

## Index

- $O()$ , big- $O$ , 7
- $R$ , regulator, 21
- $\Delta$ , Vanvermonde, 217
- $\Delta$ , discriminant, 9
- $\mathbf{F}_p$ , finite field with  $p$  elements, 110
- $\Omega$ , real period, 21
- $\gamma_L(s)$ , Gamma factor, 56
- $\lambda_E(p)$ , also called  $a_p$ , 72
- $\ll$ , less-than-less-than, 7
- $f(E)$ , conductor, 18
- $\mu$ , Möbius function, 20
- III, Tate-Shafarevich group, 22
- $\sim$ , asymptotic, 7
- $\varepsilon$ , sign of the functional equation, 56
- $\varepsilon_p$ , sign of the Gauss sum, 77
- $o()$ , little- $o$ , 7
- $(\cdot)$ , Legendre symbol, 17
- 2-Selmer group, 35, 37
- 2-descent, 345
- 4-descent, 351
  
- absolutely irreducible, 112
- additive reduction, 18
- analytic rank, 30
- $a_p$ , 17
- approximate functional equation, 40
- asymptotic to, 7
- attraction, 65
- average rank, 72
  
- Barnes  $G$ -function, 98, 102
  - $G(\frac{1}{2})$ , 254
- big- $O$ , 7
- Birch and Swinnerton-Dyer
  - for twists, 201
  - full form, 21
  - over a number field, 247
  - simplest form, 20
- Brandt matrix, 267, 276, 280, 291
- BSD, *see* Birch and Swinnerton-Dyer
- canonical divisor, 120
- canonical height, 21
- Cassels pairing, 24, 325
- Cebotarev density theorem, 123, 191
- central value
  - computing, 260
- characteristic
  - of a field, 110
- characteristic polynomial, 58, 97, 254
  - moments of, 100, 104, 155, 254
  - ratios, 157
  - secular coefficient, 162
- class group
  - analogy with III, 324
  - heuristics, 323
- class number, 204
- class number formula, 262
- CM, *see* complex multiplication
- CM curves
  - are modular, 20
- Cohen-Lenstra heuristics, 323
- complex multiplication, 13
- conductor, 18
  - and rank, 26
  - of an  $L$ -function, 56
- congruent number, 9, 15–17, 20, 35, 341
- conjugate
  - of a quaternion, 274
- constant field, *see* field of constants
- critical value
  - computing, 260
- cubic twist, 237
- curve
  - over a finite field, 112
  - zeta function of, 124
- cuspidal form, 19
  
- decomposition group, 122
- degree
  - of a divisor, 118
  - of an  $L$ -function, 56

- of characteristic polynomial, 55
- Delta symbol, 42, 47, 48
- Dirichlet series, 19, 55
- Dirichlet's class number formula, 262
- discretization, 95, 202, 252
- discretization formula, 94
- discriminant, 9
  - $\Delta$ , 9
  - of a quaternion, 291
  - of an elliptic curve, 9
- division algebra, 274
- divisor
  - canonical, 120
  - degree of, 118
  - effective, 118
  - is rational, 118
  - of  $f$ , 120
  - on a curve, 118
  - prime, 118
  - support of, 118
- Dueñez model, *see* interaction model
- $E[n]$ ,  $n$ -torsion points of  $E$ , 13
- elliptic curve, 8
  - 2-descent, 345
  - analogy with number field, 324
  - and lattices in  $\mathbf{C}$ , 9
  - as a complex torus, 9
  - as a nonsingular cubic, 8
  - complex multiplication, 13
  - conductor, 18
  - discriminant, 9
  - endomorphism ring, 12
  - family, 27, 75
  - group law, 11
  - isogeny, 12
  - $j$ -invariant, 13
  - $L$ -function, 18, 19, 215
  - modularity of, 19
  - morphism, 11
  - must be non-singular, 9
  - over a function field, 128
  - over a number field, 247
  - point at infinity, 8
  - possible torsion groups, 15
  - quadratic twist, 171, 195
  - rank, 14
  - regulator, 21
  - twist, 13
  - Weierstrass form, 8
- elliptic functions, 10
- elliptic regulator, 21
- $\text{End}(E)$ , 12
- endomorphism ring, 12
- Euler product, 19, 56
- excess rank, 46
- explicit formula, 72
- family
  - of  $L$ -functions, 33, 57
    - arithmetic, 132
    - geometric, 132
  - of a given rank, 60
  - of characters, 56
  - of elliptic curves, 27, 60, 75
  - random matrix model, 58, 59
- field
  - of constants, 110
- finite field, 110
- first descent, 346
- Fricke involution, 19, 261, 273, 361
- Frobenius element, 122
- Frobenius map, 110
- Frobenius-Schur duality, 152
- fudge factors, 233, 260, *see* Tamagawa numbers
- function field
  - over a finite field, 110
- functional equation, 19, 56, 261
  - function field  $L$ -function, 127
  - of characteristic polynomial, 58
  - sign,  $w_E$ , 19
  - twisted, 215, 250
- fundamental discriminant, 192, 216
- Gauss sum, 250
- generalized theta series, 279
- group law, 11
- Hamilton quaternions, 275
- Hasse bound, 17, 72

