

List of Names

- Abel, N.H., 47, 114
Abhyankar, S.S., 120
Ahlsvede, R., 226
Artin, E., 26, 66, 68, 113, 138, 192
Ashikhmin, A., 395
Atkin, A.O.L., 6, 37, 47
- Barg, A.M., 396
Barnes, E.S., 273
Bassalygo, L.A., 227, 399
Basse, H., 47
Belfiore, J-C., 249, 277
Berlekamp, E.R., 210, 226, 227
Betti, E., 290
Blichfeldt, H.F., 276
Blinovsky, V.M., 227
Boguslavsky, M.I., 284, 285, 333
Bos, A., 276
Boston, N., 187, 193
Brauer, R., 141, 163, 192
- Calderbank, R., 364
Carlitz, L., 48
Cassels, J.W.S., 85
Cauchy, A-L., 62
Chabauty, C., 246
Chebotarev, N.G., 73
Chebyshev, P.L., 168
Chudnovsky, D.V., 335, 338, 395
Chudnovsky, G.V., 335, 338, 395
Conway, J.H., 276
Couvreur, A., 289, 294, 295, 333
- Dedekind, R., 11, 47, 73
Deligne, P., 47, 94, 138
Deuring, M., 47, 354
Dirichlet, P.G.L., 57, 73, 176
Drinfeld, V.G., 21, 24, 48, 138, 410
- Duursma, I.M., 226
- Ehrhard, D., 226
Elias, P., 226, 227, 399
Elkies, N.D., 1, 37, 48, 124, 139, 270, 277
Euler, L., 290
- Fejes Tóth, L., 276
Feng, G.L., 138, 226
Feynman, R.P., 395
Fischer, B., 235
Fontaine, J-M., 186, 192
Fröhlich, A., 85
Fueter, R., 47
Furtwängler, P., 85
- Gallager, R.G., 226
Galois, E., 47
García, A., 37, 43, 116, 138
Gauss, K.F., 276
Ghorpade, S.R., 289, 295, 333
Gilbert, E.N., 198, 395, 399
Golod, E.S., 80, 82, 85, 141, 192
Goppa, V.D., 277, 396
Grassmann, H.G., 319
Griesmer, J.H., 399
Griess, R.L., Jr., 235
Grothendieck, A., 290
Guinand, A.P., 151
Guruswami, V., 195, 200, 206, 227
- Hajir, F., 183, 192
Hales, T., 276
Hamming, R.V., 226, 397
Harriot, T., 276
Hasse, H., 85
Havemose, A., 226
Hayes, R., 48, 76, 77, 82, 85

- Hecke, E., 47
 Heilbronn, H., 167
 Hermite, C., 47, 56
 Hilbert, D., 60, 79, 276
 Hlawka, E., 378, 395
 Hodge, W.V.D., 333
 Høholdt, T., 226
 Howe, E.W., 138
 Hurwitz, A., 52, 94

 Ihara, Y., 182, 187, 192, 193

 Jacobi, C.G.J., 47
 Jacobi, C.G.J., 114
 Jensen, H.E., 226
 Jensen, J., 197
 Johansson, T., 395
 Johnson, S.M., 196, 227
 Justesen, J., 226

 Kabatiansky, G.A., 236, 276, 395
 Kasami, T., 395
 Katz, N., 47
 Kepler, J., 231, 276
 Klein, F., 47, 138
 Kleptsyn, V.A., 193
 Kodaira, K., 266
 Koksmá, J.F., 378
 Korkine, A.M., 276
 Krachkovsky, V.Yu., 226
 Kronecker, L., 47, 68
 Kummer, E.E., 111, 138

 Lachaud, G., 246, 289, 295, 333
 Lagarias, J.C., 168, 192
 Lang, S., 47, 74
 Langlands, R.P., 47
 Larsen, K.J., 226
 Lauter, K.E., 138
 Leech, J., 231, 234, 273, 276
 Lefschetz, S., 268, 290
 Legendre, A.M., 5, 47
 Lehner, J., 6, 37
 Lenstra, H.W., Jr., 277
 Levenshtein, V.I., 236, 276
 Lin, S., 395
 Litsyn, S.N., 276, 395
 Lusztig, G., 94, 138

 MacWilliams, F.J., 395
 Madelung, Y., 226
 Maire, C., 183, 192
 Manin, Yu.I., 395
 Martinet, J., 154, 177, 179, 182, 192
 Massey, J.L., 226
 Mazur, B., 47, 186, 192
 McEliece, R.J., 401
 Milne, J.S., 85
 Minkowski, H., 142, 192, 236
 Mordell, L.J., 265, 266
 Muller, D.E., 286, 333

 Néron, A., 265, 266
 Neukirch, J., 85
 Newton, I., 276
 Niederreiter, H., 369, 378, 396
 Noether, E., 292
 Nogin, D.Yu., 333

 Odlyzko, A.M., 145, 168, 192
 Oesterlé, J., 88, 89, 94, 138
 Ogg, R., 47

 Pauli, W.E., 357
 Pellikaan, R., 138
 Picard, R., 302
 Pinsker, M.S., 227
 Plücker, J., 319
 Plotkin, M., 399
 Poincaré, H., 290

