Index

abc-conjecture, 85–87
abscissa of convergence, 148
addition formulae for $\wp$-function, 221
Alaca, S., 69
Alford, W. R., 91, 98
algebraic integers, 61, 103
algebraic number fields, 61–62, 100–101
algebraic number theory, 69, 109, 144
algebraic numbers, 51, 100
'almost all' complex numbers, 53
'almost all' real numbers, 48
'almost all' natural numbers, 13
analytic number theory, 147–161
Apéry, R., 53, 157
Apostol, T. M., 17, 160, 194
arithmetical algebraic geometry, 58
arithmetical functions, 8–18
Arno, S., 194, 232
Artin, E., 34
associated (algebraic numbers), 122
automorph of a binary form, 39
average order of arithmetical functions, 13–14

Bachet, C. G., 40, 71, 76, 80
Bachmann, P., 34
Backlund, R., 176
bad reduction (elliptic curves), 230
Baker, A., 52, 54, 58, 66, 69, 76, 78, 84, 87, 194, 238
Balasubramanian, R., 209
Ball, K., 160
Barnes, E. S., 67
basis for an ideal, 112
Bernoulli numbers, 81, 158
Bertrand's postulate, 5, 150, 152
Bertrand, J., 152
Berwick, W. E. H., 109
Bessel function $J_0(z)$, 54
Beukers, F., 158, 160
Billing, G., 78
Birch, B. J., 209
Birch–Swinnerton-Dyer conjecture, 231, 232
Blake, I. F., 98, 237
Blichfeldt's result, 56, 123
Bombieri, E., 204
Bombieri–Vinogradov sieve inequality, 206
Borevich, Z. I., 34, 88, 144
box (pigeon-hole) principle, 43
Breuil, C., 83, 231
Brun, V., 148, 198
Brun–Titchmarsh inequality, 203

canonical decomposition, 4
Cantor, G., 53
Carmichael number, 91
Cassels, J. W. S., 34, 41, 58, 59, 84, 144, 237
Catalan equation, 83–86
Catalan's conjecture, 88
Catalan, E. C., 83
Chandrasekharan, K., 17, 153, 194
Chao Ko, 84
character of a group, 184
character, Dirichlet, 184, 186
character, Dirichlet, conjugate, 185
character, primitive, 189
character, principal, 184
Chatland, H., 67, 69
Chen Jing-Run, 148, 204
Chen's theorem, 6
Chevalley's theorem, 35
Chinese remainder theorem, 19, 23, 39, 200
Chowla, S., 211
circle (Hardy–Littlewood) method, 6, 41, 207–213
Clarkson, J. A., 149, 160
class field theory, 34
class number formulae, 189–190
class number of a number field, 127

class number of quadratic forms, 37
co-different of a number field, 118
Coates, J. H., 231, 232
Cohen, H., 144
Cohn, P. M., 99
Cojocaru, A. C., 213
complete quotients of continued fraction, 44
complete set of residues, 19
complex multiplication (elliptic curves), 231, 232, 235, 237
congruences, 19–27
congruent number, 231
congruent number problem, 231, 237
conjugate fields, 101
conjugates of an algebraic number, 61, 100
Conrad, B., 83, 231
Conrey, J. B., 170
continued fractions, 3, 44–46, 53, 58, 72, 94
convergents of continued fraction, 44
convex-body theorem, 56
coprime numbers, 2
Cox, D. A., 237
Cramér, H., 183
Cremona, J. E., 237
critical strip of zeta-function, 16, 170
cryptography, 90, 97, 215, 237
cyclotomic fields, 62, 80, 83, 85, 131–136
cyclotomic reciprocity law, 134

