Index

abstract algebra, 53, 118
Adleman, Leonard, 65
Agrawal, Manindra, 126
AKS primality test, 126
al-Haytham, Abu, 62
Archimedes, 109, 119, 122
arithmetical geometry, 108
Artin's Conjecture, 85
Artin, Emil, 85
Aryabhata, 24
asymmetrical key, 69

Bachet, Claude, 24
Bessy, Frenicle de, 62
Bhaskara, 122
Binomial Theorem, 58, 62
Brahmagupta, 24, 50, 52, 122
Brouncker, William, 110, 122

Chinese Remainder Theorem, 51–52
common divisor, 16
  greatest, 17
complete residue system modulo n, 47, 48, 56, 80, 84, 88, 91
  canonical, 47, 54
composite number, 29, 57, 125, 126
congruent modulo n, 8, 43

Descartes, Rene, 41, 106
Diffie, Whitfield, 69
Diophantine approximation, 109
Diophantine equation, 20, 86, 99, 102, 109
Diophantus of Alexandria, 24
Dirichlet's Rational Approximation Theorem, 112, 113, 116
Dirichlet, Lejeune, 37, 106
discrete logarithm modulo p, 70
Disquisitiones Arithmeticae, 52
divide, 8
divisibility tests, 14, 45–46
Division Algorithm, 15

elliptic curve, 70, 108
equivalence class, 47
equivalence relation, 12
Eratosthenes, 30
  Sieve of, 30
Euclid, 41
Euclidean Algorithm, 18, 49, 66
Euler ϕ-function, 59, 60, 76, 77, 79–81
Euler's Criterion, 90, 91, 95
Euler's Theorem, 60, 62, 66, 82, 91
Euler, Leonhard, 21, 24, 40, 42, 52, 62, 63, 89, 106, 107, 110, 127
exponential time algorithm, 124

Fermat number, 127
Fermat prime, 38
Fermat's Last Theorem, 86, 99, 105, 107, 108
  exponent 4, 105

Fermat's Little Theorem, 55–60, 62, 63, 66, 74, 79, 91, 125
Fermat, Pierre de, 41, 52, 62, 104, 106, 122
Four Squares Theorem, 107
Fundamental Theorem of Algebra, 73, 74
Fundamental Theorem of Arithmetic, 30–35
  applications, 32–35
  statement, 31

Gauss' Lemma, 92
Gauss, Carl Friedrich, 39, 51, 91, 129
Germain, Sophie, 85, 86
Girard, Albert, 106
Goldbach Conjecture, 40
Goldbach, Christian, 40, 106
Great Internet Mersenne Prime Search, 42
greatest common divisor, 17
Green, Ben, 37

Hardy, G. H., 107
Hellman, Martin, 69

integer, 8
inverse modulo p, 61
irrational number, 33, 109, 110, 118
irreducible polynomial, 134
Ivory, James, 62

Kayal, Neeraj, 126
key exchange, 69, 84
Koblitz, Neal, 70

Lagrange's Theorem, 74
Lagrange, Joseph, 25, 52, 63, 73, 85, 107
Law of Quadratic Reciprocity, 94, 99
least common multiple, 23
Legendre symbol, 89
Legendre, Adrien-Marie, 39, 52, 89, 106
Lehmer, D. H., 128
Leibniz, Gottfried Wilhelm, 63
linear congruence, 48–50, 53
  systems of, 50
linear Diophantine equation, 16–22, 48, 49, 67, 83, 109, 114
Lucas, Edouard, 127
Lucas-Lehmer Test, 128

mathematical induction, 28, 130, 131
  strong, 133, 134
Mersenne prime, 38, 42, 127, 128
Mersenne, Marin, 41, 106
method of descent, 105
method of successive squaring, 44–45
Miller's Theorem, 86, 96
Miller, G. A., 86
Miller, Victor, 70
multiplicative function, 80, 81

natural number, 8

order of a modulo n, 55–57, 74, 75, 86

Pascal, Blaise, 106
Pell equation, 109, 110, 113–115, 117–119, 121, 122
  non-trivial solutions, 114–117
  nontrivial solutions, 119
  trivial solutions, 114, 119
Pell, John, 110
Pepin's Test, 128
Pepin, Theophile, 127
perfect number, 41
polynomial time algorithm, 124–126
polynomials modulo n, 45, 73, 74
Poulet number, 126
primality test, 123–127
prime number, 29, 47, 56, 65–67, 70, 76, 77, 79, 123, 127
  $4k + 1$ primes, 90
  $4k + 3$ primes, 36, 90
  Fermat prime, 38
  in arithmetic progressions, 36–37
  infinitude of, 36, 41, 90
  Mersenne prime, 38, 127, 128
  Sophie Germain prime, 86, 95, 96
Prime Number Theorem, 40
primitive Pythagorean triple, 100, 103

primitive root, 70, 75, 76, 79, 81, 84–86, 88, 95
probable prime test, 125, 126
Proth's Test, 128
Proth, Francois, 128
public key codes, 65, 66, 70
Pythagorean Theorem, 99
Pythagorean triple, 100, 104, 106, 109
  infinitude of, 101
  primitive, 100, 103
Pythagorean Triple Theorem, 101

quadratic non-residue, 88
Quadratic Reciprocity Theorem, 93
quadratic residue, 88, 103

Ramanujan, Srinivasa, 107
rational number, 33, 109
reducible polynomial, 134
relatively prime, 17, 57, 60, 74, 80
Rivest, Ronald, 65
root, 73
roots modulo n, 81–83
RSA encryption, 65–70, 123

Saxena, Nitin, 126
Shamir, Adi, 65
Shimura-Taniyama Conjecture, 108
Sieve of Eratosthenes, 30, 39
Sophie Germain prime, 86, 95, 96
strong mathematical induction, 133, 134
sums of squares, 102, 106
  representing numbers, 104
  representing primes, 102
symmetrical key, 69, 70
system of linear congruences, 50–51

Tao, Terence, 37
Taylor, Richard, 108
triangular number, 121
Twin Prime Question, 39

Wallis, John, 122
Waring, Edward, 63
Well-Ordering Axiom, 14, 119
Wiles, Andrew, 105, 108
Wilson's Theorem, 61–63, 124
  converse of, 62
Wilson, John, 63