

Name index

- Abel, 170, 181, 257
 Adleman, 70
 d'Alembert, 101
 Alexander the Great, 14
- Babbage, 117ff
 Bachet, 36, 45, 74
 Bernoulli, D., 101
 Bernoulli, J., 101
 Boole, 85, 136, 185, 195
 Brahmagupta, 45, 50, 180
 Bravais, 183
- Cantor, 85, 97ff
 Cardano, 181
 Carroll, *see* Dodgson,
 Cauchy, 148, 158, 164, 182, 216
 Cayley, 174, 182, 195
- Dedekind, 189
 De Morgan, 115, 136, 194
 Descartes, 36, 84
 Diffie, 70
 Diophantus, 33, 36, 74
 Dirichlet, 101
 Dodgson, 80
 Dyck, 182
- Eratosthenes, 26
 Euclid, 9, 14, 15, 22, 23, 29, 32ff
 Euler, 33ff, 40, 65ff, 74, 80, 101
- Faltings, 33, 74
 Fermat, 23, 33ff, 36, 63, 65, 73ff,
 Ferarri, 181
 del Ferro, 181
- Fourier, 101
 Frénicle, 34, 63, 73
- Galois, 157, 181ff, 189, 257
 Gauss, 36, 40, 194
 Gibbs, 195
 Gödel, 140
 Goldbach, 34, 74
 Grassmann, 195
 Gregory, 194
 Greiss, 229
- Hamilton, 172, 194ff
 Hasse, 111
 Hellman, 70
 Hensel, 189
 Hollerith, 118
- Janko, 229
 Jordan, 182, 216
- al-Khwarizmi, 180
 Kilburn, 118
 Klein, 183
 Kronecker, 182, 189
- Lagrange, 158, 182, 216
 Leibniz, 65, 80, 101, 117, 136
 Liouville, 182
- Mathieu, 228
 Mersenne, 34, 73
- Newton, 101, 136
 Pascal, 23, 117

Cambridge University Press

978-0-521-54050-6 - Numbers, Groups and Codes: Second Edition

J. F. Humphreys and M. Y. Prest

Index

[More information](#)

332

Name index

- | | |
|-------------------------|-----------------|
| Peacock, 194 | Taylor, B., 101 |
| Peirce, B., 185, 195 | Taylor, R., 74 |
| Peirce, C. S., 115, 195 | Turing, 118 |
| Philolaus, 28 | |
| Ptolemy, 14 | Venn, 80 |
| | Viète, 33 |
| Qín Jiǔsháo, 54 | |
| | Wallis, 23 |
| Rabin, 70 | Weber, 182, 189 |
| Ruffini, 181ff | Wiles, 33, 74 |
| Rivest, 70 | Williams, 118 |
| | |
| Serret, 182 | Xylander, 74 |
| Shamir, 70 | |
| Steinitz, 189 | Yi Xing, 54 |
| | |
| Tartaglia, 181 | Zermelo, 85 |

Subject index

Boldface indicates a page on which a term is defined.

- Abelian, *see* group, abelian
 abstract algebra, rise of, 193ff
 accept(ed), **120**
 addition modulo f , **280**
 addition modulo n , **40**
 adjacency matrix, **108**
 algebra, **192**
 of sets, **83ff**
 algebraically closed, **293**
Al-jabr wa'l muqābala, 180
 alphabet (of finite state machine), **119**
 Argand diagram, **293**
 argument (of complex number), **293**
Arithmetica, 33, 36, 74
 arithmetic modulo n , **40**
Ars Magna, 181
 automaton, **120**
 axiom, **184**
- base case, **16**, 21
 base (of public key code), **71**
 bijection, 68, **90**, 96ff, 167, 215, 219
 see also permutation
 binomial coefficient, **19**
 Binomial Theorem, **18**, 65, 75
 boolean algebra 136, 185, **192ff**, 198ff
 of sets, **84**, 135ff, 193, 199
 boolean combination, **130**
 boolean ring, **199**
- calculating machines, 117ff
 cardinality, **98**
 Cartesian product, *see* product
 casting out nines, **49**
- characteristic, **197**
 check digit, 231ff
 Chinese Remainder Theorem, **54**, 67
 code, error-correcting and error-detecting,
 230ff
 cyclic, **284ff**
 Golay, 252
 group, *see* code, linear
 Hamming, **249**
 linear, **237ff**, 284ff
 perfect, **249**
 quadratic residue, 290
 see also public key codes
 codeword, **232**, 245, 284ff
 coding function, 232ff
 codomain, **87**
 coefficient, of polynomial, **256**, 261,
 287
 common measure, 32
 complement, **80**, **192**
 double, **193**
 properties of, 83, **193**
 relative, **80**
 Completeness Theorem, 140
 complex numbers, set of (\mathbb{C}), 172, 174, 176,
 189, 192, 193ff, 221, 258, 261, 276,
 292ff
 composite, **28**
 composition (of functions), **93ff**, 149ff
 congruence, **38**, 45, 161, 205, 213
 linear, **49ff**
 non-linear, 57ff
 simultaneous linear, 54ff
 solving linear, 50