 Quebbemann, H-G., 273, 277

 Radhakrishnan, J., 227
 Raleigh, W., 276
 Randriambololona, H., 395
 Rao, T.R.N., 226
 Rapoport, M., 47
 Ree, R., 94, 101
 Reed, I.S., 200, 286, 333
 Riemann, G.F.B., 47, 144, 405
 Ritzentaler, C., 138
 Robinson, R.M., 193
 Roch, G., 405
 Rodemich, E.R., 401
 Rodier, F., 334
 Rogers, C.A., 237, 276
 Roquette, P., 85

- Rosenbloom, M.Yu., 277, 369, 396
Rosenlicht, M., 74
Rumsey, H.C., Jr., 401
Rush, J.A., 276
- Sakata, S., 226
Schmidt, W.M., 238
Schreier, O., 113, 138
Schubert, H., 323
Segre, C., 328
Serre, J-P., 193
Serre, J-P., 85, 145, 192, 280, 333, 409, 410
Severi, F., 266
Shafarevich, I.R., 80, 82, 85, 141, 192, 354
Shamir, A., 350, 395
Shannon, C.E., 226, 246
Shen, B., 226
Shimura, G., 47
Shioda, T., 266, 277
Shor, P.W., 364, 395
Sidelnikov, V.M., 276
Siegel, C.L., 141, 163, 167, 192
Simmons, G.J., 395
Singleton, R.C., 198, 217, 399
Skorobogatov, A.N., 226
Skriganov, M.M., 396
Sloane, N.J.A., 276, 395
Smeets, B., 395
Sobol, I.M., 395
Solé, P., 249, 277
Solomon, G., 200
Sørensen, A.B., 280, 333
Stark, H.M., 145, 167
Steane, A., 364
Stern, J., 246
- Stichtenoth, H., 37, 43, 116, 138
Sudan, M., 195, 200, 206, 227
Suzuki, M., 94, 96
- Tamo, I., 396
Tate, J.T., Jr., 265, 271, 277
Thue, A., 276
Tsfasman, M.A., 193, 276, 277, 280, 284, 285, 333, 369, 395, 396, 414
Tzeng, K.K., 226
- van der Geer, G., 138
Varshamov, R.R., 198, 399
Veronese, G., 329
Viazovska, M.S., 276
Vlăduț, S.G., 48, 226, 410, 414
- Wall, G.E., 273
Weber, H., 47, 68
Wei, V.K., 226
Weierstrass, K., 8, 12
Weil, A., 13, 85, 151, 160, 189, 265, 266, 409
Welch, L.R., 401
Weyl, H., 395
Wozencraft, J.M., 226
Wyner, A.D., 246
- Xing, C., 227, 395
- Yaglom, I.M., 249, 277
- Zak, F.L., 333
Zanella, C., 333
Zariski, O., 402
Zimmert, R., 170, 192
Zink, T., 414
Zolotareff, E.I., 276
Zyablov, V.V., 227

Index

- $A(q)$, 81, 87, 410, 414
 $A^-(q)$, 135
 A_N lattice, 233
 $\alpha_{\mathbb{R}}, \alpha_{\mathbb{C}}, \alpha'_{\mathbb{R}}, \alpha'_{\mathbb{C}}, \alpha''_{\mathbb{R}}, \alpha''_{\mathbb{C}}$, 145, 154
 $\text{BS}(\mathcal{K})$, *see* Brauer–Siegel ratio
“char” \mathbb{K} , *see* “characteristic”
 $\text{Cl}_{\mathbb{k}}$, *see* class group
 $\text{Cusps}(I)$, 26
 $\text{Cusps}_0(I), \text{Cusps}_1(I)$, 27
 $d(Q|P)$, *see* different exponent
 $D(V)$, *see* minimum A-distance
 (d, k, m, s) -system over \mathbb{F}_q , 380, 396
 (d, m, s) -system over \mathbb{F}_q , 380
 $\delta_{\mathcal{K}}$, *see* deficiency
 $D_{\mathbb{k}}$, *see* discriminant of an algebraic number field
 D_N lattice, 233
 d_{X_i} , *see* dimension sequence
 $D_{\mathbb{K}/\mathbb{k}}$, *see* relative discriminant
 $\mathfrak{D}_{\mathbb{K}/\mathbb{k}}$, *see* different of an extension
 $\text{deg}_{(1,k)}$, *see* weighted degree
 $\text{Diff}(\mathbb{L}/\mathbb{K})$, *see* different
 $\text{Div}(\overline{X})$, 301
 $e(Q|P)$, *see* ramification index
 E_N lattice, 233
 $F_I(x, y)$, *see* modular equation for Drinfeld curves
 $\varphi_{\alpha}, \varphi_{\mathbb{R}}, \varphi_{\mathbb{C}}$, 143, 147
 $F_K(s)$, 166
 $\Phi_N(x, j)$, *see* modular equation
 γ (Euler constant), 144
 $\gamma(\mathcal{F})$, *see* genus of a recursive tower
 $\mathcal{G}(q, N)$, 133
 Γ_N lattice, 233
 Γ (congruence subgroup), 4
 $\Gamma(1)$ (modular group), 2
 $\Gamma(N), \Gamma_0(N)$ (subgroups of the modular group), 3
 $\Gamma_0(I), \Gamma_1(I), H(I)$ (subgroups of $\text{GL}_2(A)$), 27
 $\eta(z)$, *see* Dedekind eta function
 h_i , 143
 $h_{\mathbb{k}}$, *see* class number
 $H_{q,m}(\delta)$ (q -ary m -entropy), 375
 $\text{ht}(f)$, *see* height function
 $\text{ht}(\mathbb{K})$, *see* height of a field
 j function, 5, 10
 j_N function, 11
 $\varkappa(\mathcal{K})$, 163
 $\mathbb{K}\{\tau\}$ (ring of noncommutative polynomials), 22
 K^{ab} , 66
 \mathbb{K}_N (quadratic subfield in $\mathbb{Q}(\zeta_N)$), 13
 \mathbb{k}_P , *see* residue class field
 L -construction, 412
 $\ell(D)$, 405
 $\tilde{\lambda}, \tilde{\lambda}_{\ell}$ (asymptotic packing density), 236
 $\lambda(\mathcal{F})$, *see* recursive tower, limit of
 $\tilde{\lambda}^{\text{pol}}, \tilde{\lambda}_{\ell}^{\text{pol}}, \tilde{\lambda}^{\text{exp}}, \tilde{\lambda}_{\ell}^{\text{exp}}$, 237, 244, 275
 $\tilde{\lambda}_T, \tilde{\lambda}_T^{\text{exp}}, \tilde{\lambda}_T^{\text{pol}}$, 242
 \log^* , 217
 $\mu(\mathcal{A}/K)$, *see* bilinear complexity
 (\mathcal{M}, μ) -uniform point set, 379
 $\mu^{\text{sym}}(\mathcal{A}/K)$, *see* symmetric bilinear complexity
 (ms, M, d) ordered code, 370
 n -code, 350
 r -reconstructing, 351
 t -disconnected, 351
 t -uniform, 351
generator, 351
with uniformity, 351