Davenport, H., 6, 41, 67, 69, 145, 177, 194, 209, 213
Davis, M., 7, 74, 148
deciphering key, 97
Dedekind zeta-function, 130
Dedekind's theorem, 129–131
Dedekind, R., 62, 99, 119, 120
definite and indefinite forms, 36
degree of a prime ideal, 117
degree of an algebraic number, 51, 100
degree of an algebraic number field, 61, 101
Deléglise, M., 160
Delaunay, B., 75
denominator of an algebraic number, 103
density hypothesis for zeta-function, 176, 183
Deshouillers, J.-M., 209
determinant of a lattice, 56
deterministic method, 90
Diamond, F., 83, 231
Dickson, L. E., 67, 74, 87
difference between consecutive primes, 5, 16, 183
different of a number field, 118
dimension theorem for number fields, 101–102
Diophantine approximation, 43–60
Diophantine equations, 52, 71–89, 215, 238
Diophantine geometry, 238
Diophantus, 71, 80
Dirichlet L-function, 131, 150, 186
Dirichlet character, 150, 184, 186
Dirichlet series, 148–150
Dirichlet's theorem on arithmetical progressions, 5, 187, 238
Dirichlet's theorem on Diophantine approximation, 43, 57, 64, 212
Dirichlet's unit theorem, 64, 123–126
Dirichlet, G. L., 82, 147, 184, 187–189
discriminant of a basis, 104
discriminant of a polynomial, 105
discriminant of a quadratic form, 36
discriminant of an algebraic number field, 62, 105
discriminant of an elliptic curve, 220
divisibility, 1–7
division algorithm, 1, 6, 99
division algorithm, generalized for ideals, 114
division criterion for ideals, 113
Dress, F., 209
dual basis of a number field, 118
Dyson, F. J., 52

Edwards, H. M., 17
Eisenstein series, 218
Eisenstein's criterion, 131
elliptic curves, 76, 96, 98, 193, 215–239
elliptic function, 216
elliptic isogeny theorem, 238
elliptic logarithm method, 238
elliptic modular function $j(z)$, 54, 222
Ellison, W. and F., 159
enciphering key, 97
endomorphism (elliptic curves), 235
equivalence of quadratic forms, 36
Eratosthenes sieve, 197–198
Erdős, P., 85, 88, 148, 153, 179, 183
Esmonde, J., 109
Estermann, T., 191, 194
Euclid, 4, 6, 147, 187
Euclid's algorithm, 2, 6, 46, 66
Euclidean fields, 66–67
Euler product of L-function, 186
Euler product of zeta-function, 15, 166
Euler pseudoprimes, 91–92
Euler's (totient) function ϕ, 9, 184
Euler's constant γ, 13, 53, 156, 183
Euler's criterion, 28, 91
Euler's identity, 53
Euler's theorem on congruences, 21, 97
Euler, L., 5, 6, 30, 39, 71, 82, 84, 149
even function, 218
explicit formula for $\zeta'(s)/\zeta(s)$, 172

factor base, 93
Faltings, G., 82, 88
Fermat bases, 93–94

Fermat equation, 80–83, 85
Fermat factorization, 93
Fermat primes, 5
Fermat pseudoprimes, 90–91
Fermat's last theorem, 54, 61, 62, 83, 99, 215, 231
Fermat's method of infinite descent, 40, 77, 81, 82, 227
Fermat's theorem on congruences, 21, 69, 90
Fermat, P., 5, 39, 71, 76, 80
Fermat–Catalan equation, 86
Fibonacci sequence, 59
field conjugates, 101
field of residues mod p, 20
field polynomial, 101
Fröhlich, A., 34, 109
fractional ideal, 117
fractional part of a number, 8
Frey, G., 82
Fueter, R., 76
functional equation for $\zeta(s)$, 15, 163–165
functional equation for L-function, 190
functional equation, approximate, 183
fundamental pair of periods, 216
fundamental parallelogram, 217
fundamental theorem of arithmetic, 4, 6, 62, 65

Galois field, 117
Gamma function, 177
Gauss' lemma, 29, 103
Gauss, C. F., 30, 33, 40, 66, 82, 147, 232
Gaussian field, 62, 68–69, 84
Gaussian integer, 68
Gaussian prime, 68
Gelfond, A. O., 52
Gelfond–Schneider theorem, 54
generators for an ideal, 111
Geometry of Numbers, 56, 59
Germain, Sophie, 82
Goldbach's conjecture, 6, 198, 204
Goldfeld, D. M., 193, 232
good reduction (elliptic curves), 230
Granville, A., 91, 98
greatest common divisor, 2
Green, B., 148, 213
Gross, B., 193, 231, 232
Győry, K., 87

