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
Diffee, 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
<table>
<thead>
<tr>
<th>Name</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peacock, 194</td>
<td></td>
</tr>
<tr>
<td>Peirce, B., 185, 195</td>
<td></td>
</tr>
<tr>
<td>Peirce, C. S., 115, 195</td>
<td></td>
</tr>
<tr>
<td>Philolaus, 28</td>
<td></td>
</tr>
<tr>
<td>Ptolemy, 14</td>
<td></td>
</tr>
<tr>
<td>Qin Jiushao, 54</td>
<td></td>
</tr>
<tr>
<td>Rabin, 70</td>
<td></td>
</tr>
<tr>
<td>Ruffini, 181ff</td>
<td></td>
</tr>
<tr>
<td>Rivest, 70</td>
<td></td>
</tr>
<tr>
<td>Serret, 182</td>
<td></td>
</tr>
<tr>
<td>Shamir, 70</td>
<td></td>
</tr>
<tr>
<td>Steinitz, 189</td>
<td></td>
</tr>
<tr>
<td>Tartaglia, 181</td>
<td></td>
</tr>
<tr>
<td>Taylor, B., 101</td>
<td></td>
</tr>
<tr>
<td>Taylor, R., 74</td>
<td></td>
</tr>
<tr>
<td>Turing, 118</td>
<td></td>
</tr>
<tr>
<td>Venn, 80</td>
<td></td>
</tr>
<tr>
<td>Viete, 33</td>
<td></td>
</tr>
<tr>
<td>Wallis, 23</td>
<td></td>
</tr>
<tr>
<td>Weber, 182, 189</td>
<td></td>
</tr>
<tr>
<td>Wiles, 33, 74</td>
<td></td>
</tr>
<tr>
<td>Williams, 118</td>
<td></td>
</tr>
<tr>
<td>Xylander, 74</td>
<td></td>
</tr>
<tr>
<td>Yi Xing, 54</td>
<td></td>
</tr>
<tr>
<td>Zermelo, 85</td>
<td></td>
</tr>
</tbody>
</table>
Subject index

Boldface indicates a page on which a term is defined.

