 - discriminant, 412
 - distance, 228
 - fractionnaire, 423, 436
 - norme, 425, 436, 442
 - premier, 428
- idéaux
 - fractionnaires
 - classes, 205
- indice de coïncidence, 513
- irrationalité
 - exposant, 277
 - mesure, 275
- jeu
 - arbre de, 137
 - de Nim, 135
 - du solitaire, 398
- Kronecker
 - substitution de, 299
- Langlands, 256, 461
- lemme
 - de Dedekind, 371
 - de Gauss, 44
 - de Hensel, 296, 377
 - de Krasner, 178
 - de Nakayama, 429

- LFSR, 522
- loi de réciprocité, 450
 - abélienne, 455
 - cubique, 450
 - d'Eisenstein, 455
 - de Duke-Hopkins, 53
 - quadratique, 45, 369
 - quartique, 454
- matrice
 - compagnon, 348
- Minkowski
 - constante, 427, 433, 462
- Möbius
 - formule d'inversion, 246, 397
- module
 - de Carlitz, 365
 - de Drinfeld, 460
- Mordell, 28
- mot de passe, 543
- nombre
 - algébrique, 266
 - polynôme minimal, 266
 - alterné, 172
 - d'or, 278
 - de Fermat, 174, 208
 - de Liouville, 279
 - de Markoff, 108
 - de Mersenne, 210
 - de Pythagore, 67
 - de type A,S,T,U, 285
 - décadique, 160, 162
 - décimal, 28
 - équivalents, 100, 101
 - friable, 220
 - hautement composé, 171
 - irrationnel, 76, 104, 275
 - p -adique, 164
 - plouton, 171
 - pratique, 20
 - premier, 4, 23
 - de Fermat, 259
 - de Pillai, 191
 - de Pyateckii-Sapiro, 190
 - de Sophie-Germain, 191
 - de Wilson, 191
 - de Woodall, 191
 - factoriel, 190
 - inévitables, 195
 - jumeaux, 191, 192
 - long, 31
 - primoriel, 190
 - régulier, 191
 - pseudo-premier, 212
 - réel, 80
 - surréel, 146
 - court, 151
 - transcendant, 266, 278
- norme
 - matricielle, 348
 - subordonnée, 349
- octonion, 68
- ordinal, 127
 - limite, 129
- ordre, 435
- paradoxe
 - de Russel, 126
- pgcd, 8, 11
- plan
 - de Fano, 68
- polygone
 - de Newton, 35, 38
- polynôme
 - contenu, 34
 - cyclotomique, 321
 - d'Eisenstein, 364
 - de Carlitz, 362
 - de rétroaction, 524
 - discriminant, 308
 - groupe de Galois, 308
 - primitif, 34
 - séparable, 301
- Pomerance, 225
- postulat
 - de Bertrand, 171, 193
- ppcm, 8
- produit cartésien, 134
- protocole
 - Diffie Hellman, 547
 - Fiat-Shamir, 549
 - pile ou face, 549

- quaternions, 64
- rayon spectral, 348
- registre à décalage, 522
- règle de Descartes, 345
- relation
 - d'équivalence, 101
 - d'ordre, 83, 142
 - de Bezout, 17
- réseau, 63, 418
- résolvante, 341
- résultant, 55, 267
- Riemann
 - fonction zêta, 235
 - hypothèse de, 241
- semi-groupe, 18
- Sierpinski, 28
- somme
 - de Gauss, 491
 - de Jacobi, 494
- subpotent, 131
- suite
 - de Brocot, 108
 - de Bruijn, 397
 - de Cauchy, 80
 - de Farey, 123, 177
 - de Fibonacci, 10, 106, 118, 177, 278
 - de Perrin, 189
 - de Sturm, 345
 - diatomique de Stern, 116
- symbole
 - d'Artin, 339, 456
 - de Hilbert, 506
 - de Jacobi, 45, 176
 - de Kronecker, 46
 - de Legendre, 43, 368, 451, 454
 - de Zolotarev, 50
- test
 - Rabin-Miller, 213
 - Solovay-Strassen, 212
- théorème
 - chinois, 12
 - d'Artin, 307
 - d'Artin-Schreier, 375
 - d'Eisenstein, 452
 - d'Euclidel, 5
 - d'Hurwitz, 104
 - d'Osada, 354
 - d'Ostrowski, 169, 350
 - de Baker, 283
 - de Bertrand, 193
 - de Bleicher-Erdős, 27
 - de Blichfeldt, 410
 - de Borel, 96
 - de Brauer, 354
 - de Cantor, 132
 - de Cantor-Bernstein, 131
 - de Cauchy, 350
 - de Cebotarev, 340
 - de Chevalley-Waring, 397
 - de Dedekind, 338
 - de Dirichlet, 98, 248, 418, 428
 - faible, 325, 395
 - de Erdős-Ginzburg-Ziv, 175
 - de Feit-Thompson, 392
 - de Fourier-Budan, 344
 - de Galois, 309
 - de Gauss, 199, 455
 - de Gauss-Lucas, 357
 - de Gel'fond-Schneider, 283
 - de Green et Tao, 253
 - de Greenfield, 195
 - de Hermite-Lindemann, 283
 - de Hilbert, 389
 - de Hilbert90, 371
 - de Hurwitz, 68
 - de Jensen, 356
 - de Jones, 185
 - de Kronecker, 323
 - de Kronecker-Weber, 326, 392
 - de Kummer, 314
 - de l'élément primitif, 303
 - de la base adaptée, 14
 - de la base télescopique, 264
 - de Lagrange, 14, 94, 98, 469
 - de Laguerre, 358
 - de Landau, 202
 - de Lebesgue, 484
 - de Legendre, 97
 - de Lindemann-Weierstrass, 283

- de Lüroth, 360, 361
- de Markoff, 101, 107
- de Mason, 488
- de Matijasevic, 185
- de Mertens, 181
- de Mills, 187
- de Minac et Willans, 189
- de Minkowski, 409
- de Mordell-Weil, 479
- de Perron, 353
- de Pfister, 71, 75
- de Polya, 355
- de Puiseux, 380, 381
- de Pyateckii-Sapiro, 190
- de Robinson, 21
- de Roth, 277
- de Rouché, 351
- de Rowland, 189
- de Ruiz, 189
- de Schanuel, 284
- de Shafarevitch, 392
- de Siegel, 277
- de Sophie Germain, 505
- de Steinitz, 273
- de Sturm, 346
- de Sylvester, 18, 347
- de Szemerédi, 253
- de Tchébychev, 233
- de Thue, 277, 480
- de Vahlen, 96
- de van der Waerden, 253, 390
- de Walsh, 358
- de Wedderburn, 286
- de Wilson, 186, 187, 191
- de Yéléhada, 188
- de Zermelo, 130
- de Zorn, 130
- des deux carrés, 62
- des nombres premiers, 233, 241
- des quatre carrés, 67
- fondamental de l'algèbre, 311
- théorie
 - de Galois des corps finis, 395
 - de Lubin-Tate, 460
 - du corps de classe, 457
- totalement décomposé, 207
- Ulam
 - spirale, 171, 183
- valuation
 - π -adique, 170
 - p -adique, 7, 164
 - penchée, 35
- Waring
 - problème de, 469, 490