Hadamard, J., 5, 148, 166, 179
Halberstam, H., 6, 213
Hall, M., 145
Hardy, G. H., 6, 16, 17, 26, 58, 148, 153, 170, 179, 183, 184, 207–209
Hasse (local–global) principle, 143
Hasse, H., 143, 231
Hasse–Weil L-function, 231
Hecke, E., 69
Heegner, K., 194
height, canonical (Néron–Tate), 224
height, classical (elliptic curves), 223
Heilbronn, H., 67
Hellegouarch, Y., 82
Hensel's lemma, 142
Hensel, K., 141
Hermite, C., 53
Hilbert's seventh problem, 53
Hilbert's tenth problem, 5, 7, 74
Hilbert's theorem on Waring's problem, 208
Hilbert, D., 41, 53, 208
Hoheisel, G., 183
Hua Loo-Keng, 208
Hurwitz's theorem, 47, 51
Hurwitz, A., 209
Husemöller, D., 237
Huxley, M. N., 160, 176, 183
hyperelliptic equation, 79

ideal class group, 127
ideal classes, 126–127
ideals in number fields, 111–121
ideals, fractional, 112, 117
ideals, prime, 113–114
ideals, principal, 112–113
inclusion–exclusion principle, 10, 197
indices (primitive roots), 26
Ingham, A. E., 160, 176, 177, 183
Inkeri, K., 67, 85
integer, p-adic, 140
integral basis of an algebraic number field, 62, 104
integral part of a number, 8
irrationality of $\zeta(3)$, 157–159
irreducible elements in number field, 62
isogeny (elliptic curves), 233
isomorphic (elliptic curves), 216
Ivić, A., 17, 177, 184
Iwaniec, H., 160

j-invariant, 216
Jacobi's symbol, 32, 130, 189
Jones, J. P., 7

Karatsuba, A. A., 17
Khintchine, A. Y., 58
Koblitz, N., 98, 237
Kolyvagin, A., 231
Korobov, N. M., 170, 171, 182
Kowalski, E., 160
Kronecker's theorem, 58
Kummer, E. E., 62, 80, 82, 99, 111
Kunrui Yu, 86

Lagrange multipliers, 201

Lagrange's theorem, 22
Lagrange, J. L., 22, 40, 48, 71
Lamé, G., 82
Lambert series, 18
Landau, E., 6, 41, 70, 148, 160
Lang, S., 109
lattice, 30, 56, 123
law of quadratic reciprocity, 30, 34
Lebesgue, V. A., 84
Legendre normal form, 236
Legendre's formula, 197
Legendre's symbol, 28, 130
Legendre, A. M., 30, 40, 82, 143, 147, 179
Lehman, R. S., 171
Leo Hebraeus, 84
Levinson, N., 170
Lewis, D. J., 209
Lindelöf hypothesis, 176
Lindelöf, E., 176
Lindemann, F., 53, 54
line of convergence, 148
linear congruence, 19
linear forms in logarithms, 53, 54, 76, 83–86
linear independence, 56, 57
Linnik, Yu. V., 148, 204, 213
Liouville function, 149
Liouville's theorem, 51–53, 75
Littlewood, J. E., 148, 171, 184, 207–209
Liu, Ming-Chit, 213
Ljunggren, W., 76
local fields, 139–144
logarithmic derivative of zeta-function, 157, 167
lowest common multiple, 4
Lutz–Nagell criterion, 228

