

Index

- abacus, 65–66
- absolute pseudoprime, 99
- Adleman, Len, 108
- algebra of congruences, 76–78
- amicable numbers, 33–34, 38, 40, 42
- applying congruences, 87–99
- area of triangle, 50–53
- Arithmetica*, 3, 53–54

- Bachet, Claude, 54
- base, 58, 60, 64–68, 89
 - base-5 system, 58
 - base-8 system, 67–68
 - base-10 system, 58, 68
 - base-12 system, 61
 - base-20 system, 58, 62
 - base-60 system, 59, 62
- Bible, 1
- binary digits, 62, 67
- binary system, 66–68
- binomial coefficients, 81
- binomial law, 80–81
- bits, 67–68, 108
- Bletchley Park, 101

- Caesar, Julius, 91, 102, 105
- Caesar cipher, 102–105
- calculating devices, 64–66
- calculation, 1
- calculus, 1, 66
- calendar
 - Gregorian, 91–93
 - Julian, 91
 - Mayan, 42
- Carmichael number, 99
- Carmichael, R. D., 99
- casting out nines, 88–90
- checks on computation, 87–90
- cipher
 - Caesar, 102–105
 - monoalphabetic, 102–106
 - polyalphabetic, 106–108
 - public key, 108–113
 - RSA, 108–113
 - substitution, 102–105
 - transposition, 102
 - Vigenère, 105–108
- ciphertext, 102
- coded decimals, 68
- codetalkers, 101
- common divisor, 35–37, 39, 43–45, 51
 - greatest, 35–36, 39–41, 51, 73, 111, 113
- common multiple, 41
 - least, 41–42, 59
- composite number, 15–18, 49, 97–99
- computations, checks on, 87–90
- computer, 21, 55, 66–68, 107, 112–113
- congruence, 73–84, 87–99
- congruent, 73
- Cooper, Curtis, 21
- counting
 - Danish, 58–59
 - English, 59
 - French, 58
 - German, 59
 - Mayan, 58, 62–63
 - Mesopotamian, 59, 62
- counting board, 87
- credit card, 107, 109
- cross-bone check, 89–90
- cryptarithm, 68–71
- cryptology, 101–113
- cube number, 4

- days of the week, 91–95
- decimal system, 57–58, 61, 66, 68, 87, 89
- Descartes, René, 33
- Diffie, Whitfield, 108

- digit sum, 87
- Diophantine problem, 3
- Diophantus of Alexandria, 3, 53–54
- Disquisitiones Arithmeticae*, 23, 87
- division, 38
- division rule, 37, 78
- divisor, 15
 - common divisor, 35–37, 39, 43–45, 51
 - trivial divisor, 15
- Dozenal Society of America, 61
- Dudeney, H. E., 69
- Dürer, Albrecht, xii, 8, 12

- early calculating devices, 64–66
- Egyptian surveyors, 3
- Enigma, 101
- Eratosthenes, 17
 - sieve of, 17–19
- Euclid, 19
- Euclid's algorithm, 38–40, 11, 113, 126
- Euclid's *Elements*, 40
- Euler, Leonhard, 20, 22, 32, 54–55, 83–85
- Euler's phi-function, 83–85, 110–111
- Euler's theorem, 84
- even-prime, 27, 118–119

- factor, 15
- factor table, 18, 25
- factorization, 15, 25–34
- Fermat number, 22, 24, 68, 80, 98, 118
- Fermat prime, 22–24, 118
- Fermat, Pierre de, 22, 33, 48, 53, 55
- Fermat's conjecture, 53–55
- Fermat's last theorem, 53–55, 82
- Fermat's little theorem, 80–84, 97–99
- Fermat's method, 112–113
- figurate number, 4–7
- floor, 38, 92
- Franklin, Benjamin, 10–13, 117
- fundamental factorization theorem, 25–26
- fundamental theorem of arithmetic, 26

- Gauss, C. F., 23–24, 73, 87
- gematria, 31

- geometric series, 32
- Germain, Sophie, 55
- Germanic folklore, 1
- Gillies, Donald B., 21
- GIMPS, 21
- greatest common divisor, 35–36, 39–41, 51, 73, 111, 113
- greatest integer, 38
- Greeks, 2, 4, 6, 22, 31, 33, 52
- Gregorian rules, 92–93
- Gregory, XIII, Pope, 91
- Gregorian calendar, 91–93