- congruence class, 36, **38**, 50, 115, 196, **279**, 286
 invertible, **43**, 44ff, 52
 order of, **61ff**
 set of invertible (G_n), **47**, 63ff, 172, 212, 220, 223
- congruent (integers), **36**
 congruent (polynomials), **279**
 conjecture, **34**
 conjugate, **164**, 166, 212, 230
 conjugate, complex, **293ff**
 conjunction, **129**
 consistency, **134**
 contradiction, **134**
 contrapositive, **132**, 142
 converse, **132**
 coprime, *see* prime, relatively
 corollary, **8**
 coset decoding table, **241ff**
 with syndromes, **246**
 coset leader, **244**
 coset (left, right), **212ff**, 228
 counterexample, **35**, **143**
Cours d'Algèbre supérieure, 182
 covering, **113**
 cut, **159**, 169
 cycle, *see* permutation, cyclic
 cycle decomposition (of permutation), 154, **155**, 163
 cyclic group, *see* group, cyclic
 cyclic permutation, *see* permutation, cyclic
- decoding table, *see* coset decoding table
 deduction, rules of, 140
 degree (of polynomial), **256**, 262, 264, 279
 De Morgan laws, *see* law, De Morgan
 Difference Engine, 117ff
 digit sum, (iterated), **49**
 digraph, *see* directed graph
 directed graph (of a relation), **107**
 direct product, *see* product
 disjoint permutations, **153**, 163
 disjoint sets, **81**, 98, 113, 214
 disjunction, **129**
Disquisitiones Arithmeticae, 36, 40
 distance, **234**, 236, 237, 249
 divide, **3**, 36, 46, 218, **262**, 265
 division algorithm, *see* Euclidean algorithm
 Division Theorem, **3**, **264**
 domain, **87**
 element, **78**
Elements (Euclid's), 9, 14, 15, 22, 26, 29, 32
 equivalence class, **114**
 equivalence relation, *see* relation, equivalence
 equivalent (propositions), *see* logical equivalence
 Erlanger programme, 183
 error-correction, 231ff, 236, 240ff
 error-detection, 230ff, 236
 Euclidean algorithm, **9ff**, **269ff**
 Euler phi-function ($\phi(n)$), **66ff**, 98, 172
 Euler's Theorem, **68**, 72, 143, 144, 218
 evaluate (polynomial), **257**
 existential quantifier, **138**
 exponent (of public key code), **71**
- factorial ($n!$), **18**
 Fermat's Theorem, **63**, 76, 143, 144, 217
 Fermat's 'Theorem', 33, **73ff**, 127
 Fibonacci sequence, **23**
 field, **189ff**, 194, 282, 283
 of fractions, 198
 finite state machine, **119ff**, 186ff
 fix, **153**
 fractions, *see* rational numbers
 function, **87ff**, 103, 185ff
 bijjective, *see* bijection
 characteristic, **103**
 concept of, 86ff, 100ff
 constant, **92**
 identity, **92**
 injective, *see* injection
 one-to-one, *see* injection
 onto, *see* surjection
 surjective, *it see* surjection
 Fundamental Theorem of Algebra, 189, 258, **276**, 293
 Fundamental Theorem of Arithmetic, *see* Unique Factorisation Theorem
- Galois field, 282
 gcd, *see* greatest common divisor
 generated, **209ff**, **286**
 generator matrix, **237**, 287
 generator polynomial, **286**
 generators, of group, **209**
 Goldbach's conjecture, **34ff**
 graph, of function, **89**
 directed, *see* directed graph
 greatest common divisor, **7**, **12**, 31, 32, 43, 50, **268ff**