Abelian, see group, abelian
abstract algebra, rise of, 193ff
accepted, 120
addition modulo $f$, 280
addition modulo $n$, 40
adjacency matrix, 108
algebra, 192
of sets, 83ff
algebraically closed, 293
Al-jabr wa’l muq¯abalah, 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
dependencies, 83, 193
properties, 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
correspondence (of functions), 149ff
correspondence (of sets), 84, 135ff, 193, 199
congruence, 38, 45, 161, 205, 213
linear, 49ff
non-linear, 57ff
non-linear, 57ff
simultaneous linear, 54ff
solving linear, 50
<table>
<thead>
<tr>
<th>Subject index</th>
</tr>
</thead>
<tbody>
<tr>
<td>congruence class, 36, 38, 50, 115, 196, 279, 286</td>
</tr>
<tr>
<td>invertible, 43, 44ff, 52</td>
</tr>
<tr>
<td>order of, 61ff</td>
</tr>
<tr>
<td>set of invertible $\left(G_{n}\right)$, 47, 63ff, 172, 212, 220, 223</td>
</tr>
<tr>
<td>congruent (integers), 36</td>
</tr>
<tr>
<td>congruent (polynomials), 279</td>
</tr>
<tr>
<td>conjecture, 34</td>
</tr>
<tr>
<td>conjugate, 164, 166, 212, 230</td>
</tr>
<tr>
<td>conjugate, complex, 293ff</td>
</tr>
<tr>
<td>conjunction, 129</td>
</tr>
<tr>
<td>consistency, 134</td>
</tr>
<tr>
<td>contradiction, 134</td>
</tr>
<tr>
<td>contrapositive, 132, 142</td>
</tr>
<tr>
<td>converse, 132</td>
</tr>
<tr>
<td>coprime, see prime, relatively</td>
</tr>
<tr>
<td>corollary, 8</td>
</tr>
<tr>
<td>coset decoding table, 241ff</td>
</tr>
<tr>
<td>with syndromes, 246</td>
</tr>
<tr>
<td>coset leader, 244</td>
</tr>
<tr>
<td>coset (left, right), 212ff, 228</td>
</tr>
<tr>
<td>counterexample, 35, 143</td>
</tr>
<tr>
<td>Cours d’Algèbre supérieure, 182</td>
</tr>
<tr>
<td>covering, 113</td>
</tr>
<tr>
<td>cut, 159, 169</td>
</tr>
<tr>
<td>cycle, see permutation, cyclic</td>
</tr>
<tr>
<td>cycle decomposition (of permutation), 154, 155, 163</td>
</tr>
<tr>
<td>cyclic group, see group, cyclic</td>
</tr>
<tr>
<td>cyclic permutation, see permutation, cyclic</td>
</tr>
<tr>
<td>decoding table, see coset decoding table</td>
</tr>
<tr>
<td>deduction, rules of, 140</td>
</tr>
<tr>
<td>degree (of polynomial), 256, 262, 264, 279</td>
</tr>
<tr>
<td>De Morgan laws, see law, De Morgan</td>
</tr>
<tr>
<td>Difference Engine, 117ff</td>
</tr>
<tr>
<td>digit sum, (iterated), 49</td>
</tr>
<tr>
<td>digraph, see directed graph</td>
</tr>
<tr>
<td>directed graph (of a relation), 107</td>
</tr>
<tr>
<td>direct product, see product</td>
</tr>
<tr>
<td>disjoint permutations, 153, 163</td>
</tr>
<tr>
<td>disjoint sets, 81, 98, 113, 214</td>
</tr>
<tr>
<td>disjunction, 129</td>
</tr>
<tr>
<td>Disquisitiones Arithmeticae, 36, 40</td>
</tr>
<tr>
<td>distance, 234, 236, 237, 249</td>
</tr>
<tr>
<td>divide, 3, 36, 46, 218, 262, 265</td>
</tr>
<tr>
<td>division algorithm, see Euclidean algorithm</td>
</tr>
<tr>
<td>Division Theorem, 3, 264</td>
</tr>
<tr>
<td>domain, 87</td>
</tr>
<tr>
<td>element, 78</td>
</tr>
<tr>
<td>Elements (Euclid’s), 9, 14, 15, 22, 26, 29, 32</td>
</tr>
<tr>
<td>equivalence class, 114</td>
</tr>
<tr>
<td>equivalence relation, see relation, equivalence</td>
</tr>
<tr>
<td>equivalent (propositions), see logical</td>
</tr>
<tr>
<td>equivalence</td>
</tr>
<tr>
<td>Erlanger programme, 183</td>
</tr>
<tr>
<td>error-correction, 231ff, 236, 240ff</td>
</tr>
<tr>
<td>error-detection, 230ff, 236</td>
</tr>
<tr>
<td>Euclidean algorithm, 91ff, 269ff</td>
</tr>
<tr>
<td>Euler phi-function $\phi(n)$, 66ff, 98, 172</td>
</tr>
<tr>
<td>Euler’s Theorem, 68, 72, 143, 144, 218</td>
</tr>
<tr>
<td>evaluate (polynomial), 257</td>
</tr>
<tr>
<td>existential quantifier, 138</td>
</tr>
<tr>
<td>exponent (of public key code), 71</td>
</tr>
<tr>
<td>factorial ($n!$), 18</td>
</tr>
<tr>
<td>Fermat’s Theorem, 63, 76, 143, 144, 217</td>
</tr>
<tr>
<td>Fermat’s “Theorem”, 33, 73ff, 127</td>
</tr>
<tr>
<td>Fibonacci sequence, 23</td>
</tr>
<tr>
<td>field, 189ff, 194, 282, 283</td>
</tr>
<tr>
<td>of fractions, 198</td>
</tr>
<tr>
<td>finite state machine, 119ff, 186ff</td>
</tr>
<tr>
<td>fix, 153</td>
</tr>
<tr>
<td>fractions, see rational numbers</td>
</tr>
<tr>
<td>function, 87ff, 103, 185ff</td>
</tr>
<tr>
<td>bijective, see bijection</td>
</tr>
<tr>
<td>characteristic, 103</td>
</tr>
<tr>
<td>concept of, 86ff, 100ff</td>
</tr>
<tr>
<td>constant, 92</td>
</tr>
<tr>
<td>identity, 92</td>
</tr>
<tr>
<td>injective, see injection</td>
</tr>
<tr>
<td>one-to-one, see injection</td>
</tr>
<tr>
<td>onto, see surjection</td>
</tr>
<tr>
<td>surjective, it see surjection</td>
</tr>
<tr>
<td>Fundamental Theorem of Algebra, 189, 258, 276, 293</td>
</tr>
<tr>
<td>Fundamental Theorem of Arithmetic, see</td>
</tr>
<tr>
<td>Unique Factorisation Theorem</td>
</tr>
<tr>
<td>Galois field, 282</td>
</tr>
<tr>
<td>gcd, see greatest common divisor</td>
</tr>
<tr>
<td>generated, 209ff, 286</td>
</tr>
<tr>
<td>generator matrix, 237, 287</td>
</tr>
<tr>
<td>generator polynomial, 286</td>
</tr>
<tr>
<td>generators, of group, 209</td>
</tr>
<tr>
<td>Goldbach’s conjecture, 34ff</td>
</tr>
<tr>
<td>graph, of function, 89</td>
</tr>
<tr>
<td>directed, see directed graph</td>
</tr>
<tr>
<td>greatest common divisor, 7, 12, 31, 32, 43, 50, 268ff</td>
</tr>
</tbody>
</table>
Subject index

group, 170ff, 184, 185, 200ff, 257
Abelian (=commutative), 170, 173, 182, 209, 224, 225, 259
alternating, 167, 174, 208, 216, 218, 228
cyclic (G_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 (Z), 1, 171, 185, 188, 210, 213
integers modulo n, set of (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

Huí zhēng sì 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
Subject index

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 ordering, 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, 141ff
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 (ℍ), 172, 176, 194ff, 198, 228

quotient, 3, 263

quotient field, see field of fractions

rational numbers, set of (ℚ), 2, 172, 189, 198

real numbers, set of (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 shì jì chāng, 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 suān 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
Subject index

vector space, 191
Venn diagram, 79

weight, 234, 237
well-ordering principle, 2, 20, 22, 24
word, 232

zero
concept of, 22
congruence class, 38
of polynomial, 58, 257, 265, 276, 293
zero-divisor, 43, 46, 188, 192