

- Poincaré, H. (1882). Théorie des groupes fuchsiens. *Acta Mathematica*, **1**, 1–62. An English translation of the relevant part is in Stillwell (1996), 123–129.
- Poincaré, H. (1883). Mémoire sur les groupes kleinéens. *Acta Mathematica*, **3**, 49–92. An English translation of the relevant part is in Stillwell (1996), 131–137.
- Rousseau, G. (1991). On the quadratic reciprocity law. *Journal of the Australian Mathematical Society*, **51**, 423–425.
- Samuel, P. (1970). *Algebraic Theory of Numbers*. Hermann.
- Scharlau, W., and Opolka, H. (1985). *From Fermat to Minkowski: Lectures on the Theory of Numbers and Its Historical Development*. Springer-Verlag.
- Shallit, J. (1994). Origins of the analysis of the Euclidean algorithm. *Historia Mathematica*, **21**, 401–419.
- Sigler, L. E. (1987). *Leonardo Pisano Fibonacci. The Book of Squares*. Academic Press. English translation of Fibonacci's *Liber quadratorum*.
- Stark, H. M. (1978). *An Introduction to Number Theory*. MIT Press.
- Stillwell, J. C. (1992). *Geometry of Surfaces*. Springer-Verlag.
- Stillwell, J. C. (1994). *Elements of Algebra*. Springer-Verlag.
- Stillwell, J. C. (1996). *Sources of Hyperbolic Geometry*. American Mathematical Society.
- Taylor, A. E. (1972). *Plato. Philebus and Epinomis*. Thomas Nelson and Sons Ltd.
- Vajda, A. (1989). *Fibonacci & Lucas Numbers and the Golden Section*. Halsted Press.
- Viète, F. (1579). *Universaliū inspectionium ad canonem mathematicum liber singularis*.
- von Neumann, J. (1923). Zur Einführung der transfiniten Zahlen. *Acta litterarum ac scientiarum Regiae Universitas Hungaricae Francisco-Josephine, Sectio scientiarum mathematicarum*, pages 199–208. English translation in *From Frege to Gödel* (Ed. J. van Heijenoort), Harvard University Press, 1967, 347–354.

- Wallis, J. (1655). *Arithmetica infinitorum*. In his *Opera*, volume 1, 355–478.
- Weil, A. (1984). *Number Theory. An Approach through History*. Birkhäuser.
- Young, R. M. (1992). *Excursions in Calculus*. Mathematical Association of America.

Index

A

abelian group, 210
additive notation, 210
identity element, 210
inverse, 210
multiplicative notation, 210
properties, 210
absolute value, 217
is multiplicative, 217
addition
mod 12, 177
of points
on hyperbola, 297
addition formula, 152
for cis, 154
for cosh, 297
for cosine, 152
for exponential function, 292
and Pythagorean triples, 157
rational, 157
for sine, 152

for sinh, 297
for tan, 157
and complex numbers, 220
additive function, 165
and axiom of choice, 174
and basis over \mathbb{Q} , 166
on finite set, 165
additive inverse, 10
property, 10
uniqueness, 10
additive property of log, 287
al-Haytham, 209
al-Khazin, 217
Alberti's veil, 276
algebraic
curve, 150, 282
factorization, 6
function, 150, 281, 282
number
ideal, 209

- analytic geometry, 38
in Descartes, 38, 54
in Fermat, 54
in Hilbert, 38
- angle
alternate, 88
at the circumference, 48
and half angle formulas, 156
is constant, 49
- bisection of, 41
- dihedral, 159
of tetrahedron, 160
- measure, 143
and completeness of \mathbb{R} , 145
via arc length, 144
- non-Euclidean, 101
- preserved by similarities, 109
- replication, 42
- as a set of reals, 149
- sum, 147, 149
of n -gon, 47
of quadrilateral, 45
of triangle, 45
- vertically opposite, 44, 88
- antilogarithms, 305
- Apollonius
Conics, 254
focal property of ellipse, 254
- arc length
and angle measure, 144
of circle
related to area, 283
- and completeness of \mathbb{R} , 145
as least upper bound, 144
- Archimedes
approximation to π , 146, 171
areas and volumes, 65
axiom, 84
- found $1^2 + 2^2 + \dots + n^2$, 286
found area of parabola, 286
and burning mirrors, 254
- area
bounded by curve, 284
of circle
proportional to R^2 , 285
related to arc length, 283
- by cutting and pasting, 52
- under hyperbola, 287
defines logarithm, 287
- of hyperbolic sector, 295, 297
- integer
of rational right triangle, 142
- invariance
proved by Hilbert, 61
as least upper bound, 284
- of lune, 285
- measure, 51
- of polygon, 52
- of rational right triangles, 131
- of rectangle, 51
- of triangle, 52, 60
- Aristotle, 64
- arithmetic
equivalence, 180
of even and odd, 178
of lengths and areas, 51
 $\text{mod } n$, 179
 $\text{mod } 9$
and casting out nines, 181
- Arithmetica*, 117
conspicuous omissions, 138
- Artmann, 67
- Āryabhāṭa, 31
- ascent, 24
- base step, 24

