

Bibliography

- [Cox13] David A. Cox, *Primes of the form $x^2 + ny^2$* , second edition ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013, Fermat, class field theory, and complex multiplication. MR 3236783
- [CS03] John H. Conway and Derek A. Smith, *On quaternions and octonions: their geometry, arithmetic, and symmetry*, A K Peters, Ltd., Natick, MA, 2003. MR 1957212 (2004a:17002)
- [FR15] Sylvia Forman and Agnes M. Rash, *The whole truth about whole numbers*, Springer, Cham, 2015, An elementary introduction to number theory. MR 3309165
- [JJ98] Gareth A. Jones and J. Mary Jones, *Elementary number theory*, Springer Undergraduate Mathematics Series, Springer-Verlag London, Ltd., London, 1998. MR 1610533
- [Mara] Kimball Martin, *Number Theory I course notes (Fall 2009)*, <http://www.math.ou.edu/~kmartin/nti/>.
- [Marb] ———, *Number Theory II course notes (Spring 2010)*, <http://www.math.ou.edu/~kmartin/ntii/>.
- [Rou91] G. Rousseau, *On the quadratic reciprocity law*, J. Austral. Math. Soc. Ser. A **51** (1991), no. 3, 423–425. MR 1125443
- [Ste09] William Stein, *Elementary number theory: primes, congruences, and secrets*, Undergraduate Texts in Mathematics, Springer, New York, 2009, A computational approach. MR 2464052
- [Sti03] John Stillwell, *Elements of number theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2003. MR 1944957

Index

- R^\times , 93
- U , 131
- U^+ , 131
- U_d , 131
- U_d^+ , 131
- \mathbb{C}^\times , 29
- $\text{GCD}(a, b)$, 74
- \mathbb{N} , 18
- \mathbb{Q} , 25
- \mathbb{Q}^\times , 29
- \mathbb{R}^\times , 29
- \mathbb{Z} , 25
- $\mathbb{Z}/n\mathbb{Z}$, 37
- ε_d , 136
- ε_d^+ , 136
- $\text{gcd}(a, b)$, 67
- μ_n , 53
- $\phi(n)$, 93
- $a \mid b$, 16, 64
- $a \nmid b$, 16, 64
- $n\mathbb{Z} + a$, 36
- p -adic integers, 57
- p -adic numbers, 57

- abelian group, 91
- absolute norm, 60
- additive group, 91
- additive inverse, 30
- additive notation, 91
- algebraic integers, 81
- associative, 27

- base b , 19
- binary quadratic form, 119
- binary operation, 27

- Chinese remainder theorem, 112
- closed, 34

- common divisor, 67
- commutative, 27
- complex numbers, 25
- composition law, 106, 120, 127, 131
- congruence class, 36
- congruent, 36
- conjugate, 51, 126
- continued fraction, 140
- converge, 143
- coprime, 68, 79
- coset, 95
- CRT, 112
- cyclic (finite) group, 99
- cyclic subgroup, 98
- cyclotomic field, 55
- cyclotomic ring, 55

- decimal system, 19
- descent, 23
- descent principle, 23
- dihedral group, 92
- Diophantine equation, 86
- Diophantine equations, 5
- Dirichlet's approximation theorem, 133
- divides, 64
- division property, 73
- division ring, 126
- divisor, 64

- Eisenstein integers, 56
- equivalence class, 36
- equivalence classes, 25
- equivalence relation, 25
- equivalent, 36
- Euclidean algorithm, 67
- Euler phi (totient) function, 93
- Euler's criterion, 115
- Euler's theorem, 99

- extended Euclidean algorithm, 70
 Fermat descent, 23
 Fermat's last theorem, 146
 Fermat's little theorem, 98
 Fermat's two square theorem, 108
 Fibonacci numbers, 144
 field, 30
 finite group, 91
 first supplemental law, 114
 floor, 140
 fundamental +unit, 136
 fundamental theorem of algebra, 26
 fundamental theorem of arithmetic, 20, 59
 fundamental unit, 136

 Gauss's three square theorem, 123
 Gaussian integers, 5, 49
 Gaussian numbers, 49
 gcd, 67, 70, 74
 generator, 99
 golden ratio, 144
 greatest common divisor, 67, 74
 greatest integer function, 140
 group, 90

 Hamilton's quaternions, 124
 hexadecimal, 20
 Hurwitz integers, 128

 identity, 28
 imaginary quadratic, 47
 induction axiom, 22
 integers, 25
 inverse, 90
 invertible, 90, 93
 irreducible, 62, 127

 Lagrange's four square theorem, 123
 Lagrange's lemma, 107
 Lagrange's theorem, 97
 law of quadratic reciprocity, 116
 Legendre symbol, 113
 Legendre's three square theorem, 123
 Lipschitz integers, 128

 method of descent, 23

 mod n , 36
 multiplicative group, 91
 multiplicative inverse, 30, 90
 multiplicative notation, 91

 natural numbers, 18
 non-square, 46
 noncommutative ring, 126
 norm, 51, 60, 126

 order, 91, 98

 Peano axioms, 22
 Pell's equation, 130
 period, 142
 periodic (continued fraction), 142
 pigeonhole principle, 133
 prime, 64
 prime divisor property, 64
 prime factorization, 21
 prime-power factorization, 21
 primitive Pythagorean triple, 109
 Pythagorean triple, 109

 quadratic field, 47
 quadratic form, 119
 quadratic integers, 48
 quadratic reciprocity, 116
 quadratic residue symbol, 113
 quadratic ring, 47
 quaternions, 124

 rational numbers, 25
 real quadratic, 47
 reduced form (of a rational), 25
 reducible, 62, 127
 reduction mod m , 87
 relatively prime, 68, 79
 repeated squaring, 99
 ring, 30
 ring of integers, 82
 roots of unity, 53
 RSA, 102

 second supplementary law, 121
 skew field, 126
 square, 46, 88

squarefree, 81
subfield, 34
subgroup, 95
subring, 34
symmetric group, 92

tableau method, 70
trivial (sub)group, 96
trivial solution, 132, 146

unary, 20
unique factorization, 59, 64
unit, 61, 127

whole numbers, 19
Wilson's theorem, 107

zero ring, 33