

# Index

- $\mathbb{Z}$ -basis, 95
- $\mathbb{Z}$ -combination, 94
- $\mathbb{Z}$ -span, 95
- $f$ -equivalence of ordered pairs, 143, 326
- $p$ -automorph map, 241
  - image, 241
  - kernel, 241
- $p$ -congruence subgroup, 236
- $p$ -equivalence of quadratic forms, 236
- $p$ -matrix group of discriminant  $\Delta$ , 240
  
- algebraic integer, 56
- algebraic number, 56
- associate elements
  - in a quadratic domain, 66
  - in the Gaussian integers, 26
- automorph
  - of  $x^2 - dy^2$ , 258
  - of a quadratic form, 142, 367, 376
  - of an indefinite quadratic form, 318
- automorphism of a field, 334
  
- Baker, 87
- basis element
  - of a discriminant, 61
- basis index
  - of a discriminant, 61
- Bhāskara, 253
- binary quadratic form, 132
- Brahmagupta, 253
- Brouncker, 253
  
- candidate form
  - of positive discriminant, 286
- Cattle Problem of Archimedes, 253
- Cauchy sequence, 246
- character
  - of a Gaussian integer, 32
  - of a quadratic integer, 68
  - of an ideal, 97
  - of an ideal number, 75
- characteristic polynomial, 336, 372
- Chinese Remainder Theorem, 5
- class of an ideal, 172
- class of quadratic forms, 137
- combination, 94, 101
  - of a pair of integers, 2
- complete ideal, 113
- complete quadratic domain, 65, 91, 227, 291
- composite number, 2
- composition of quadratic forms, 164, 167
- congruence
  - modulo an ideal, 98
  - modulo an integer, 4
- congruence cancellation property, 4, 37
- conjugate
  - of a complex number, 26
  - of a matrix, 133
  - of a quadratic form, 133
  - of a quadratic integer, 61
  - of a quadratic number, 57, 269
  - of an ideal, 102
  - of an ideal number, 75
- conjugate subgroup, 143
- continued fraction, 247
  - finite, 259
  - finite simple, 260
  - infinite simple, 260
  - of a quadratic form, 301
  - period length, 269
  - periodic, 269
  - purely periodic, 269
- continued fraction algorithm, 249, 265
- convergent of a continued fraction, 249, 261, 311

- denominator, 261
- numerator, 261
- coset, 143
- cyclic group, 334
- Dedekind, 93, 104, 164
- discriminant, 61, 91, 132, 270
  - of a quadratic form, 132
  - of a quadratic number, 60, 91, 269
  - of a quadratic polynomial, 6, 57, 346
  - primitive, 61
- Disquisitiones Arithmeticae, 164
- divisibility
  - in a quadratic domain, 66
    - using ideal form, 71
  - in the Gaussian integers, 26
    - using ideal form, 35
  - in the integers, 1
  - of ideals, 108
- division algorithm, 1
  - for Gaussian integers, 27
  - quotient, 1
  - remainder, 1
- divisor
  - of a Gaussian integer, 32
  - of a quadratic integer, 68
  - of an ideal, 97
  - of an ideal number, 75
- equivalence
  - of ideals, 154
  - of quadratic forms, 137
- equivalence algorithm
  - for indefinite quadratic forms, 301
  - on candidate forms, 288
- Euclid's Lemma, 2
- Euclidean algorithm, 3, 247
- Euler, 21, 253
- Euler totient function, 363
- Euler's Criterion, 8
- Fermat, 17, 21, 253
- Fermat's Christmas Theorem, 21
- Fibonacci sequence, 250, 335
- floor function, 51
- form class group, 173, 320
- Fundamental Homomorphism Theorem, 239
- fundamental solution of Pell's equation, 254, 371
- Fundamental Theorem of Finite Abelian Groups, 178
- fundamental unit, 316
- Galois, 269
- Gauss, 87, 164
- Gaussian integer, 25
  - primitive, 32
- genus (genera), 147, 291
- genus equivalence
  - of ideal classes, 191
  - of ideals, 191
  - of quadratic forms, 147, 291
- genus symbols
  - for a quadratic form, 146, 291
  - for an ideal, 191
  - for an ideal class, 191
- Girard, 17, 21
- golden ratio, 63, 249, 337
- greatest common divisor, 2
- group of automorphs of a quadratic form, 142
- group of units of a field, 334
- ideal, 94
  - nontrivial, 94
  - primitive, 97
  - proper, 94
- ideal class group, 172, 320
- ideal form
  - for a Gaussian integer, 32
  - for a quadratic integer, 68, 91
- ideal multiplication formula, 119
- ideal notation for a quadratic form, 135
- ideal number, 75, 88, 91, 93
- ideal number notation for an ideal, 96
- ideal of a quadratic form, 154
- indefinite quadratic form, 132
- index
  - of a class of quadratic forms, 173
  - of a discriminant, 61
  - of a quadratic form, 132
  - of an ideal, 108
  - of an ideal class, 172
- inert prime, 83, 106
- integral domain, 64
- invariant factor type, 178, 187
- involution of quadratic forms, 138
- irreducible
  - Gaussian integer, 27
    - in ideal form, 38
  - ideal number, 89
  - quadratic integer, 67
    - in ideal form, 81