- $\nu(\mathcal{F})$, *see* recursive tower, splitting rate of
 $N(x)$, $\text{Norm}(x)$, *see* norm
 $((n, K))$ code, $[[n, k]]$ code, *see* quantum code
 $[n, k, d]_q$ code, 397
 $[n, k, d]_q$ system, 398
 projective, 398
 (n, t, d, r) arithmetic secret sharing scheme, 351
 $N_q(g)$, 87
 $N_q(K_i)$, $N_{\mathbb{R}}(K_i)$, $N_{\mathbb{C}}(K_i)$, $N_{\alpha}(K_i)$, 143
 $\text{NS}(S)$, *see* Néron–Severi group
 $\mathcal{O}_{\mathbb{k}}$ (ring of integers), 55
 $\text{ord}_{\mathfrak{p}}(x)$, 58
 \mathfrak{p} -adic topology, 62
 P -construction, 412
 $P(t)$, *see* numerator of the zeta function
 p -extension, 79
 (p, L) -list-decodable code, 195
 (p, \widehat{L}) -list-decodable family, 195
 P_I (probability of a successful impersonation attack), 344
 P_S (probability of a successful substitution attack), 344
 $\text{Pic}(\overline{X})$, *see* Picard group
 proj_t , $\text{proj}_{[t_1, t_2]}$, 217
 q -ary entropy, 400
 q -expansion, 10
 at infinity, 10
 of the j function, 10
 Q -polynomial, 206
 q -twisted code, 346
 r -torsion point group, 352
 R_i , 143
 $R_{\mathbb{k}}$, *see* regulator of an algebraic number field
 r_{X_i} , *see* degree sequence
 rd , rd_K , *see* root discriminant
 $\tilde{\sigma}$ (modified embedding), 253
 s -linear complexity, 335
 $\text{Sing}(X)$, *see* singular locus
 T -lattice, 241
 (t, m, s) -net in base b , 379, 396
 (t, s) -sequence in base b , 380, 396
 \mathcal{T}_1 tower, 120, 138
 \mathcal{T}_2 tower, 121, 138
 $T_{\ell}(r, m)$, *see* Tsfasman–Boguslavsky bound
 $\text{Tr}(x)$, *see* trace
 $V(\mathcal{F})$, *see* ramification locus
 \mathcal{W}_1 tower, 44, 116, 122, 138, 217
 codes from, 125, 223
 \mathcal{W}_2 tower, 43, 116, 123, 130, 138, 389
 $w_m, w_{\ell}^{(n)}$, *see* Atkin–Lehner involution
 $X(N)$, $X_0(N)$, $Y(N)$, $Y_0(N)$, *see* modular curves
 $X_0(I)$, $X_1(I)$, $C(I)$ (Drinfeld modular curves), 27
 $\dot{X}_0(I)$, $\dot{X}_1(I)$, $\dot{X}(I)$ (Drinfeld modular curves), 42
 $X_0(\ell^n)$, $Y_0(\ell^n)$ (modular curves), 37
 $\xi_{\mathcal{K}}(s)$, $\xi_{\varphi}(s)$, 144
 $\dot{Y}_0(I)$, $\dot{Y}_1(I)$, $\dot{Y}(I)$ (affine Drinfeld modular curves), 43
 $Z(\mathcal{F})$, *see* splitting locus
 $\zeta_{\mathcal{K}}(s)$, $\zeta_{\varphi}(s)$, *see* limit zeta function
 $\tilde{\zeta}_{\mathcal{K}}(s)$, $\tilde{\zeta}_{\varphi}(s)$, *see* completed zeta function

A-code, 343, 395
 I-equitable, 345
 systematic, 343
 without secrecy, 343
Abel–Jacobi map, 114
abelian covering, 75
Abhyankar’s lemma, 120, 138
absolute class field, *see* Hilbert class field
absolute discriminant, *see* discriminant of an algebraic number field
absolute irreducibility, 289
absolute norm of an ideal, 69
absolute value, 58
 non-Archimedean, 59
 normalized, 59
adjunction formula, 303
affine closed set, 402
affine Reed–Muller code, 287
affine subspace
 periodic, 217
 canonical representation of, 218

