
Subject Index

- Algebraic number theory, 64, 89
Ambiguous class, *see* Class group
Ambiguous form, *see* Quadratic forms, binary
Automorphism, *see* Quadratic forms
- Baker, A., 187
Binomial coefficients, 19, 20, 30
Birch and Swinnerton–Dyer conjecture, 188
Box principle, 48. *See also* Pigeon-hole principle
- Character, group, 88
Chebyshev, P. L., 1, 3, 17, 19
Chinese remainder theorem, 64, 65–66
Class group, 102, 147, 152–156, 160, 183. *See also* Class number; Quadratic forms, binary
 ambiguous class, 159, 160, 164–168
 composition:
 of classes, 151–153
 of forms, 149, 154
 concordant forms, 149, 150, 155
 principal class, 152, 154
Class number, 133, 183–189. *See also* Class group
 equals one, 155–156, 184–185
 finiteness, 58, 61–62, 129, 152, 181
Composite integer, 2, 3, 94
 witness, 94
Composition, *see* Class group; Product identities
Concordant forms, *see* Class group
Congruences, 25, 26. *See also* Integers mod m
 biquadratic
 $x^4 \equiv a$, 34, 95, 103
 composite modulus 65–67
 linear, 66, 69, 127, 155
 quadratic, *see also* Legendre symbol
 $x^2 \equiv -1$, 25, 27–28, 30, 178
 $x^2 \equiv \pm 2$, 31, 53–54, 76
 $x^2 \equiv -3$, 31, 38
 $x^2 \equiv 5$, 31
 $x^2 \equiv a$, 28, 63–64, 67–69, 70, 95, 97–98, 99, 102
 $x^2 + y^2 \equiv -1$, 52
 $x^2 + y^2 \equiv a$, 55
 others, 95, 175–177
Conjugation in quadratic ring, 111, 117
Continued fractions, 10, 135, 138
 nearly simple, 135–136, 140
Convenient numbers, *see* Genus group
Convex set, 50
Cyclic groups, 29, 31, 131
Cyclotomic ring, 89
- Decimal fractions, 31
Dedekind domain, 89
Descent, 25, 50–52, 105
 infinite, 52
Deuring, M., 186
Diophantine approximation, *see* Rational approximation
Diophantine equations, vii. *See also* Sum of squares; Pell equation
 linear, 1, 11–16, 119, 124
 positive solutions, 16, 17
 quadratic:
 $x^2 = 2y^2$, 52, 105
 $x^2 + y^2 = n$, *see* Sum of squares, two
 $x^2 \pm 2y^2 = n$, 33–34, 50, 53–54
 $x^2 + 3y^2 = n$, 38, 62
 $x^2 + xy + y^2 = n$, 38, 60, 62

- Diophantine equations, vii. (*Continued*)
 $x^2 + 5y^2 = n$, 102, 148, 154, 160
 $x^2 + 36y^2 = p$, 103, 161
 $x^2 + 64y^2 = p$, 95, 161
 $y^2 = 2x^2 + 1$, 105–108
 $x^2 - dy^2 = \pm 1$, *see* Pell equation
 $x^2 - dy^2 = m$, 123, 124
 $ax^2 + bxy + cy^2 = m$, 104–105, 118–123,
 128, 134. *See also* Prime numbers,
 representation by quadratic forms
 $x^2 + y^2 = z^2$, 54
 others:
 $y^2 = x^3 + k$, 34, 39
 $x^2 + 3y^2 = z^3$, 39
 $x^3 + y^3 = z^3$, 55
 $x^3 + py^3 + p^2z^3 = 0$, 53
 $x^3 + dy^3 + d^2z^3 - 3dxyz = 1$, 118
 $y^2 = x^3 - x$, 55
 $x^4 + y^2 = z^4$, 55
 $x^4 + y^4 = z^2$, 54
 $x^4 + y^4 = z^4$, 54
 Dirichlet, P. G. L., primes in arithmetic
 progressions, 4, 5, 23, 99, 158–159, 162,
 172, 204
 $3k + 2$, 5
 $4k + b$, 4, 22–23, 24, 32
 $5k - 1$, 76
 $6k + 5$, 5
 $8k + b$, 34, 76
 $10k + 1$, 32
 $10k + 9$, 76
 $p^nk + 1$, 32
 Discriminant, 95, 180. *See also* Quadratic
 forms, binary
 fundamental, 183, 184
 Divisibility, 2, 25
 divisor a product, 10
 of factors in product, 8, 9
 Division algorithm, 6, 28, 35
 Divisors:
 common, 6
 greatest common (GCD), 1, 6, 7, 9, 12, 13,
 35–36
 number, 10
 sum, 10, 11
 Duplication theorem, *see* Genus group
 Egyptian fraction, 47
 Elementary divisors, 16
 Elliptic curve, 187–188
 Equivalence of forms, *see* Quadratic forms
 Eratosthenes, 3
