
Index

- abelian, 2
- AKS algorithm, 137
- arithmetic function, 81
- associates, 10

- Bertrand's postulate, 32
- binary operation, 1
- binomial coefficients, 33
- birthday problem, 114

- Carmichael numbers, 141
- Cauchy–Schwarz inequality, 119
- characteristic of a field, 83, 92
- characteristic zero, 92
- Chinese Remainder Theorem, 99
- comaximal ideals, 102
- common divisor, 13
- completely multiplicative function, 81
- composite number, 41
- congruence class, 46
- congruences, 5
- coprime, 49
- coset, 87
- cyclic group, 3, 49, 83

- De Bruijn sequence, 126
- degree of a polynomial, 7
- design, 115
- Diffie–Hellman key exchange, 140
- direct product of groups, 94
- direct product of rings, 100

- Dirichlet convolution, 81
- discrete logarithm problem, 139
- divisibility, 9
- division algorithm, 17

- equivalence class, 46
- equivalence relation, 46
- Euclidean algorithm, 21
- Euclidean domain, 17
- Euler's theorem, 89
- Euler's totient function, 49

- factoring, 138
- Fano plane, 115
- Fermat's little theorem, 89
- field, 1, 8
- field of fractions, 9
- finite characteristic, 92
- finite projective plane, 115
- Fundamental Theorem of Algebra, 65
- Fundamental Theorem of Arithmetic, 27

- Gaussian integers, 1
- generator of a group, 86
- greatest common divisor, 13
- group, 1

- harmonic sum, 30

- ideal, 12

- integral domain, 6, 7
- irreducible, 11
- isomorphism, 83
- isomorphism of fields, 90
- isomorphism of groups, 84
- isomorphism of rings, 90

- Lagrange's theorem, 87

- maximal ideal, 53
- mean, 118
- minimal polynomial, 125
- moments, 118
- monic polynomial, 65
- multiplicative function, 75
- Möbius function, 75
- Möbius inversion formula, 74

- Noetherian ring, 17
- normal subgroup, 88

- order of an element, 86

- partition into equivalence classes, 47
- perfect difference set, 114
- polynomial ring, 5
- polynomial time algorithm, 136
- polynomials, 1
- primality testing, 140
- prime, 11
- prime ideal, 52
- prime number theorem, 40
- primitive polynomial, 161
- principal ideal, 12
- principal ideal domain (PID), 12
- pseudoprime, 140
- public key cryptosystem, 138

- quotient ring, 45

- rapid algorithm, 136
- rational functions, 9
- reduced residue class, 49
- repeated squaring, 139
- residue class, 48
- Riemann hypothesis, 40
- ring, 1, 4
- root of a polynomial, 64

- Sidon set, 111

- square-free number, 75
- strong pseudoprime, 141
- subfield, 92

- unique factorization domain (UFD), 15
- units, 8

- variance, 118
- vector space, 83, 93

- Wilson's theorem, 50

- zero divisor, 6
- zero ring, 4