- ultra-periodic, 218
- algebraic design, 218
- algebraic function field, *see* function field
- algebraic geometry bound
 - for A-codes, 348
 - for NRT codes
 - asymptotic, 377
- algebraic geometry code, 412
 - NRT, 373
- algebraic integer, 55
- algebraic number field, 55
 - degree of, 55
 - totally complex, 59
 - totally real, 59
- algebraic set, 291
- algebraic variety
 - absolutely irreducible, 289
 - linear, 291
 - nondegenerate, 292
- almost normal
 - number field, 165
 - tower, 165
- alphabet, 397
 - extension, 401
 - restriction, 401
- Archimedean coefficients, *see* $\alpha_{\mathbb{R}}$, $\alpha_{\mathbb{C}}$, $\alpha'_{\mathbb{R}}$, $\alpha'_{\mathbb{C}}$, $\alpha''_{\mathbb{R}}$, $\alpha''_{\mathbb{C}}$
- Archimedean place, 58
- arithmetic genus, 303
- arithmetic secret sharing, 350
 - scheme, 351
- Artin map
 - global, 68, 71
 - local, 66
- Artin symbol, 26, 66
- asymptotic rate of d -torsion, 350
- asymptotic upper bounds, 400–401
- asymptotically bad
 - family of global fields, 143
 - infinite global field, 148
 - tower, 117
- asymptotically exact
 - family of global fields, 143
- asymptotically good
 - family of global fields, 143
 - infinite global field, 148
 - quantum code, 362
- tower, 117
- asymptotically optimal
 - tower, 117
- Atkin–Lehner involution, 6, 37
- attack
 - impersonation, 344
 - substitution, 344
- authentication code, *see* A-code
- authentication function, 343
- authenticator, *see* tag
- automorphic function, 10
- basic algebraic geometry bound, 414
- basic construction of LRC codes
 - from algebraic curves, 386
- basic decoding algorithm, 195, 226
- basic equality
 - for the function field case, 158
 - GRH, 159
- basic inequality
 - GRH, 151
 - in the function field case, 149
 - unconditional, 154
- basic inequality', 154
- basic inequality'', 154
- basic lattice construction, 242
- Bassalygo–Elias bound, 399
 - asymptotic, 401
 - for NRT codes, 372
 - asymptotic, 377
- Berlekamp's algorithm, 227
- Berlekamp–Massey algorithm, 226
- Betti numbers, 290
 - corrected, 293
- bilinear complexity, 336
 - symmetric, 336
- birational isomorphism, 403
- blow-up, 304
- Boston's conjecture, 187, 193
- Brauer–Siegel inequality
 - generalized, 164
- Brauer–Siegel ratio, 163, 177, 180, 187
 - bounds, 173
 - unconditional, 174
- Brauer–Siegel theorem
 - classical, 163
 - generalized, 163, 187

- GRH, 164
 - unconditional, 165
- Calderbank–Shor–Steane
 - construction, 364
- canonical class, 405
 - of a surface, 303
- canonical height, 265
- canonical representation of an
 - (r, Δ, b) -periodic subspace, 218
- canonical subspace, 219
- cascaded subspace design, 219
- Cauchy sequence, 62
- center density, 231
- Chabauty–Shannon–Wynner bound, 246
- character of a quadric, 314
- “characteristic”, 22
 - “finite”, 22
 - “general”, 22
- Chebotarev density theorem, 73
- Chudnovsky algorithm, 338, 395
- Chudnovsky method, 337
- class field theory, 104
- class field tower problem, 79, 85
- class group, 59
- class number, 59, 408, 409
- closed set, 402
- code, 397
 - cardinality of, 397
 - degenerate, 398
 - dimension, 397
 - distance, *see* minimum distance
 - length, 397
 - linear, 397
 - locally recoverable, *see* LRC codes
 - nondegenerate, 398
 - projection of, 401
 - q -ary, 397
 - q -twisted, 346
 - rate, 397
 - repetition of, 401
 - spherical, 245
 - transitive, 35
 - vector, 397
- codes
 - asymptotically good family of, 400
 - direct sum of, 401
 - equivalent, 398
 - from Deligne–Lusztig varieties, 331, 334
 - from flag varieties, 332, 334
 - on Drinfeld curves, 33
 - on modular curves, 16
 - tensor product of, 401
- codeword, 397
- complete field, 62
- complete intersection, 293
- complete splitting in a tower, 119
- completed zeta function, 144, 155
- completely decomposable exterior form, 320
- completion of a field with valuation, 62
- complex embedding, 56
- concatenation, 401
 - bound, 415
- conductor of an extension, 72
- conductor-discriminant formula, 192
- congruence subgroup, 4, 25
 - modulo an ideal, 72
 - principal, 3
- consecutive block, 325
- constant field, 50, 406
- Construction A, 241
- Construction D, 251
- Couvreur’s bound, 295, 300, 333
- covering, 52
- covering radius, 235
- cubic surface, 304, 305, 333
- curve, 404
 - algebraic, 404
 - complete, 404
 - modular, 5
 - Drinfeld, 24
 - number of points of, 407, 409
 - projective, 404
 - quasiprojective, 404
 - smooth complete, 404
- decomposition group, 54, 70
- Dedekind eta function, 11
- Dedekind zeta function, 73
- deep holes, 235
- deficiency, 153
- defining modulus, 72