 Euclid, 2, 17, 34
 Euclidean algorithm, 6, 36, 119
 Euclidean domain, 36
 Euclid's lemma, 8
 Euler, L., 17, 22, 23, 52, 63, 73, 161, 185
 Euler product, 17–18, 22–23
 Factorization, 119
 of factorials, 20
 uniqueness, 36, 89
 Gaussian integers, 25, 34–36
 integers, 1, 8–9, 18
 other rings, 38, 39
 Farey sequences, 39–45, 47
 Father, vii
 Fermat, P., 5, 24, 50, 51
 last theorem, 54, 55, 89
 little theorem, 26–27, 30
 Fibonacci numbers, 9, 118
 Fourier transform, 84–89
 Frobenius, G., 185
 Fundamental theorem of arithmetic, *see*
 Factorization, uniqueness
 Fundamental unit, *see* Order, units in
 Gardner, Martin, vii
 Gauss, C. F., 1, 17, 34, 63–64, 72, 77, 80, 83,
 102, 129, 147, 149, 157, 162, 163, 178, 180,
 181, 183, 184
 Gaussian form, *see* Quadratic forms, binary
 Gaussian integers, 34–38
 generalizations, 89, 111–112. *See also* Order
 Gauss lemma, 64, 80–83
 Gauss sums, 64, 83, 89, 90–91
 Gauss symbol, *see* Genus group
 Genus group, 102, 147–148, 157–158. *See also*
 Class group
 convenient numbers, 161
 duplication theorem, 159, 160, 162, 168, 172,
 175
 Gauss symbol, 157
 principal genus, 157, 160, 175
 Geometry of numbers, *see* Minkowski's
 theorem
 Goldfeld, D. M., 187, 188
 Greatest common divisor, *see* Divisors, greatest
 common
 Gronwall, 186
 Gross, B. H., 188
 Hadamard, J., 17
 Heegner, K., 186, 187
 Heilbronn, H., 186
 Hensel's lemma, 65, 69

- Identity, *see* Product identities
 Infinite descent, *see* Descent, infinite
 Integers, *see also* Factorization; Prime numbers
 nonsquare, 99, 109
 relatively prime, 7
 squarefree, 11
 Integers mod m , 25, 26. *See also* Congruences
 invertible, 26, 30
 primitive roots, 29–32, 54, 74, 75
 roots of polynomials, 28, 30, 67, 69
 Irrational numbers, 11, 105, 109, 111, 116
- Jacobi symbol, 92–93
- Kronecker symbol, 64, 95–99, 100, 157–158, 160
- Lagrange, J. L., 52, 74
 Landau, E., 23, 186
 Lattices:
 integer, 40–43
 in \mathbf{R}^2 , 47
 fundamental parallelogram, 47
 Least common multiple, 11
 Lee Ah Huat, vii
 Legendre, A. M., 17
 Legendre symbol, 64, 70–73, 80, 92, 93. *See also* Quadratic reciprocity
 evaluation, *see also* Congruences, quadratic
 $(-1/p)$, 71, 81
 $(2/p)$, 71–72, 81, 91, 93
 $(5/p)$, 74–75
 L series, 23, 187
- Mestre, J.-F., 188
 Minkowski's theorem, 25, 47–50
 Modular forms, 187
 Modular functions, 185, 186
 Module of binary form, *See* Quadratic forms, binary
 Montgomery, H. L., 187, 188–189
- Negative Pell equation, *see* Pell equation, negative
 Neighbor of binary form, *see* Reduction, binary forms
 Newton's method, *see* Hensel's lemma
 Nonsquare integers, *see* Integers, nonsquare
 Norm in quadratic ring, 34, 111–112, 117, 120
- Order, 112, 117, 122, 183
 square discriminants, 113, 117
 units in, 105, 112–114, 120. *See also* Pell equation
 fundamental unit, 114, 117
- Partial fractions, 16
 Pell equation, 104–117, 119, 124–126, 145
 and automorphisms of forms, 105, 124–126, 142, 145
 negative, 109, 116, 127, 168
 Pell form, 108
 and units in orders, 105, 113–114, 117
 Pell form, *see* Pell equation, Pell form
 Perfect numbers, 11
 Period of quadratic form, *see* Reduction, binary forms
 Pi, 23, 45
 Pigeon-hole principle, 110. *See also* Box principle
 Primality tests, 3, 65, 93–94
 Prime numbers, vii, 1, 2, 93. *See also* Factorization