Mahler, K., 209
Maillet, E., 209
Marcus, D. A., 109, 120
Markoff chain, 47
Mason, R. C., 86
Mason–Stothers theorem, 86
Masser, D. W., 85, 238
Matiyasevich, Yu. V., 7, 74, 148
Mazur, B., 230
Mersenne prime, 5, 15, 34
Mertens, F., 148, 150, 154
Mignotte, M., 85
Mihăilescu, P., 83, 85, 88
Miller–Rabin test, 92
minimal polynomial, 51
minimum polynomial, 100
Minkowski's conjecture, 58
Minkowski's constant, 128–129
Minkowski's linear forms theorem, 57, 124
Minkowski's theorem, 55–58, 123
Möbius function μ, 10
Möbius inversion formulae, 10
modular forms, 222
monic polynomial, 100
Montgomery, H. L., 41, 58, 177, 202
Mordell equation, 76–80, 139, 215, 216
Mordell, L. J., 76, 77, 79, 82, 87
Mordell–Weil group, 216, 220–222
Mordell–Weil rank, 228
Mordell–Weil theorem, 77, 80, 225–228
Mordell–Weil theorem, weak, 225
multiplicative functions, 9
Murty, M. R., 109, 160, 213

Nagell, T., 6, 26, 75, 84, 87, 89
Narkiewicz, W., 69
Neukirch, J., 120
Niven, I., 41, 58
non-singular elliptic curve, 229
norm in quadratic fields, 62
norm of an ideal, 114
norm, absolute, of an algebraic number, 102
norm, field, 102
norm, relative, 102
normal field, 117
number field, p-adic, 139
number field, $\mathfrak{p}$-adic, 140
number fields, 99–110
number fields, the different, 117–120
number of divisors τ, 12

odd function, 218
Oesterlé, J., 85, 194, 232
Oppenheimer, H., 67
Ostrowski, A., 139

parallelogram law, 225
parameterization of elliptic curves, 220
partial quotients of continued fraction, 44, 95
partial summation formula, 153
partition function, 207
Patterson, S. J., 17
Peano axioms, 1, 6
Pell equation, 39, 50, 64, 71–75, 95
perfect number, 14
Perron, O., 58, 67
Pillai, S. S., 153
Pollard's $p-1$ method, 96
Pomerance, C., 91, 98
Prachar, K., 182, 194
primality test, 90
primality testing, 90–98
prime, 4
prime ideal, 113
prime-number theorem, 5, 16, 179–182
primes in an interval, 202
primes in arithmetical progressions, 187–189, 204, 206

primes in quadratic fields, 65
primitive roots, 23–25, 185
principal form, 36
principal ideal, 112
principle of mathematical induction, 1
probabilistic method, 90
product formula in number fields, 141
product of ideals, 112
pseudoprime, Euler, 91
pseudoprime, Fermat, 90
pseudoprime, strong, 92
purely periodic continued fractions, 50
Putnam, H., 7, 74, 148
Pythagorean triples, 81

quadratic character, 130
quadratic congruence, 28
quadratic fields, 61–70
quadratic forms, 36–42
quadratic irrationals, 48–50
quadratic residues, 28–35
quaternions, 40
quotient ring for ideals, 114

Rényi, A., 148, 204
Rédei, L., 67
radical (or conductor) of an integer, 85
Ramanujan's sum, 18, 210
Ramanujan, S., 89, 148, 207
ramification index, 117
Rankin's trick, 214
rational approximations, 46–48, 59
reduced curve, mod p, 229
reduced set of residues, 21
reduction of quadratic forms, 37
regular prime, 80
regulator, 125
Reisel, H., 98
relatively prime numbers, 2
Remak, R., 67
repeated-squaring method, 90, 97
representation by binary forms, 38
residue class, 19
residue class ring for ideals, 114
Ribenboim, P., 87, 160
Ribet, K. A., 83
Richert, H. E., 6, 213
Rieger, G. J., 208
Riemann hypothesis, 16, 54, 170, 183, 204
Riemann hypothesis, generalized, 207, 210
Riemann hypothesis, quasi, 171
Riemann zeta-function, 5, 15–17, 53, 130, 162, 183, 190
Riemann, B., 148
Riemann–Roch theorem, 215
Riemann–von Mangoldt formula, 174, 190
Rivat, J., 160
Rivoal, T., 160
Robinson, J., 7, 74, 148
roots of unity in number fields, 122
Rosser, J. B., 160
Roth, K. F., 52, 57, 204, 205
RSA algorithm, 97, 98
Runge, C., 80