- degree
 - of a divisor, 404
 - on a surface, 302
 - of a place, 51, 407
- degree map, 22
- degree sequence, 294
- Deligne–Lusztig curves, 94, 104
- Deligne–Lusztig varieties, 94, 138
- density
 - of a lattice packing, 230
 - of a packing, 230
- density exponent, 231
- detectable quantum error, 357, 358
- determinant of a lattice, 230
- Deuring–Shafarevich theorem, 354
- different, 53, 61
 - of an extension, 60
- different exponent, 53, 119
- digital (t, m, s) -net over \mathbb{F}_q , 380
- digital (t, s) -sequence over \mathbb{F}_q , 381
- digital method, 380, 396
- dimension
 - of a code, 397
 - of a variety, 403
- dimension sequence, 294
- dimension vector, 219
- direct sum of codes, 401
- Dirichlet L -function, 73
- Dirichlet character, 73
- Dirichlet density, 73
- Dirichlet’s unit theorem, 57
- discrepancy (factor), 378, 396
- discrete valuation, 51, 406
- discriminant
 - of a lattice, 230
 - of an algebraic number field, 56, 61, 253
 - relative, 60
- discriminant function, 12
- divisor, 404
 - degree of, 404
 - effective, 405
 - group, 404
 - of a function, 405
 - on a surface, 301
 - positive, 405
 - principal, 405
 - space associated to, 405
 - support of, 404
- domain of spherical codes, 246
 - polynomially constructible, 247
- Drinfeld–Vlăduț bound, 87, 88, 129, 141, 410
- Drinfeld curves, *see* Drinfeld modular curves
- Drinfeld modular curves, 21, 24
- Drinfeld module, 25
 - ε -normalized, 77
 - normalized, 43, 76
- Drinfeld–Vlăduț bound, 149
- Drinfeld–Vlăduț inequality, *see* Drinfeld–Vlăduț bound
- Drinfeld–Vlăduț theorem, *see* Drinfeld–Vlăduț bound
- dual basis, 56
- dual lattice, 231
- EC code, 343
 - related to an A-code, 345
- elementary tensor, 335
- Elkies conjecture, 124, 139
- Elkies lattices, 270
- Elkies towers, 37
- elliptic A -module, 22
 - rank of, 22
- elliptic modules, 22
 - homomorphism of, 22
 - isogenous, 23
 - isomorphism of, 23
- elliptic quadric, 314
- elliptic surface, 266, 267
- enumerators of a quantum code, 358
- equivalent
 - $[n, k, d]_q$ systems, 398
 - absolute values, 58
 - codes, 398
 - divisors, 405
 - fractional ideals, 59
 - projective systems, 398
 - valuations, 62
- error operator, *see* quantum error
- eta function, 11
- Euler characteristic, 290
- evaluation map, 412
- even lattice, 234
- exceptional curve (line), 304

- exceptional divisor, 307
- exceptional fibre, 266
- exceptional zero, 167
- existence theorem (for abelian extensions), 72
- explicit formula, 410
 - GRH, 159
 - in the function field case, 158
 - Weil, 160
- extension
 - Galois, 65
 - just-infinite, 186
 - tamely ramified, 64
 - totally ramified, 63
 - unramified, 52, 60, 63
 - wildly ramified, 64
- family
 - of global fields, 142
 - asymptotically bad, 143
 - asymptotically exact, 143
 - asymptotically good, 143
 - of packings, 236
 - (asymptotically) good, 236
 - exponential, 237
 - polynomial, 237
 - τ -asymptotically good, 250
- Fermat surface, 268
- fiber products
 - of Artin–Schreier curves, 113
 - of Kummer curves, 111
- field descent, 401
- finite place, 59
- finite prime, 68
- first-order Reed–Muller NRT code, 373
- Fischer–Griess Monster, 235
- flag, 328
- flag variety, 328
- FMCD (multiplicative function field congruence code construction), 263
- FML (multiplicative function field lattice construction), 258
- FMLD (multiplicative function field congruence sublattice construction), 260
- Fontaine–Mazur conjecture, 192
- form, 402
- fractional ideal, 59, 61
- Frobenius element, 66, 70
- function
 - (element of a function field), 51
 - divisor of, 405
 - pole of, 53
 - rational, 403
 - regular, 51, 403
 - zero of, 53
- function field, 50, 51, 406
 - field of constants of, 50, 406
 - infinite, 141
 - valuation ring of, 50, 406
- functional equation, 408
- fundamental basis of an algebraic number field, 56
- Galois group for an infinite extension, 65
- García–Stichtenoth towers, 37, 116, 120, 122–124, 389
- Gaussian binomial coefficient, 319
- generalized Brauer–Siegel inequality, 164
- generalized Brauer–Siegel theorem, 163, 187
 - GRH, 164
 - unconditional, 165
- generalized Jacobian, 75
- generalized Riemann hypothesis, 144
- generalized weight, 399
- generating matrices (for the digital method), 380, 381
- generator matrix, 397
 - of a lattice, 230
- generator of an n -code, 351
- genus
 - arithmetic, 303
 - geometric, 303
 - of a curve, 61, 405
 - of a number field, 142
 - of a recursive tower, 117
- geometric genus, 303
- Ghorpade–Lachaud conjecture, 295, 333
- Gilbert–Varshamov bound, 235, 236, 399, 415