induction step, 24
with trivial induction step, 34
associative law, 10
for $+$, 10
Grassmann proof, 29
for \times , 11
asymptotes, 258
axiom
Archimedean, 84
of choice, 174, 175
of circle construction, 40
of congruence, 48
of infinity, 28
of line construction, 40
via equations, 72
parallel, 44
of Euclid, 44
fails in non-Euclidean
plane, 100
of Playfair, 44
via equations, 72
“whole is greater than part”,
61

B

Bachet's Diophantus, 138
base step, 24
basis over \mathbb{Q} , 165
and additive function, 166
construction, 166
for \mathbb{R} , 175
Beltrami, 241
Bhāskara I, 31
Bhāskara II, 39
binomial theorem
mod p , 189
ordinary, 189
Bombelli, 222

Brahmagupta
cyclic quadrilateral formula,
123
described rational triangles,
120
identity, 218
and norm on $\mathbb{Z}[\sqrt{d}]$, 267
solved some Pell equations,
271
Brouncker continued fraction,
172

C

calculus
fundamental theorem, 172
Cantor, 108
and algebraic numbers,
304
diagonal argument, 108
proved uncountability of \mathbb{R} ,
108
transcendental numbers
easy construction, 304
cardinality, 107
of \mathbb{N} and \mathbb{R} , 107
cartesian
coordinate grid, 306
product, 85
casting out nines, 181
Chinese remainder
problems, 31
theorem, 189, 194
involving $\mathbb{Z}/lm\mathbb{Z}$, 195
traditional, 195
chord construction, 142
circle
arc length
related to area, 283

- circle (*continued*)
area
 proportional to R^2 , 285
 related to arc length, 283
division by rational points, 170
equation of, 71, 86
non-Euclidean, 101
transcendental area function, 287
circular functions, 147
 limit properties, 151
cis, 154
 addition formula, 154
combinatorics, 34
commutative law, 10
 for $+$, 10
 Grassmann proof, 29
 for \times , 11
completeness
 of \mathbb{R} , 83
 and angle measure, 145
 and arc length, 145
 implies uncountability, 108
complex analysis, 109
composition
 of functions, 92
 of reflections, 91, 97
 inverse of, 97
cone, 247
congruence
 angle-side-angle, 48
 axioms, 48
 in Hilbert, 48
classes
 introduced by Dedekind, 209
and motion, 47
side-angle-side, 47
side-side-side, 48
of triangles, 47
congruence classes, 183
difference, 183
product, 183
ring properties, 184
sum, 183
congruences
 addition, 181
 linear, 197
 mod n , 179
 multiplication, 181
 notation, 180
 quadratic, 197
 completing the square, 198
 subtraction, 181
conic sections, *see* conics
conics
 construction using, 247, 260
 eccentricity, 251
 equations for, 250
 focus-directrix property, 251
 have degree 2, 247
 integer points on, 263
 intersection of, 262
 as paths of projectiles, 247
 as sections of cone, 247
 simplest curves, 247
conjugation
 properties, 225
 and reflection, 225
constructible
 number, 75
 points, 73
 of non-Euclidean plane, 101
construction
 of basis over \mathbb{Q} , 166
 of ellipse
 by thread, 254