- Jacobi symbol, 14, 148
- kernel of  $\mathcal{F}_{p^2\Delta}$ , 229
- Kronecker symbol, 13, 83, 230
- Kummer, 93, 164
- Lagrange, 164, 274
- least common multiple, 3
- Legendre symbol, 7
- linear congruence, 5
- Lucas sequence, 343
- matrix of a quadratic form, 133
- maximal ideal, 104
- Mersenne, 21
- minimum polynomial of a quadratic number, 60, 91, 269
- negative
  - of a quadratic form, 133
- negative conjugate
  - of a quadratic form, 133
- negative definite quadratic form, 132
- norm
  - of a complex number, 26
  - of a Gaussian integer, 26
  - of a quadratic integer, 61
  - of a quadratic number, 57
  - of an ideal, 97
- norm class of quadratic forms, 138
- norm equivalence of quadratic forms, 138
- number of proper representations
  - by  $x^2 + y^2$ , 49
- number of representations
  - by  $x^2 + y^2$ , 18, 50
  - by a quadratic form, 144
- number of solutions
  - of a linear congruence, 5
  - of a quadratic congruence, 7
- order
  - of a quadratic recursive sequence, 344
  - of an element in a group, 334
  - of an integer modulo  $m$ , 4, 344
- ordered basis of an ideal, 161
- palindromic quadratic number, 278, 314
- Pell, 253
- Pell's equation, 254
- Pell's equation algorithm, 255
- polar coordinates, 33
- polynomial
  - monic, 56
  - over a finite field, 334
- positive definite quadratic form, 132
- prime element
  - of a quadratic domain, 80
- prime ideal, 104
- prime number, 2
- primitive ordered pair, 140
- principal form, 62
- principal genus, 192
- principal ideal, 94, 99
- principal ideal domain, 81, 100, 170
- principal ideal number, 75, 91
- principal ideal number domain, 81, 100
- principal polynomial, 62, 91
- principal square domain, 206
- product of ideals, 107
- projection homomorphism, 235, 376
  - kernel, 238
- proper representation
  - by  $2x^2 + 13y^2$ , 216
  - by  $2x^2 + 15y^2$ , 211
  - by  $2x^2 + 3y^2$ , 207
  - by  $2x^2 + 7y^2$ , 213
  - by  $2x^2 + xy - 7y^2$ , 325
  - by  $2x^2 + xy - 8y^2$ , 326
  - by  $2x^2 - 3y^2$ , 321
  - by  $2x^2 - 5y^2$ , 325
  - by  $3x^2 + 10y^2$ , 211
  - by  $5x^2 + 13y^2$ , 218
  - by  $5x^2 + 6y^2$ , 211
  - by  $\pm(5x^2 + xy - 11y^2)$ , 324
  - by  $\pm(5x^2 - 7y^2)$ , 323
  - by  $\pm(x^2 + xy - 55y^2)$ , 324
  - by  $\pm(x^2 - 23y^2)$ , 326
  - by  $\pm(x^2 - 35y^2)$ , 323
  - by  $\pm(x^2 - 7y^2)$ , 325
  - by  $x^2 + 14y^2$ , 213
  - by  $x^2 + 26y^2$ , 216
  - by  $x^2 + 2y^2$ , 85, 200
  - by  $x^2 + 30y^2$ , 211
  - by  $x^2 + 3y^2$ , 85, 202
  - by  $x^2 + 6y^2$ , 207
  - by  $x^2 + 7y^2$ , 84, 203
  - by  $x^2 + xy + 2y^2$ , 84
  - by  $x^2 + xy + y^2$ , 85
  - by  $x^2 + xy - 14y^2$ , 325
  - by  $x^2 + xy - 16y^2$ , 326
  - by  $x^2 + y^2$ , 18
  - by  $x^2 - 10y^2$ , 325
  - by  $x^2 - 6y^2$ , 321
  - by a principal form, 84

