Index

absolute error, 14
algorithm, 28
aliquot part, 184
analysis, 46
arithmetic progression, **29**, 156
asymptotically equivalent, 14

bad prime, **160**, 188
base, 189
Bertrand, Joseph, 16
Bézout equation, 59, 62, **63**, 107
biquadrate, 18, 53
Brahmagupta, 177

Carmichael number, 103
Chebyshev, Pafnuty, 16
Chinese remainder theorem, xi, 62, 81, 85, 87, **89**, 92, 107, 112
composite, **12**
condition 2-N-p, 128
condition N-C, **41**, 76, 84, 99, 132
condition p-N-p, 138
congruence, ix, 29, 76, 82, **81–84**
consecutive, 35, **41**, 75–78, 84, 85, 126, 131, 132, 142, 149, 151, 152

descent, *see* method of descent
determinant, 174
Diophantine equation, **18**, 20, 86
Diophantus of Alexandria, 18
Dirichlet, Gustav Lejeune, x, 32, 96
discriminant, 174
divide, 26
divides, 28
divisible, 28
division algorithm, 28
divisor, **28**, 28, 71

Eisenstein, Gotthold, x, xi, 161, 164
equality of fractions, 65
equivalence class, 84
error correction, 16
Euclid, x, 45, 60, 66, 102, 181
Euclid's lemma, xi, **47**, 51, 58, 69
Euclidean algorithm, 59, **62**, 107
Euler phi function identity, 118
Euler triple, 54
Euler's criterion, 121, 122, 160
Euler's phi function, **110**
Euler's theorem, 112
Euler, Leonhard, x–xi, 2, 16–19, 45, 51, 96, 102, 104, 112, 115, 117, 121, 122, 156, 178, 182, 187, 191
even, 23
expand, 64
exponent, 183

fantasy numbers, 47
Fermat number, xii, 102, 190–192
Fermat prime, 192
Fermat's last theorem, ix–x, 2–4, 7, 9–11, 16, **19**, 21, 23, 25, 34, 36, 42, 45, 71, 72, 77, 78, 99, 101, 125, 137, 142, 145, 147
Fermat's theorem, ix–xi, 76, 81, 96–97, **101**, 106–114, 120–121, 155, 164, 181
Fermat, Pierre de, x, xi, 2, 14, 17–20, 45, 54, 57, 91, 102, 104, 142, 155–158, 164, 169, 177, 181
fraction, x, 59, 64, 69, 104
fundamental theorem of arithmetic, 51

Gauss, Carl Friedrich, ix–xi, 2, 3, 8, 10, 14, 18, 21, 25, 29, 59, 72, 81, 82, 92, 96–97, 110, 119, 120, 160, 164
gcd, *see* greatest common divisor
geometric progression, 30, 189
Germain prime, *see* Sophie Germain prime
Germain's basic lemma, **77**, 81, 84, 99
Germain's theorem, *see* Sophie Germain's theorem
Germain, Sophie, ix–xi, 1–4, **7–10**, 19, 21–22, 29, 71, 74, 81, 99, 120, 137–138, 142, 147, 149, 151
Goldbach's conjecture, 16
Goldbach, Christian, 16, 51
good prime, **160**, 188
greatest common divisor, **60**, 68, 69

Hardy, G. H., 16

infinitude of primes, 30
integer, 18
inverse, 71, 72
isomorphism, 123
Ivory, James, x, 105

Lagrange's four-square theorem, 17
Lagrange's theorem, 105, 113, **115**
Lagrange, Joseph-Louis, x, xi, 2, 8, 17, 96, 105, 113, 115, 159, 169
least common multiple, 88
least residue, 82
Legendre symbol, 160
Legendre, Adrien-Marie, ix–xi, 2, 3, 8–9, 14, 18, 21–22, 25, 29, 44, 45, 80, 83, 120, 142–143, 147, 149–151, 158–160, 162
Leibniz, Gottfried, x, 96, 102
Libri, Guglielmo, 151
linear congruence, xi, 81, **85**, 85
linear equation, 85
logarithm, 122

mathematical induction, 12, **57**
Mersenne number, 102, 183
Mersenne prime, xii, **183**
method of descent, 19, **54**, 58, 192
Millennium Prize Problems, 17
modular arithmetic, 82
modulus, 82
multinomial theorem, 103
multiple, 28

natural number, **10**, 11, 13
non-consecutive, **41**, 76, 84, 101
nontrivial prime divisor, 157
number
  composite, *see* composite
  Fermat, *see* Fermat number
  Mersenne, *see* Mersenne number
  natural, *see* natural number
  prime, *see* prime
number theory, **10**, 11, 13, 16, 17, 19, 21, 24–26, 29, 34, 45, 47, 58, 59, 74, 81, 96, 101, 106, 164, 182
numerical integration, 16

$o(a)$, 110
odd, 23
order, **108**, 108, 110, 116–118, 121
Ore, Oystein, xi

parity, 48
perfect number, **102**, 181
perfect square, 18
period, 34
φ, 110
polygonal number theorem, 18
polynomial, 85, 96, 113, 115, 116
power residue, ix, xi, 25–26, **32**, 35, 71–80, 84, 99–105, 107, 121, 125–134, 138–146, 155
powers and relative primality, 50, 51
primality testing, 16
prime, **12**
  Fermat, *see* Fermat prime
  Mersenne, *see* Mersenne prime
  Sophie Germain, *see* Sophie Germain prime
prime factorization
  uniqueness of, *see* uniqueness of prime factorization
prime number theorem, 14
prime to, 46
primitive Pythagorean triple, 46
primitive root, x, 76, 81, 85, 99, **100**, **109**, 118
Pythagorean proportionality, **66**, 69
Pythagorean triangle, **18**, 57
Pythagorean triple, **11**, 45

quadratic form, xi, 122, 143, 155, 156, 169
quadratic reciprocity, xi, 18, 96, 122, 143, 155, 158, 160, 161, **162**, 164
quadratic residue, **155**, 157, 160, 181
quotient, 28

random number, 16
reduce, 65
relative error, 14
relatively prime, 46
remainder, 26, **28**
residue, 26, **28**, 71, 72
Riemann hypothesis, 17
RSA cryptosystem, xi, 16, 81, 91, 101, 106, 113

Sophie Germain prime, xii, **145**, 164, 181, 188
Sophie Germain's theorem, 9, 137, **142**, 142, 144, 145, 147
Sunzi, x, 87
synthesis, 46
system of linear congruences, xi, 81, 87

trivial, 23
Twain, Mark, ix
twin prime conjecture, 15

uniform finiteness, 43
uniqueness of prime factorization, x, **51**, 58, 69, 104, 187
unit, **83**, 108, 109, 116
unity, 25, 26, **36**

Wiles, Andrew, 20
Wilson's theorem, x, 81, 96, **97**, 115, 121

zero divisor, 83