- and intersections, 72
impossibility of, 71
of points, 73
of product, 75
of quotient, 75
of regular pentagon, 76
of square root, 75
ruler and compass, 40
 bisecting an angle, 41
 bisecting a line, 41
 of equilateral triangle, 41
 of non-Euclidean circle, 103
 in non-Euclidean plane, 100
 n -secting a line, 42
of parallel, 42
of perpendicular, 42
of reflection in a circle, 102
of regular 17-gon, 43
of regular hexagon, 43
replicating an angle, 42
 of square, 43
using conics, 260
 of $\sqrt[3]{2}$, 260
 of cube roots, 261
continued fraction, 269
 Brouncker, 172
 periodic, 269
 for π , 173
 for $\sqrt{2}$, 269
 for $\sqrt{3}$, 271
convex, 52
coordinate, 69
 complex
 on non-Euclidean plane, 239
 on sphere, 239
 origin, 69
cosh, 293, 295
 addition formula, 297
cosine, 147
 addition formula, 152
 double angle formula, 156
function
 is transcendental, 150
half angle formula, 156
infinite series, 293
inverse, 152
rational values of, 169
countability
 of algebraic numbers, 304
 of \mathbb{N} , \mathbb{Z} and \mathbb{Q} , 107
cube
 Dehn invariant, 163
cube roots, 261
cubes mod p , 200
cubic
 curve, 141
 parameterization, 141
 rational points, 142
equation, 222
 Cardano formula, 222
 Viète solution, 223
cuboid, 56
curve
 algebraic, 150, 282
 area bounded by, 284
 cubic, 141
 elliptic, 141
 length of, 95
 quadratic
 degenerate, 256
 rational points, 124
cyclic group, 211
 finite, 211
 and primitive roots, 211
infinite, 211
 and Pell equation, 301

D

- Dürer, 276
- de Moivre formula, 154
- Dedekind, 26
- and successor function, 27, 30
 - cut, 79
 - for $\sqrt{2}$, 78
 - defined real numbers, 55
 - defined succession, 34
 - definition by induction, 35
 - definition of irrationals, 79
 - definition of reals, 79
 - definition of $+$ and \times , 80
 - ideals, 209
 - influenced set theory, 35
 - introduced congruence classes, 209
 - proof that $\sqrt{2}\sqrt{3} = \sqrt{6}$, 81
 - set of ideas, 28
- degree
- of equation, 247
 - geometric significance, 256
- Dehn, 159
- invariant, 161
 - of cube, 163
 - and equidecomposability, 163
 - of tetrahedron, 168
 - theorem, 168
- derivative, 154
- Descartes
- analytic geometry, 38
 - and cartesian product, 85
 - and coordinates, 69
 - Geometry*, 38
 - identified quadratic curves, 256
- descent, 2
- and Egyptian fractions, 3
- and Euclidean algorithm, 14
- in Fermat, 33, 131
 - in fundamental results, 23
 - gives prime divisor, 8
 - preferred to ascent, 32
 - and prime divisor property, 19
 - and sums of powers of 2, 183
 - used by Euclid, 32
- dilatation, 109
- as complex function, 227
- Diocles, 254
- focal property of parabola, 254
 - On Burning Mirrors*, 254
- Diophantine equations, 137
- and rational points, 137
- Diophantus, 117
- on area of triangles, 131
 - Arithmetica*, 117
 - circle without rational points, 125
 - identity, 216
 - Euler proof, 218
 - innovations in notation, 137
 - Pythagorean triples in, 116
 - rational points on circle, 140
 - sought rational solutions, 137
 - split a square in two, 139
- directrix, 251
- Dirichlet
- approximation theorem, 272
 - class number formula, 309
 - on Euclidean algorithm, 31
 - pigeonhole principle, 272, 308
 - theorem on primes, 9
 - unit theorem, 308
 - Vorlesungen*, 31