- asymptotic, 401
- for q -ary quantum codes, 368
- for A-codes, 347
- for LRC codes
 - asymptotic, 392
- for NRT codes, 372
 - asymptotic, 377
- for stabilizer codes, 360
- global Artin map, 68, 71
- global class field theory, 68
- global field, 49
 - infinite, 141, 142
- Golod–Shafarevich theory, 80, 141
- good reduction modulo \mathfrak{p} , 13
- Grassmann code, 319, 330, 333
- Grassmann variety, 319
- Grassmannian, *see* Grassmann variety
- GRH, *see* generalized Riemann hypothesis
- GRH basic equality, 159
- GRH basic inequality, 151
- GRH explicit formula, 159
- GRH generalized Brauer–Siegel theorem, 164
- Griesmer bound, 399
 - asymptotic, 400
- group of units, 50, 406
- Guinand–Weil explicit formula, 151
- Guruswami–Sudan algorithm, 200, 201, 227
 - for algebraic geometry codes, 206
 - for Hermitian codes, 211
 - for Reed–Solomon codes, 202
- Hajir–Maire towers, 183, 192
- Hamming bound
 - asymptotic, 400
 - for NRT codes, 372
 - asymptotic, 376
 - for quantum codes, 359
- Hamming metric, 397
- Hamming weight, 397
- Hayes module, 77
- Hayes theory, 76, 77, 85
- height function, 257
- height of a field, 257
- Hermitian code, 211, 312, 330, 333, 413–414
- Hermitian curve, 94, 114, 211, 215, 388, 412
 - function field of, 104
- Hermitian variety, 311
- hexagonal lattice, 231
- Hilbert p -class field tower, 79
- Hilbert class field, 60, 79
 - (S, ℓ) -, 80
- Hilbert class field tower, 79
 - (S, ℓ) -, 81
- Hilbert different formula, 54
- Hodge postulation formula, 333
- honest-but-curious adversary, 352
- Hurwitz bound, 94
- Hurwitz formula, 52, 61
 - for function fields, 53
- Hurwitz inequality, *see* Hurwitz bound
- hyperbolic quadric, 314
- I-equitable A-code, 345
- ideal class group, *see* class group
- Ihara’s conjecture, 187, 193
- image of a rational map, 403
- impersonation attack, 344
- increasing-zero basis, 204
- index
 - of a quadric, 314
 - of a regular birational map, 304
 - of an ordered orthogonal array, 382
- inertia, 52
- inertia group, 54, 64
- infinite function field, 141
- infinite Galois extension, 65
- infinite global field, 141, 142
 - asymptotically bad, 148
 - asymptotically good, 148
- infinite place, 58
- infinite prime, 68
- integral element of an algebraic number field, 55
- interpolation system, 337
 - symmetric, 337
- intersection index, 302
- inverse limit, *see* projective limit

- irreducible component, 403
- irredundant decomposition, 294
- isogeny of elliptic modules, 23
- iterated logarithm, 217
- Johnson bound, 196, 197, 227
- Johnson radius, 197
- just-infinite extension, 186
- Kabatiansky–Levenshtein bound, 236, 246, 276
- Kepler conjecture, 231, 276
- kissing number, 230, 246
 - asymptotic polynomially constructible, 248
- Kodaira–Néron model, 266
- Koksma–Hlawka inequality, 378
- Kronecker–Weber theorem, 68
- Lachaud’s bounds, 294, 333
- Lachaud–Stern bounds, 246
- Lagarias–Odlyzko’s estimate, 168, 192
- Lang–Rosenlicht theory, 74
- large symplectic code, 359
- lattice (lattice packing), 230, 235
 - construction complexity, 244
 - dual, 231
 - even, 234
 - unimodular, 231
- lattice (over a finite extension of \mathbb{k}_∞), 24
 - morphism of, 24
 - rank of, 24
- lattice construction
 - basic, 242
 - simplest, 241
- Leech lattice, 231, 234, 273, 276
- Lefschetz number, 268
- Lefschetz–Grothendieck trace formula, 290
- Legendre modulus, 5, 47
- length vector, 219
- level structure, 25
- limit zeta function, 143, 155
- linear equivalence, 405
 - on a surface, 302
- linear programming bound for quantum codes, 359
- linear variety, 291
- list decodable code (family), 195
- list decoding, 195, 226
- local Artin maps (local reciprocity maps), 66
- local class field theory, 66
- local code, 384
- local existence theorem, 66
- local field, 63
 - Archimedean, 63
 - non-Archimedean, 63
- local parameter, 50, 404, 406
- local reciprocity law, 66
- local recovery, 385
- local ring, 50, 406
 - of a point, 403
- local uniformizing parameter, 66
- locality (of an LRC code), 384
- locally recoverable code, *see* LRC code
- log-cardinality, 397
- low-discrepancy
 - point set, 378
 - sequence, 378
- LRC codes, 384, 396
 - from algebraic curves
 - basic construction, 386
 - from Hermitian curves, 388
 - optimal, 384
- MacWilliams duality for the NRT metric, 396
- MacWilliams identities for quantum codes, 358
- map
 - dominant, 403
 - rational, 403
 - image of, 403
 - regular, 403
- maximal abelian extension, 78
- maximal ideal, 403
- maximal order, 55
- McEliece–Rodemich–Rumsey–Welch (MRRW) bound, 236, 401
- minimal model, 304
- minimum A-distance, 345
- minimum distance, 397
 - of a lattice, 230