- by a quadratic form, 132
- quadratic congruence, 6
  - modulo a prime, 6
  - modulo a prime power, 10
  - modulo a relatively prime product, 12
- quadratic continued fraction algorithm, 256, 296, 368
- quadratic domain, 61, 91
- quadratic extension field, 334, 345
- quadratic field, 57
- quadratic form, 132
  - coefficients, 132
  - primitive, 132
- quadratic form composition formula, 167
- quadratic form of an ordered basis, 161
- quadratic integer, 56, 91
  - primitive, 68, 84, 254
- quadratic number, 56, 91, 269
- Quadratic Reciprocity Theorem, 8
- quadratic recursive sequence, 336, 369, 371, 376
- quadratic subdomain, 65, 91, 227
- ramified prime, 83, 106
- rational integer, 25, 57
- recurrence relation, 336
- reduced ideal, 186
- reduced quadratic form, 179
- reduced quadratic number, 270, 277
- reducible, 67
  - Gaussian integer, 27
- reduction algorithm
  - for ideal forms
    - in the Gaussian integers, 45
  - for ideal numbers, 77
- relatively prime, 2
- representation
  - by  $x^2 + y^2$ , 18
  - by a principal form, 84
  - by a quadratic form, 132
  - by an indefinite form, 320
- semi-reduced quadratic number, 277, 313
- set of representatives of  $\mathcal{F}_\Delta$  in  $FGp^2\Delta$ , 228
- split prime, 83, 106
- squarefree integer, 18, 57
- squarefree part of a discriminant, 61
- standard notation for a quadratic form, 135
- Stark, 87
- subnorm
  - of a Gaussian integer, 32
  - of a quadratic integer, 68
  - of an ideal, 97
  - of an ideal number, 75
- suborder
  - of a quadratic recursive sequence, 344, 372, 376
  - of an element of  $\mathbb{F}_p$ , 350
- suborder function on  $\mathbb{F}_p$ , 350
- suborder number, 351, 373
- suborder sequence, 357
- suborder subsequence, 362
- sum of ideals, 101
- symmetric matrix, 133
- translation of quadratic forms, 139
- transpose of a matrix, 133
- unimodular matrix, 136, 367
- unique factorization domain, 80, 82, 86, 170
- unit
  - in a quadratic domain, 66, 316
  - in the Gaussian integers, 26
- upper bound
  - of a negative discriminant, 77, 180, 187
  - of a positive discriminant, 286
- Wallis, 253