 in arithmetic progressions, *see* Dirichlet distribution, 1, 3, 17, 19, 21, 204
 generated by polynomial, 6
 infinitely many, 1, 2, 5, 17, 18
 largest known, 5
 representation by quadratic forms, 56, 59, 63, 64, 99–103, 148, 159–160
 size of n th, 21
 sum of reciprocals, 17–19, 22
 Prime number theorem, 17
 Primitive roots, *see* Integers mod m , primitive roots
 Principal class, *see* Class group
 Principal form, *see* Quadratic forms, binary
 Principal genus, *see* Genus group
 Product identities, 33, 52, 102, 106, 112, 148, 154
 Pythagoras, 105
 Pythagorean triples, *see* Diophantine equations, $x^2 + y^2 = z^2$
- Quadratic field, 111, 183, 185, 186
 Quadratic forms, 204. *See also* Diophantine equations; Reduction
 binary, 5, 55. *See also* Class group; Genus group
 ambiguous, 165, 168
 special, 165, 168
 automorphisms, 105, 124
 improper, 125, 126–127, 134
 proper, 105, 125–126, 142, 144–145, 166.
 See also Pell equation

- Quadratic forms (*Continued*)
 discriminant, 55, 60. *See also* Discriminant
 equivalence, 57, 61, 100–102
 proper, 57, 61–62, 102, 105, 128, 147,
 151–153, 181
 gaussian, 152
 integral, 55
 module, 119
 Pell form, *see* Pell equation, Pell form
 positive definite, 55, 61
 primitive, 101, 183
 principal, 152
 representation of integers by, 55, 156. *See*
 also Prime numbers; Diophantine
 equations
 proper, 102, 124, 128, 134
 roots, 139–140, 143
 square discriminants, 61–62, 118–119, 123
 ternary, 168–169
 classically integral, 172
 determinant, 169, 171
 equivalence, 169
 matrix, 169
 $y^2 - xz$, 169, 171, 174–175
 Quadratic nonresidue, 70, 74, 76–77
 Quadratic reciprocity, 63–65, 72–73, 98, 101
 proofs, 64, 76, 78–80, 82–83, 84, 91, 163–164
 supplement, 71, 81. *See also* Congruences,
 quadratic; Legendre symbol, evaluation
 Quadratic residue, 70, 76–77. *See also*
 Congruences, quadratic; Legendre symbol
- Rational approximation, 25, 45–47, 50,
 105–108, 110, 118
 Reduced form, *see* Reduction, binary forms
 Reduction, *see also* Quadratic forms
 binary forms, 169
 negative discriminant, 25, 58–61, 181–183
 reduced form, 59, 168, 183–184
 positive nonsquare discriminant, 61, 105,
 128–132, 141–142
 and automorphisms, 144
 neighbor, 129, 132, 134, 140
 modified, 142
 and Pell equation, 145
 period, 130
 reduced form, 129, 130–131, 139, 142
 positive square discriminant, 61–62
 zero discriminant, 62
 ternary forms, 169–171
 Representations of integers, *see* Diophantine
 equations; Prime numbers; Quadratic
 forms
 Riemann, G. F. B., 17
 Riemann hypothesis (GRH), 186, 189
 Roots of quadratic forms, *see* Quadratic forms,
 binary
- Schur, I., 84, 85
 Siegel, C. L., 186
 Solovay, R., 93–94
 Squarefree integers, *see* Integers, squarefree
 Stark, H. M., 187
 Strassen, V., 93–94
 Sum of squares:
 two, 5, 24, 25, 33, 36–37, 38, 46–47, 49–51,
 59, 63, 76, 95, 102–103, 133–134, 168, 178
 three, 147, 148, 159, 172, 177–178
 four, 52–53, 179
 Symmetric set, 50
- Triangular numbers, 179
- Unique factorization, *see* Factorization,
 uniqueness
 Unique factorization domain, 35, 36
- de la Vallée Poussin, C. J., 17
 Vandermonde matrix, 87, 88
 Visible point, 40
- Weinberger, P. J., 187, 188–189
 Wilson's theorem, 27, 28
 generalized, 31
 Witness, *see* Composite integer, witness
- Zagier, D., 188
 Zeta functions, 186