- Disquisitiones Arithmeticae*, 19
distance
 basic properties, 86
 Euclidean, 85
 non-Euclidean, 100
divisibility
 by 11
 test for, 182
 by 9
 test for, 182
 by 3
 test for, 182
division
 algorithm, 5
 mod n , 186
 and inverses mod n , 187
property
 of natural numbers, 5
 of polynomials, 135
 in $\mathbb{Z}[\sqrt{-2}]$, 233
 in $\mathbb{Z}[i]$, 230
 with remainder, 4
divisor, 4
 of $a^2 + 2b^2$, 238
 in terms of prime factors, 20
integer, 4
prime, 7
proper, 21
 of sum of two squares, 237
double angle formulas, 156
- E**
- e , 290
 infinite series, 294
 irrationality, 294
 is transcendental, 295
eccentricity, 251
Egyptian fractions, 3
- and descent, 3
unsolved problems, 4
ellipse
 equation of, 250
 focal property, 254
 integer points, 263
 no points at infinity, 279
 relative to horizon, 276
 as section of cone, 248
 as section of cylinder, 251
 sum of focal distances, 254
 thread construction, 254
- elliptic
 curve, 141
 parameterization, 141
 functions, 141
 parametrize cubic curves,
 141
- empty set, 28
equation
 of circle, 71, 86
 of cone, 248
 cubic, 222
 degree of, 247
 Diophantine, 137
 of ellipse, 250
 of hyperbola, 250
 indeterminate, 137
 of line, 86, 247
 linear, 13
 reason for name, 70
 of parabola, 250
Pell, 271
polynomial
 number of roots, 150
quadratic
 integer solutions, 309
 solved by Euclid, 56
quartic, 262

- equiangular spiral, 307
 equidecomposability, 62
 and Dehn invariant, 163
 equidistant line, 87, 253
 and reflection, 90
 Euclid, 7
 congruence concept, 47
 formula for perfect numbers,
 21
 formula for Pythagorean
 triples, 114
 variations, 115
 parallel axiom, 44
 proof of Pythagorean
 theorem, 53
 proof of triangle inequality,
 94
 solved quadratic equations, 56
 summed geometric series, 34
 synthetic geometry, 38
 theorem on perfect numbers,
 21
 theorem on primes, 7
 used descent, 32
- Euclidean
 distance, 85
 and Pythagorean theorem,
 85
 geometry
 defined by equations, 71
 defined by similarities, 109
 plane, 86
 isometries, 89
 in non-Euclidean space, 241
 space, 97
 isometries, 97
- Euclidean algorithm, 13
 avoided by Gauss, 31
 correctness, 14
- Euclid's description, 13
 and Fibonacci numbers, 16
 and Gaussian integers, 32
 and inverses mod n , 189
 periodicity, 268
 for polynomials, 135
 reinstated by Dirichlet, 31
 and side and diagonal
 numbers, 270
 solves linear congruence, 198
 speed up, 15
 and square roots, 267
 subtraction form, 13
 in $\mathbb{Z}[i]$, 230
- Eudoxus, 285
- Euler
 constant, 291
 criterion
 and primitive roots, 200
 for squares mod p , 198
 in terms of $\left(\frac{a}{p}\right)$, 199
 formula for $e^{i\theta}$, 292
 formula for cot, 151
 found divisor of $2^{2^5} + 1$, 193
 named Pell equation, 271
 phi function, *see* phi function
 product formula, 173
 proof of Diophantus' identity,
 218
 proved two squares theorem,
 139
 series for π
 and Brouncker fraction, 173
 series for even powers of π ,
 173
 solution of $y^3 = x^2 + 2$, 236
 theorem on perfect numbers,
 23
 proof by Dickson, 23

exponential function, 154, 283,
 290
addition formula, 292
of complex variable, 293
 defined geometrically, 306
 embraces cos and sin, 293
and hyperbola, 283
infinite series, 293
inverse to log, 290
is transcendental, 293
exponential map, 306

F

factor, 6
factorization, 5
 algebraic, 6
 of Pythagorean triples, 159
 of sums of squares, 237
Fermat
 and coordinates, 69
 and descent, 33
 descent proof, 131
 identified quadratic curves,
 256
last theorem, 139, 190
 fourth power case, 141
 inspired by Diophantus,
 140
little theorem, 190
 and Euler's criterion, 198
 and prime recognition, 212
 and RSA, 212
number, 193
primes, 7
 and constructible n -gons, 44
on rational right triangles, 131
solved some Pell equations,
 271

sought factors of $2^n - 1$, 22
theorem about $x^2 + 2y^2$, 242
theorem about $x^2 + 3y^2$, 242
theorem on fourth powers,
 133
 Cassels proof, 134
trouble with $x^2 + 5y^2$, 242, 245
two squares theorem, 139, 233
 and Gaussian primes, 234
 proved by Euler, 139
Ferrari, 262
Fibonacci, 3
 Liber Abacci, 3
 Liber Quadratorum, 131
numbers, 16
 and Euclidean algorithm,
 16
 and integer points, 301
on area of triangles, 131
proved Diophantus' identity,
 217
field, 12
 in Euclidean geometry, 106
finite, 221
 of fractions, 12
focal property
 of ellipse, 254
 of parabola, 253, 254
focus, 251
 at infinity, 255
means fireplace, 252
 in theory of gravitation, 252
foundations
 of arithmetic, 26
 of calculus, 26
 of geometry, 26
fractions
 addition, 12
 Egyptian, 3