- harpedonapts, 3
- Hellman, Martin, 108
- Heron, 52
- Heronian triangle, 52–53
- hexagonal number, 6
- highly composite number, 30
- Hindu mythology, 1
- Hindu–Arabic number system, 58
- Hurwitz, Alexander, 21

- Julian calendar, 91

- k -gonal number, 6–7
- Kummer, Ernst, 55

- leap year, 91–93
- least common multiple, 41–42, 59
- Legendre, A.-M., 54–55
- Lehmer, D. H., 98
- Lehmer, D. N., 16, 18
- logarithm, 21, 62, 64–66
- Lucas, Édouard, 20
- lucky number, 1

- magic circle, 10, 12–13, 117
- magic square, 7–12, 68, 116–117
- magic sum, 7, 9, 11–12, 117
- Melencolia I*, xii, 8
- Merkle, Ralph, 108
- Mersenne, Marin, 20
- Mersenne prime, 19–21, 31, 32
- Mesopotamians, 2, 3, 59, 62
- modulus, 73
- monoalphabetic cipher, 102–106

- multiple, 41
- multiplication sign, 89
- natural number, 1
- Navajo, 101
- Nim, 66
- number
 - amicable pair, 33–34, 38, 40, 42
 - composite, 15–18, 49, 97–99
 - cube, 4
 - Fermat, 22, 24, 68, 80, 98, 118
 - hexagonal, 6
 - highly composite, 30
 - k -gonal, 6–7
 - lucky, 1
 - natural, 1
 - pentagonal, 5–6
 - perfect, 19, 31–33, 68, 119
 - polygonal, 5–7
 - prime, 4, 15–24, 97–99
 - rectangular, 4
 - relatively prime, 37
 - square, 4
 - triangular, 5
- number of divisors, 28–29
- number system, 57–68
- numerology, 1, 2, 31, 33
- octal system, 67–68
- one-time pad, 108
- pentagonal number, 5–6
- Pepys, Samuel, 63
- perfect number, 19, 31–33, 68, 119
- perimeter of triangle, 52–53, 122
- phi-function, 83–85, 110–111
- plaintext, 102
- Plato's *Republic*, 2
- polyalphabetic cipher, 106–108
- polygon, 5–6, 22–24, 118
- polygonal number, 5–7
- positional system, 58
- positive integer, 1
- Poulet, P., 98
- powers of congruence, 78–80
- prime number, 4, 15–24, 97–99
- primitive Pythagorean triple, 43–46
- primitive triangle, 47–53, 83, 121
- proof by contradiction, 26
- pseudoprime, 98–99
- public key cipher, 108, 112–113
- Pythagoras, 2
- Pythagorean equation, 2–3, 44–46
- Pythagorean problem, 2
- Pythagorean theorem, 43–55
- Pythagorean triangle, 47–53, 82–83, 122
- Pythagorean triple, 43–44, 47, 121
- Pythagoreans, 57
- quotient, 35, 38
- rectangular number, 4
- reductio ad absurdum, 26
- regular n -gon, 22–24
- regular polygon, 6, 22–24
- regular prime, 55
- relatively prime numbers, 37–38
- remainder, 38, 75–76
- Renaissance, 6, 87
- Riesel, H., 21
- right-angled triangle, 2, 43, 47–53
- Rivest, Ron, 108
- Robinson, R. M., 21
- round-robin schedule, 95
- Royal Society, 63
- RSA cipher, 109–113
- RSA system, 108, 112
- secret key, 101, 105–108
- sexagesimal system, 59, 61–62
- Shamir, Adi, 108
- sieve of Eratosthenes, 17–19
- square number, 4
- semi-magic square, 117
- Stifel, Michael, 11
- Strand Magazine*, 69
- substitution cipher, 102–105
- straightedge and compass, 22–24
- sum of two squares, 48–50, 53
- social security number, 112–113
- table
 - amicable pairs, 34
 - prime numbers, 17

- primitive Pythagorean triples, 46
- number of divisors, $\tau(n)$, 29
- Thābit ibn Qurra, 33
- tournament schedule, 95–97
- transposition cipher, 102
- triangular number, 5
- trivial divisor, 15
- trivial factorization, 15

- Vigenère, Blaise de, 106
- Vigenère cipher, 105–108

- Wiles, Andrew, 55