- Hasse principle, 23  
 Hasse-Weil  $L$ -function, 18  
 Hecke operator, 19, 267, 268, 276, 290  
 Hecke relations, 85, 238  
 Heegner point, 203  
   as an embedding of quaternions, 264  
   of discriminant  $D$ , 264  
 height, 205  
   canonical, 21  
   of the generators, 64, 203  
   pairing, 276, 290  
 Heine-Szegö formula, 155  
 Hilbert class field, 204  
 Hilbert symbol, 347  
   of a quaternion algebra, 274  
  
 independent model, 63, 205  
 inertia group, 122  
 interaction model, 63, 204  
 isogeny, 12  
 isomorphism of curves, 114  
  
 $J_0(q)$ , jacobian of  $X_0(q)$ , 29  
 $j$ -invariant, 13  
 Jacobi-Trudi identity, 155  
  
 Kohnen subspace, 268  
 Kronecker symbol, 32, 96  
 Kummer map, 347  
  
 $L$ -function, 55  
   attached to Galois representation, 129  
   conjectured moment, 217, 219  
   cubic, 134  
   Dirichlet series, 19  
   Euler product, 19  
   examples over function fields, 127  
   functional equation, 19  
   of an elliptic curve, 18, 19, 215  
   spectral interpretation, 130  
   twisted, 215, 273  
 $\lambda_E(p)$ , also called  $a_p$ , 72  
 Legendre symbol, 17  
  
 $\ll$ , 7  
 little- $o$ , 7  
 lowest zero, 65  
  
 magic squares, 164  
 Miller model, *see* independent model  
 Möbius function, 20  
 modular symbol, 250  
 modularity  
   of a CM curve, 20  
   of an elliptic curve, 19  
 mollifier, 84  
 monodromy group, 45, 136, 138  
 Mordell's theorem, 14  
 Mordell-Weil group, 14, 20, 21, 26, 30, 97, 205, 346  
   analogy with unit group, 324  
 morphism  
   of elliptic curves, 11  
 morphism of curves, 113  
 multiplicative reduction, 18  
  
 naïve height, 21  
 Neumann-Setzer curves, 210  
 non-split reduction, 18  
 norm  
   of a quaternion, 274, 290  
  
 $O()$ , 7  
 $o()$ , 7  
 $\Omega$ , real period, 21  
 one-level density, 61  
   for restricted matrices, 63  
 order  
   in a quaternion algebra, 290  
  
 $\wp$ -function, 10  
 $p$ -Selmer group, 30, 325  
 parity conjecture, 30, 37, 171, 177  
 place of  $\mathbb{Q}$ , 274  
 plane partition, 161  
 Poincaré duality, 126  
 point at infinity, 8  
 prime divisor, 118  
  