- of a quantum code, 358
 - q -ary, 367
- of a small symplectic code, 359
- of a sphere packing, 229
- of a spherical code, 245
- relative, 397
- minimum distance decoder, 195
- Minkowski bound, 142, 235, 236
- Minkowski constant, 142, 192
- modular curves, 5, 47
 - Drinfeld, 24
 - over \mathbb{F}_q , 26
 - over finite fields, 12
- modular equation, 11, 47
 - for Drinfeld curves, 28
- modular form, 12
 - parabolic, 12
- modular functions, 47
- modular group, 2
- modulus, 69, 74
 - defining, 72
- monoidal transformation, *see*
 - blow-up
- Mordell–Weil group, 268
- Mordell–Weil lattice, 266, 277
 - narrow, 266
- Mordell–Weil theorem, 265
- morphism
 - of varieties, 403
- multiplication algorithm, 336
 - symmetric, 336
- multiplicative valuation, 58

- NAC (additive number field code
 - construction), 255
- NAL (additive number field lattice
 - construction), 253
- narrow Mordell–Weil lattice, 266
- Néron–Severi group, 266, 303
- Néron–Tate form, 265
- Néron–Tate theorem, 265
- net (point set), 378, 396
- Newton number, *see* kissing number
- Niederreiter–Rosenbloom–Tsfasman
 - metric, *see* NRT metric
- NML (multiplicative number field
 - lattice construction), 257
- NMLD (multiplicative number field
 - congruence sublattice
 - construction), 261
- Noether’s normalization theorem,
 - 292
- non-Archimedean place, 59
- nonbinary quantum code, 367, 395
- norm, 56
 - absolute, 69
 - relative, 59
- norm residue map, 66
- normalized valuation, 66
- normalizing field, 78
- NRT
 - code, 370
 - algebraic geometry, 373
 - first-order Reed–Muller, 373
 - Reed–Solomon, 372
 - metric, 369, 396
 - weight, 369
- number field, *see* algebraic number
 - field
 - infinite, 141
- number of effective divisors, 407
- number of points, 407, 409
 - of degree r , 407
- numerator of the zeta function, 408,
 - 409

- Odlyzko–Serre bounds, 145, 149
- Oesterlé bound, 88, 89, 138
- OOA, *see* ordered orthogonal array
- open set, 402
- opponent (in an authentication
 - system), 343
- optimal LRC codes, 384
- order of an algebraic number field, 55
- ordered code, 370
 - linear, 370
- ordered Hamming space, *see* NRT
 - space
- ordered Hamming weight, *see* NRT
 - weight
- ordered orthogonal array, 382, 396

- packing, 235
 - random, 239
- packing family, *see* family of
 - packings

- parabolic quadric, 314
- parabolic subgroup, 328
- parity-check matrix, 398
- Pauli matrices, 357
- perfectization, 76
- Picard group, 302
- Plücker embedding, 319
- place, 50, 406
 - degree of, 51, 407
 - inert, 52
 - of an algebraic number field, 58
 - Archimedean, 58
 - complex, 58
 - finite, 59
 - infinite, 58
 - non-Archimedean, 59
 - real, 58
 - ramified, 52
 - totally ramified, 52
 - unramified, 52
 - valuation ring of, 50, 406
 - value at, 51
- Plotkin bound, 399
 - asymptotic, 400
 - for NRT codes, 370
 - asymptotic, 375
- Poincaré duality, 290
- point, 50
 - local ring of, 403
 - nonsingular, 404
 - regular, 403
 - singular, 403
 - smooth, 403
- point random field, 239
- point set
 - (\mathcal{M}, μ) -uniform, 379
 - low-discrepancy, 378
 - uniform, 379, 395, 396
- Poisson random field, 239
- pole of a function, 53
- pole order, 53
- polynomial $P(t)$, *see* numerator of the zeta function
- polynomially constructible family of spherical codes, 246
- position, 397
- prime, 59, 66, 68
 - finite, 68
 - infinite, 68
 - complex, 68
 - real, 68
- principal congruence subgroup, 3
- principal ideal, 404
- principal ideal theorem, 72
- profinite group, 65
- projection of a code, 401
- projective $[n, k, d]_q$ system, 398
- projective closed set, 402
- projective closure, 402
- projective limit, 62
- projective Reed–Muller code, 286, 329, 333
- projective structure, 14
- projective system, 398
- proper intersection, 291
- pull-back, 75
- pure q -ary quantum code, 367
- quadric, 313
 - elliptic, 314
 - hyperbolic, 314
 - parabolic, 314
- quality parameter
 - of a (t, m, s) -net, 379
 - of a (t, s) -sequence, 380
- quantum code, 357
 - asymptotically good, 362, 395
 - enumerators, 358
 - minimum distance, 358
 - q -ary, 367
 - minimum distance, 367
 - pure, 367
 - weight of, 367
- quantum error
 - detectable, 357, 358
 - q -ary, 367
 - weight of, 357
- quantum stabilizer code, *see* stabilizer code
- quasiprojective set, 402
 - irreducible, 402
 - reducible, 402
- quaternary MacWilliams identities, 358
- ramification, 52
 - in a tower, 118