Schinzel, A., 80, 88
Schmidt, W. M., 57, 59
Schmitt, S., 237, 238
Schoenfeld, L., 160
Schoof, R., 88
Selberg formula, 183
Selberg, A., 148, 170, 179, 183, 198
Selberg, S., 84
Selfridge, J. L., 85, 88
Seroussi, G., 98, 237
Serre, J.-P., 144
Shafarevich, I. R., 34, 88, 144
Shimura, G., 232
Siegel zero, 193
Siegel's theorem on L-functions, 191–194
Siegel, C. L., 52, 57, 79, 80, 190
Siegel–Walfisz theorem, 190
sieve methods, 6, 197–207
sieve, Eratosthenes, 6, 198, 199
sieve, large, 204–207
sieve, Selberg, 198–204
Silverman, J. H., 237
Skewes number, 171
Skewes, S., 171
Skolem, T., 76, 87
Smart, N. P., 98, 237, 238
Solovay–Strassen test, 92
squaring the circle, 53
standard factorization, 4
Stark, H. M., 6, 66, 78, 194
Stewart, C. L., 86
Stewart, I., 69, 88
Stickelberger's criterion, 105
Stothers, W. W., 86
strong pseudoprime, 92
sum of divisors σ, 12
sum of four squares, 40
sum of ideals, 114
sum of three squares, 40
sum of two squares, 39, 69
superelliptic equation, 79, 84
Swinnerton-Dyer, H. P. F., 67
Sylvester's argument, 10
Sylvester, J. J., 160
symmetric function theorem, 99
Szpiro, L., 86

Tall, D., 69, 88
Taniyama–Shimura conjecture, 83

Tao, T., 148, 213
Tate, J., 34, 237
Taylor, M. J., 109
Taylor, R., 83, 231
Tchebychev functions, 156
Tchebychev's estimates, 151–153
Tchebychev, P. L., 147, 149, 152, 160, 206
te Riele, H. J. J., 171
Thaine, F., 85
Thue equation, 74–76
Thue, A., 52, 57, 75
Tijdeman, R., 83, 84
Titchmarsh, E. C., 17, 177
torsion subgroup (elliptic curves), 228
totally ramified, 117
trace, absolute, of an algebraic number, 102
trace, field, 102
trace, relative, 102
transcendence theory, 57, 58, 238
transcendental numbers, 51–55
Trost, E., 183, 194
Tunnell's criterion, 232
twin-prime conjecture, 6, 198, 199, 204

uniformization theorem, 222
unimodular substitution, 36
unique factorization domain, 62, 65
units in number fields, 62–65, 122–126
unramified prime ideal, 117
Uspensky, J. V., 207

Vallée Poussin, C. J. de la, 5, 148, 166, 170, 171, 179, 189
valuation, 139
valuation, p-adic, 139
valuation, Archimedean, 139
valuation, non-Archimedean, 139
van der Corput, J. G., 211
Vaughan, R. C., 41, 177, 202, 213
Vinogradov's notation, 75, 157, 167
Vinogradov, A. I., 204
Vinogradov, I. M., 6, 26, 148, 170, 171, 182, 207, 208, 210, 212
von Mangoldt's function Λ, 17, 157, 167
von Mangoldt, H., 148
Voronin, S. M., 17

Wagstaff, Jr., S. S., 81
Waldspurger, J.-L., 232
Walfisz, A. Z., 190
Wang, Tianze, 213
Waring's problem, 41, 207
Waring, E., 21, 207
Washington, L. C., 98, 237
Watkins, M., 194
Weber, H., 99
Weierstrass $\wp$-function, 54, 216–220
Weierstrass equation, 215
Weil, A., 34, 77, 109
Wieferich criterion, 85
Wieferich, A., 82
Wiles, A., 80, 82, 88, 231, 232
Williams, K. S., 69
Wilson's theorem, 21
Wolfskehl Prize, 83
Wolstenholme's theorem, 27
Wooley, T., 209
Wright, E. M., 6, 17, 26, 58, 153, 183
Wüstholz, G., 58, 87, 238

Zagier, D., 193, 231, 232
Zimmer, H. G., 237, 238
Zuckerman, H. S., 41, 58
Zudilin, W., 160