Index

ABC-conjecture, 222
Abel, N. H., 5
AGM, 199, 200, *see also* arithmetic–geometric mean
Agrawal, M., 124
arithmetic–geometric mean, 5, 199

Bachet, C., 2
Baker, A., 7, 9, 59, 82, 98, 100, 117, 137, 138, 148, 225
Baker-Wüstholz theorem, 102, 107, 123, 137, 225
Bernstein, D., 117
Bhaskara, 5
Bilu, Y., 105, 108, 110, 124, 197
binary form, 97, 151, 155, 220, *see also* quadratic form, cubic form, quartic form
Birch, B. J., 152
Birch–Swinnerton–Dyer algorithm, 187
Birch–Swinnerton–Dyer conjecture, 193
Bombieri, E., 105
Brahmagupta, 5

Cantor's algorithm, 216
Cassels, J. W. S., viii, 17, 183, 222
Catalan's equation, 222
Catalan, E., 222
Chabauty, C., 217
Cholesky, 66
Coates, J., 117, 124, 134
Coghlan, F. B., 206
Cohen, H., viii, 198
Coleman, R. F., 218
complexity, 8, 42, 50
continued fraction, 4, 59, 105
  convergents, 60
  partial quotient, 60
  purely periodic, 61
Coombes, K. R., 219
Cremona, J. E., xii, 190, 210
Crouch, S., xii
cubic form, 151

Davenport, H., 7, 59, 82
David's theorem, 205, 207, 227
David, S., 197, 205, 207, 227
decomposable form, 155
Dem'janenko, V., 218
descent, 2, 52
  2-descent, 183
  higher, 185
  infinite, 190
  via 2-isogeny, 183
Diophantos, 2
discriminant form, 165
discriminant form equation, 45, 165–167, 169–172, 174
divisor, 213

elliptic curve, 1, 50, 124, 177, *see also* descent
  canonical height, 180, 181, 191, 192, 210, *see also* height
  conditional algorithm, 192
  conductor, 124, 193
  group law, 179
  height, 226
  height pairing matrix, 182
  integral points, 10–12, 45, 111–115, 150, 151, 202–210
  L-series, 193
  minimal model, 178
  naive height, 180, 191
  Neron–Tate height, 181, *see also* elliptic curve, canonical height
  regulator, 182
elliptic function, 198
elliptic logarithm, 198
  p-adic, 209
Ellison, W. J., 7
Eratosthenes, 40

Euler, L., 3, 4, 221
Evertse, J. H., 134, 152
exponential time, 8

factoring, 1, 40, 48, 53, 119, 144
  polynomial, 75
Faltings' theorem, 9, 152, 213, 217
Fermat's last theorem, 1, 3, 193, 221
Fermat's little theorem, 20, 34
Fermat, P., 2, 52, 221
Fincke-Pohst, algorithm, 66
Flynn, E. V., 218
form, *see also* binary form, discriminant form
  decomposable, 155
formal group, 208
Frey curve, 221
Frey, G., 221

Gaál, I., 165, 171–173
Gauss, C. F., 4, 5, 199
Gram matrix, 75
Gram–Schmidt Process, 67
Grant, D., 219
GRH, 9, 50, 98
Guy, R., 205
Győry, K., x, 134, 152, 153, 167

Hanrot, G., 105, 108, 110, 124, 197
Hardy, G. H., 59
Hasse principle, 40, 49, 182, 184
Hasse's theorem, 40
Hasse, H., 5
height, 134, 147, *see also* elliptic curve, canonical height
  function, 22
  Mahler, 22
  modified, 106, 126, 148, 225–227
  Weil, 22
Hensel's lemma, 23, 36, 47
Hensel, K., 5, 23
Hermite's theorem, 66, 192, 194
Hermite, C., 151, 190
Hilbert, problems, 6
Holzer's theorem, 49
Hunt, D., 124
hyper-graph, 154
hyperelliptic curve, 50, 215
hypergeometric functions, xi

index form, 166
integral point, 10, *see also* elliptic curve, integral points
invariant theory, 187