- ramification divisor, 8, 53, 61
- ramification groups, 54, 64
 - higher, 64
- ramification index, 52, 63, 119
- ramification locus, 118
- random packing, 239
- rank
 - of a tensor, 335
 - of an elliptic curve over a global field, 265
- rate
 - of a code, 397
 - of a systematic I-equitable A-code, 346
 - asymptotic, 346
- rational surface, 304
- ray class field, 72
- ray class group, 69
- real embedding, 56
- real Weil system, 189
- reciprocity law, 72
- reciprocity map, *see* global Artin map
- recursive tower, 116
 - asymptotically bad, 117
 - asymptotically good, 117
 - asymptotically optimal, 117
 - basic function field of, 117
 - genus of, 117
 - limit of, 117
 - splitting rate of, 117
- Ree curves, 101
 - function field of, 104, 106
 - zeta function of, 103
- Ree group, 102
- Reed–Muller code
 - affine, 287
 - projective, 286, 329, 333
- Reed–Solomon code, 412
 - decoding, 200
- Reed–Solomon NRT code, 372
- regulator of an algebraic number field, 58
- relative discriminant, 60
- repetition of a code, 401
- residue class field, 51
- residue field, 63
- Riemann hypothesis, 409
- Riemann–Roch theorem, 405
- ring of integers of an algebraic number field, 55
- Rogers bound, 237
- root discriminant, 144
- root-finding, 208–210
- Schubert code, 324
- Schubert variety, 324
- secret, 351
- secret sharing, 350, 395
- secret-component, 350
- Segre embedding, 328
- semiconstructive lower bound for A-codes, 347
- Serre bound, 409, 410
- Shamir’s scheme, 395
- shape (of an element of an ordered Hamming space), 369
- shares, 351
- shares-component, 350
- Siegel zero, 167
- sign function, 76
- simplest lattice construction, *see* Construction A
- Singleton bound, 399
 - asymptotic, 400
 - for list decoding, 198, 217
 - for LRC codes, 384
 - for NRT codes, 370
 - for quantum codes, 358
- singular locus, 292
- small symplectic code, 359
- Solé–Belfiore bounds, 249, 277
- solvable group, 64
- source state, 343
- space associated to a divisor, 405
- special linear group $SL_2(\mathbb{Z})$, 2
- sphere packing, 229, 276
- spherical code, 245
 - minimal angle, 245
 - minimum distance, 245
 - parameters, 246
- splitting, 52
- splitting locus, 119
- splitting rate, 117
- stabilizer code, 359
- Stark formula, 145

- Stark's inequality, 145, 149
- strict transform, 307
- structure
 - of level I , 25
 - of level N , 13
 - projective, 14
- structure morphism, 22
- subfield restriction, 401
- subspace design, 218
 - cascaded, 219
 - dimension of, 218
- substitution attack, 344
- Sudan algorithm, 200, 227
- supersingular module, 31, 32
- "supersingular" points, 32
- supersingular surface, 268
- support of a divisor, 404
- surface
 - cubic, 304, 305
 - rational, 304
- Suzuki curves, 96
 - function field of, 104, 105
- Suzuki group, 99
- symmetric bilinear complexity, 336
- symmetric interpolation system, 337
- symplectic code
 - large, 359
 - small, 359
- systematic A-code, 343
- tag, 343
 - size, 343
- tame ramification, 64
 - in a tower, 118
- TBC, *see* Tsfasman–Boguslavsky conjecture
- tensor product
 - of codes, 401
- tensor rank, 335
- torsion-riddled pro- p group, 187
- total ramification, 52
- total splitting, 52
- totally complex field, 59
- totally ramified extension, 63
- totally real field, 59
- tower, 116
 - almost normal, 165
 - of global fields, 142
 - recursive, 116
- towers
 - of classical modular curves, 37
 - of Drinfeld modular curves, 42
- trace, 56
 - relative, 59
- transmission rate, 397
- Tsfasman–Boguslavsky bound, 285
- Tsfasman–Boguslavsky conjecture, 284, 333
- Tsfasman–Serre–Sørensen bound, 280, 300, 333
- Tsfasman–Vlăduț–Zink bound, *see* basic algebraic geometry bound
- unconditional generalized
 - Brauer–Siegel theorem, 165
- uniform point set, 379, 395, 396
- uniformity (of an n -code), 351
- unimodular lattice, 231
- unirational surface, 268
- unit of an algebraic number field, 57
- unramified extension, 52, 60, 63
 - largest, 63
- unramified Fontaine–Mazur conjecture, 186
- valency (of a vertex), 296
- valid message, 344
- valuation, 58
 - normalized, 66
- valuation ring, 404
 - discrete, 50, 406
 - of a function field, 50, 406
 - of a place, 50, 406
- value
 - of a function at a point, 403
 - at a place, 51
- variety, 402
 - dimension of, 403
 - projective, 402
 - quasiprojective, 402
- Veronese embedding, 329
- weak approximation theorem, 53
- Weierstrass discriminant function, 12
- Weierstrass points, 8
- weight, 397
 - generalized, *see* generalized weight

- of a quantum error, 357
 - q -ary, 367
- weighted degree, 201
- Weil bound, 90, 409
- Weil explicit formula, 160
- Weil pairing, 13
- Weil theorem, 409
- wild ramification, 64
 - in a tower, 118
- wild ramification subgroup, 54
- Yaglom bound, 249, 277
- Yaglom map, 249, 277
- Zariski topology, 402
- zero of a function, 53
- zero of multiplicity r , 206
- zero order, 53
- zeta function
 - completed, 144, 155
 - of a curve, 407
 - Dedeking, 73
 - limit, 143, 155
 - numerator of, 408, 409