- fractions (*continued*)
 - extend natural numbers, 5
 - field of, 12
 - in lowest terms, 5
 - multiplication, 12
 - unit, 3
 Frey, 141

 function
 - additive, 165
 - and axiom of choice, 174
 - algebraic, 150, 281, 282
 - circular, 147
 - limit properties, 151
 - composition, 92
 - continuous, 174
 - continuous additive, 174
 - elliptic, 141
 - exponential, 154, 283, 290
 - hyperbolic, 295
 - linear fractional, 241
 - and geometry, 241
 - periodic, 150
 - recursive, 35
 - transcendental, 150, 281
 - in geometry, 282
 fundamental theorem
 - of algebra, 221
 - and completeness of \mathbb{R} , 304
 - of arithmetic, 20
 - first stated by Gauss, 20
 - of calculus, 172
G

 gap, 83
 - in countable set of reals, 108
 - in rationals, 82
 Gauss
 - avoided Euclidean algorithm, 31
 - congruence concept, 179
 - construction of 17-gon, 43
 - description of gcd and lcm, 20
 - Disquisitiones Arithmeticae*, 19
 - on prime divisor property, 20
 - proof of Wilson's theorem, 191
 - proved primitive roots exist, 200
 - results using congruence, 208
 - on Wilson's theorem, 208
 Gaussian integers, 221, 227
 - division property, 230
 - Euclidean algorithm, 32, 230
 - form a ring, 227
 - gcd, 231
 - linear representation, 232
 - norm, 228
 - prime divisor property, 232
 - refine understanding of \mathbb{Z} , 227
 - unique prime factorization, 230
 - units, 228
 Gaussian primes, 228
 - classification, 235
 - infinitely many, 229
 - and two squares theorem, 234
 gcd, 13
 - of Gaussian integers, 231
 - linear representation, 232
 - and inverses mod n , 187
 - linear representation, 14, 31
 - in terms of prime factors, 20
 - produced by Euclidean algorithm, 14

- geometric algebra, 54
on Greek coin, 67
and product of lengths, 54
relates lengths via areas, 54
- geometric series
and perfect numbers, 21
and periodic decimals, 82
summed by Euclid, 34
and volume of tetrahedron, 58
- geometry
analytic, 38, 54
in Descartes, 38
in Hilbert, 38
reason for name, 71
- defined by isometries, 96
- Euclidean
defined by equations, 71
Klein definition, 95
non-Euclidean, 71
projective, 275
of sphere, 97
synthetic, 38
in Euclid, 38
in Hilbert, 38
- glide reflection, 93
and complex numbers, 226
from three reflections, 93
- Grassmann, 26
defined + and \times by induction,
27
Lehrbuch, 34
proof of associative law, 29
proof of commutative law, 29
proved ring properties of \mathbb{Z} ,
27
- gravitation, 64
and focus, 252
- great circle, 97
reflection in, 97
- greatest common divisor, *see gcd*
- Gregory, 172
- group, 211
abelian, *see abelian group*
cyclic, *see cyclic group*
infinite cyclic, 267
of integer points, 301
nonabelian, 211, 243
in number theory, 243
of similarities, 109
of transformations, 97
- H**
- half angle formulas, 156
and Pythagorean triples, 156
- half turn, 88
is composite of two
reflections, 92
- of non-Euclidean plane
about i , 239
of sphere, 239
- Hamilton, 216
- Heiberg, 65
- Hermite, 295
- Hero, 123
triangle area formula, 123
- Hilbert
analytic geometry, 38
congruence axioms, 48
Foundations of Geometry, 38
invariance of area, 61
synthetic geometry, 38
third problem, 159
solution by Dehn, 168
- Hippocrates of Chios, 285
- horizon, 276
- hyperbola, 126
addition of points, 297