- group, **170ff**, 184, 185, 200ff, 257
 Abelian (=commutative), **170**, 173, 182,
 209, 224, 225, 259
 alternating, 167, **174**, 208, 216, 218, 228
 concept of, xi, 147, 180ff, 200
 cyclic (C_n), **209**, 212, 216, 217, 220ff, 224
 dihedral (D_n), 178, **179**, 211, 221, 228
 general linear, **175**, 206, 208, 210, 211
 Klein four, **224**, 226
 Mathieu, 228, 252
 of matrices, 175ff
 Monster, 229
 of numbers, 171ff
 p -, **218**
 of permutation, *see* group, symmetric
 simple, **228ff**
 of small order, 224ff
 special linear, **208**
 sporadic simple, 228ff
 symmetric, **149**, 174, 209, 211, 213, 216,
 220ff, 223
 of symmetries, 177ff
- Hasse diagram, **111**
 hcf, *see* highest common factor
 highest common factor, *see* greatest common
 divisor
- idempotent, **185**, 196
 identity, logical, *see* logical identity
 identity element, **170**
 image, **87**
 imaginary part, **292**
 immediate predecessor, **111**
 immediate successor, **111**
 implication, **132**
 induction
 course of values, *see* induction, strong
 definition by, **18**
 hypothesis, **16**
 principle, **16**, 20, 23, 24
 proof by, **16ff**, 22ff, 143
 step, **16**, 21
 strong, **21**, 28
 inductive construction, **15**
 infinite order, *see* order, infinite
 injection, **90**, 186
 integers, set of (\mathbb{Z}), **1**, 171, 185, 188, 210, 213
 integers modulo n , set of (\mathbb{Z}_n), **38**, 171, 189,
 210, 213, 220, 261, 272, 278, 281ff,
 283ff
- integral domain, **192**, 194, 196
 integral linear combination, 7, 44
 intersection, **80**, 209
 inverse, **43ff**, **170**, **282**
 of function, **95**, 96, 220
 of polynomial congruence class, **282**
 invertible congruence class, **43**, 44ff, 52
 invertible matrix, **175**
 irrational numbers, 32, 101, 190
 irreducible (polynomial), **273ff**, 282
 ISBN code, **231**
 isomorphism, **219ff**
- Jiǔ zhāng suàn shù*, *see* *Nine Chapters on the
 Mathematical Art*
- join, **192**
- knapsack codes, 70
- Lagrange's Theorem, 66, 143, 144, **216**, 218,
 225, 226, 231
- law,
 absorption, **83**, **134**
 associative, **83**, 94, **134**, **170**, **188**,
193
 commutative, **83**, **134**, **170**, **188**
 contrapositive, **134**
 De Morgan, **83**, **134**, **193**
 distributive, **83**, **134**, **188**, **193**, 260
 double negative, **134**
 excluded middle, **134**
 idempotence, **83**, **134**, **193**
 index, 159, 204
Laws of Thought, 185
- lcm, *see* least common multiple
 leading coefficient, **256**
 leading term, **256**
 least common multiple, **14**, 31, 162
 lemma, **8**
 length
 of code, **284**
 of permutation, **152**, 161
 of word, **232**
- Linear Associative Algebras*, 185
 logical equivalence, **133**, 136, 193
 logical identity, **133**
- map (mapping), *see* function
Master Sun's Arithmetical Manual, 1
Mathematical Treatise in Nine Sections,
 54, 56

- matrix,
 diagonal, **176**, 208
 groups and rings of, 175ff, 188, 192, 195,
 206, 208
 invertible, **175**
 method (for gcd), **10ff**
 upper triangular, **175ff**
 maximum likelihood decoding, **241**
 meet, **192**
 member, *see* element
Methodus Incrementorum, 101
 mod(ulo), *see* congruent
 modulus (of complex number), **293**
 move, **153**
 Multinomial Theorem, 75
 multiplication modulo f , **280**
 multiplication modulo n , **40**
- natural numbers, set of (\mathbb{N}), **2**
 negation (of proposition), **129**
Nine Chapters on the Mathematical Art, 9
 non-commutative, **151**
 notation, mathematical, 32ff, 181, 194
- order
 of congruence class, **61**, 65, 69
 of element, **205**, 209, 216ff
 finite multiplicative, **60**
 of group, **216ff**, 218, 222
 infinite, **205**
 of permutation, **161ff**, 206
 order (=ordering), *see* partial order
- parity-check digit, **233**
 parity-check matrix, **245**
 parity polynomial, **287**
 partially ordered set, **110**
 partial order(ing), **109**
 strict, **110**
 partition, **113**, 214
 Pascal's triangle, 19, 20
 permutation, **90**, **148ff**, 252, 285ff
 commuting, 153
 cyclic, **152**
 even, **165**
 odd, **165**
see also bijection
 permutation representation, **175**, 178, 179
 permutations, group of, *see* group, symmetric
 polygon, regular, group of symmetries of, 179
 polynomial, **255ff**
 congruence class, *see* congruence class,
 constant, **256**
 cubic, **256**
 linear, **256**, 276
 quadratic, **256**, 276
 quartic, **256**
 quintic, **256**
 polynomial equations, solution of, 58, 181ff,
 189, 257
 complex solutions, 181ff
 cubic, 181, 257
 negative solutions of, 180ff
 quadratic, 180ff, 257
 quartic, 181, 257
 quintic, 181ff, 257
 solution 'in radicals', **181**
 polynomial function, **255**
 polynomials,
 addition of, 191, **258ff**
 algebra of, **191ff**, **258ff**
 division of, **262ff**
 factorising, **265ff**, 274ff
 multiplication of, 191, **258ff**
 set of, 191, 258, 260, 281
 subtraction of, **260ff**
 poset, *see* partially ordered set
 positive integers, set of (\mathbb{P}), **1**
 power
 of element, **18**, 59, **204**, 209
 of permutation, **159ff**
 primality, **26**
 prime, **25ff**, 29, 33ff, 47, 63ff, 71ff, 189, 192,
 217, 218, 228, 273ff
 Fermat, **34**, 76
 Mersenne, **34**, 76
 relatively, **12**, 43ff, 54, 60, 67, 68, 224
 primes, infinitely many, 29
 primitive polynomial class, **282**
Problèmes plaisants et délectables, 45
 product
 of congruence classes, **40**, **280**
 of groups, **222ff**
 of sets, 68, **84**
 proof by contradiction, **5**, 142
 proof, methods of, 141ff
 proof, notion of, xivff, 23, 33, 127ff
 proofs, reading, xvff, 4ff, 8ff
 proposition, **8**, **128ff**, 137
 propositional calculus, 128ff