Jacobian, 214
Julia, G., 190

knapsack problem, 79
Koblitz, N., 17

Lagrange, J. L., 4, 52, 151, 199
Lang, S., 23, 197
lattice, 65, *see also* LLL
  approximation, 64
  basis, 65
  determinant, 66
  enlargement, 191
  successive minima, 66
Lebesgue, V. A., 222
Lenstra, A. K., viii, 7, 67
Lenstra, H. W., viii, 7, 67, 152
Ljunggren, W., 206
LLL, 36, 67–75
  de Weger's variant, 73
  reduced basis, 67
Lovász, L., viii, 7, 67

Mahler, K., 117
Manin, J., 218
Mansfield, E., xii
Matijasevič, J., 7
Merriman, J. R., 152
Mordell's equation, 206
Mordell, L. J., vii, 5, 45, 111, 180, 217
Mordell–Weil group, 50, 177, 179, 197, 215, 218
Mordell–Weil theorem, 180, 190, 216
  weak form, 182–186, 188–190

Nagell, T., 6, 222
Neron, A., 181
Number field sieve, 119

Ochoa curve, 205

p-adic
  elliptic logarithm, 209
  exponential, 31
  integer, 18
  logarithm, 28
  metric, 17
Padé approximations, xi
Pell's equation, 4, 62

Pethő and de Weger's lemma, 103, 122, 123, 137, 141, 229
Pethő, A., xii, 6, 97, 103, 105, 165, 171, 172, 229
Picard group, 214
Pohst, M., viii, 165, 171, 172
Poincaré, J. H., 5, 180
polynomial time, 8, 73
van der Poorten, A. J., 124
Prime ideal removing lemma, 118
product formula, 21
Pythagorean triples, 2

quadratic form, 66, 171, 181, 186, 216
  binary, 5, 54, 55, 112, 114, 151, 172, 184
  quarternary, 211
  ternary, 46, 51, 54, 112, 114, 171, 172, 184
quartic form, 184, 188
  covariants, 188
  invariants, 187

Ramanujan, S., 6
Ramanujan–Nagell equation, 6
Rémond, G., 210
Ribet, K., 221
Rose, H., viii

S-integers, 21
S-unit equation, 99, 133–152, 156, 167, 205
S-units, 21
Schmidt, W. M., 105
Selmer group, 185
Selmer, E., 40
seminvariants, 188
Serre, J. P., 221
Shimura–Taniyama–Weil conjecture, 193, 222
Shipsey, R., xii
Shorey, T., vii
Siegel's identity, 36, 37
Siegel, C. L., 99, 134
Siksek, S., xii, 51, 191
Silverman, J. H., 23, 181, 191
Skolem's method, 33, 36–39, 97, 103, 105
Skolem, Th., 5, 36
Stephens, N., xii, 206
Strassmann's theorem, 25, 33–36, 218
Stroeker, R., 206
subexponential time, 8, 48
superelliptic curve, 220

Tate, J., 181
Tate–Shaferevich group, 185
Thue equation, ix, 7, 33–36, 38, 45, 97, 99–117, 120, 122, 129, 133, 135, 137, 151, 170–173, 197, 211, 220
Thue, A., 7, 97
Thue–Mahler equation, ix, 97, 117–135, 137, 151, 153, 161
Tijdeman, R., vii, 223
triangularly connected decomposable forms, 153–163, 165, 167, 173, 220
Tzanakis, N., 97, 98, 105, 117, 210

Urfels, F., 210

Waldschmidt, M., 9
de Weger, B. M. M., vii, xii, 6, 7, 31, 73, 82, 97, 98, 103, 105, 117, 206, 229
Weierstrass
  $\wp(z)$-function, 198
  long form, 177–179, 202
  short form, 179, 183, 215
Weierstrass, K., 5
Weil, A., 180
Wildanger, K., 133
Wiles, A., 1, 193, 221, 222
Wright, E. H., 59
Wüstholz, G., 9, 137, 138, 148, 225

Yu's theorem, 121, 123, 141, 226
Yu, K., 9, 226

Zagier, D., 201, 205, 210
Zassenhaus, H., viii