 quadratic twist, 19, 171, 195

- in an arithmetic progression, 208
  - random matrix prediction, 33
  - rank at least four, 177
  - secondary terms, 215
- quaternion, 274, 290
  - conjugate of, 274
  - discriminant of, 291
  - norm of, 274
  - order in, 290
  - trace of, 274
- quaternion algebra, 274
- $R$ , regulator, 21
  - relation to III, 203
- ramification index, 121
- rank, 14
  - analytic, 30
  - and conductor, 26
  - bounding average, 72
- Rankin-Selberg convolution, 57
- rational divisor, 118
- rational function
  - on a curve, 115
- ratios
  - of characteristic polynomials, 157
- real period, 21
- reduced (quadratic) form, 263
- reduced norm, 290
- regulator, 21
- repulsion, 65, 137
- residue degree, 121
- Riemann hypothesis
  - for  $E \bmod p$ , 17
  - for a curve, 125
- Riemann-Hurwitz formula, 132
- Riemann-Roch theorem, 120
- root number, 30, *see* sign of the functional equation, 185
- Saturday night conjecture, 211
- Schur function, 149
  - combinatorial definition, 160
- second descent, 351
- secular coefficient, 162
- Selmer group, 23, 25, 30, 35, 46, 339, 341, 346
- separable field, 111
- III, 22
  - 2-part, 341
  - analogy with class group, 324
  - and 2-Selmer group, 346
  - and local-global principle, 324
  - Cassels pairing, 24, 325
  - cohomological definition, 25
  - conjectured to be finite, 24
  - heuristics, 323
  - primes dividing, 240
  - relation to regulator, 203
- Shimura correspondence, 266, 269, 273, 289–291, 315, 320
- sign
  - of the functional equation, 19
- Snaith model, *see* interaction model
- $SO(N)$ , 33, 58, 61, 94, 97, 205
- $Sp(N)$ , 58, 157
  - Haar measure, 158
- special value, 30
- spherical polynomials, 315
- split reduction, 18
- support of a divisor, 118
- symplectic matrix, 157
- Tamagawa number, 21
  - and quadratic twists, 189
  - Tate's algorithm for, 233
- Tate's algorithm, 233
- Tate-Shafarevich group, *see* III, 22, 71, 80, 104, 105, 198, 262
  - annoyed by, 332
  - cohomological definition, 25
- torsion group
  - 15 possibilities, 15
- trace
  - of a quaternion, 274
- twist, 13
  - and conductor, 19
  - by fundamental discriminants, 189
  - cubic, 237, 243, 249

- higher order, 243, 249  
 order 5, 249  
 quadratic, 19, 171, 195, 201
- $U(N)$ , 58, 144, 254  
 characters of, 150  
 Haar measure, 145
- Vandermonde, 151, 217  
 vanishing of quadratic twists  
 effect of 2-torsion, 189  
 power of logarithm, 189  
 random matrix prediction, 189  
 role of Tamagawa numbers, 189
- $w_E$ , sign of the functional equation, 19
- $w_N$ , the Fricke involution, 261
- Waldspurger formula, 269, 289, 315
- Weierstrass equation, 8
- Weierstrass  $\wp$ -function, 10
- Weyl character formula, 158
- Weyl integration formula, 144
- $X_0(27)$ , 237  
 table of data for twists, 246
- $X_0(32)$   
 table of data for twists, 246
- $X'_0(32)$ , 241
- $x^3 + y^3 = 13293998056584952174157235$   
 has rank at least 11, 237
- $x^3 + y^3 = m$ , 237
- $y^2 + 17xy - 120y = x^3 - 60x^2$ , 15
- $y^2 + 43xy - 210y = x^3 - 210x^2$ , 15
- $y^2 + 5xy - 6y = x^3 - 3x^2$ , 15
- $y^2 + 7xy = x^3 + 16x$ , 15
- $y^2 + xy + y = x^3 - x^2 - x - 14$   
 has conductor  $N = 17$ , 196  
 quadratic twists of, 196
- $y^2 + xy + y = x^3 - x^2 - 14x + 29$ , 15
- $y^2 + xy - 5y = x^3 - 5x^2$ , 15
- $y^2 + xy = x^3 - 45x + 81$ , 15
- $y^2 + y = x^3 + x^2 + x$ , 173
- $y^2 + y = x^3 - x$   
 has conductor 11, 19
- $y^2 + y = x^3 - x - 9$ , 231
- $y^2 + y = x^3 - x^2$   
 has discriminant  $\Delta = 11$ , 17
- $y^2 + y = x^3 - x^2 - 10x - 20$ , 230, 235
- $y^2 - xy - 4y = x^3 - x^2$ , 15
- $y^2 - y = x^3 - x$ , 15
- $y^2 = x^3 + 1$ , 15
- $y^2 = x^3 + 4$ , 15
- $y^2 = x^3 + 4x$ , 15
- $y^2 = x^3 + 8$ , 15
- $y^2 = x^3 - 1$   
 quadratic twists, 207
- $y^2 = x^3 - 2$ , 15
- $y^2 = x^3 - 24300$ , 25
- $y^2 = x^3 - 432m^2$ , 237
- $y^2 = x^3 - 4x$ , 15
- $y^2 = x^3 - 4x^2 - 160x - 1264$ , 235
- $y^2 = x^3 - d^2x$ , 35
- $y^2 = x^3 - m^2x$ , 241
- $y^2 = x^3 - x$ , 20, 173, 234, 241  
 has complex multiplication, 13  
 has discriminant  $\Delta = 64$ , 17  
 twists of, 13
- Young diagram  
 conjugate, 149  
 of a partition, 149
- Zagier and Kramarz, 237
- Zariski closed set, 112
- zeta function  
 of a curve, 124  
 spectral interpretation, 126