- propositional term (in), *see* term (in)
 public key codes, 70ff
 Pythagoras' Theorem, 36
- quantifiers, **138**
- quaternions, set of (\mathbb{H}), **172**, 176, 194ff, 198, 228
- quotient, **3**, 263
- quotient field, *see* field of fractions
- rational numbers, set of (\mathbb{Q}), **2**, 172, 189, 198
- real numbers, set of (\mathbb{R}), 172, 189, 191, 221
- real part, **292**
- rectangle, symmetries of, 180, 221, 229
- recursion, definition by, **18**
- refine, **117**
- reflection, **177ff**
- relation, **103ff**
- antisymmetric, **106**
 - complementary, **105**
 - equivalence, **112ff**, 214
 - reflexive, **105**
 - reverse, **105**
 - symmetric, **105**
 - transitive, **106**
 - weakly antisymmetric, **106**
- remainder, **3**, 263
- representative
- of class, **39**, **279**
 - of coset, **213**
- ring, **187**
- root (of polynomial), *see* zero, of polynomial
- rotation, **177ff**
- RSA Labs (website), 72
- RSA (public key codes), 70ff
- scalar, **191**
- multiplication, **191**
- semigroup, **185ff**
- series (infinite), 101
- set, **78**
- cardinality of, **98ff**
 - empty, **79**
 - universal, **80**
- shape (of permutation), **164**
- shuffle, **159**, 169
- Shù shū jiǔ zhāng*, *see* *Mathematical Treatise in Nine Sections*
- sieve of Eratosthenes, **26**, 35
- sign (of permutation), **165ff**
- square, symmetries of, 179
- standard representative, **39**, **279**
- state (of finite state machine), **119**
- acceptance, **120**
 - initial, **119**
- state diagram, **120**
- subgroup, **206ff**, 212ff, 218
- identity, *see* subgroup, trivial
 - normal, **228**
 - proper, **208**
 - trivial, **208**
- subset, **79**
- proper, **79**
- substitutions, group of, 182
- summation notation, **256**
- sum of congruence classes, **40**, **280**
- Sūn tǐ suàn jīng*, *see* *Master Sun's Arithmetical Manual*
- surjection, **90**, 186
- switch, **156**
- Sylow's Theorems, 218
- symmetric difference, **86**, **196**
- symmetry, **177**
- syndrome, **245**
- tables
- addition and multiplication, 43, 48, 157, 185, 187
 - group, **172ff**, 184, 219, 223, 225ff, 229
- tautology, **133**
- term (in), **130**
- term (of polynomial), **256**
- Tractatus de Numerorum Doctrina*, 40, 66
- Traité des substitutions et des équations algébriques*, 182
- transition function, **119**
- transposition, **152**, 166, 167, 211
- Triangle Arithmétique*, 23
- triangle, symmetries of, 177ff, 221
- truth table, **129ff**, 140
- truth value, **128**
- Turing machine, 118ff, 124
- union, **81**
- Unique Factorisation Theorem, **28**, **274**
- unit, *see* identity element
- universal quantifier, **138**
- vector, **191**, 195, 214

Cambridge University Press

978-0-521-54050-6 - Numbers, Groups and Codes: Second Edition

J. F. Humphreys and M. Y. Prest

Index

[More information](#)

338

Subject index

vector space, **191**Venn diagram, **79**weight, **234**, 237well-ordering principle, **2**, 20, 22, 24word, **232**

zero

concept of, 22

congruence class, **38**of polynomial, 58, **257**, 265, 276,
293zero-divisor, **43**, 46, **188**, 192