

- congruence, 19, 193
- conjugate, 32
- continued fraction, 155
  - factorization method, 158-159
- convergent, 155
- cryptanalysis, 56
- cryptography, 54
  - public key, 85
- cryptosystem, 54-55, 83
  - classical, 88
  - composition, 64, 79
  - Diffie-Hellman, 98-99, 181-182
  - ElGamal, 100-101, 109, 182
  - elliptic curve, 181-182
  - knapsack, 113-115
  - Massey-Omura, 100, 109, 182, 216
  - Merkle-Hellman, 113-114
  - private key, 88
  - product, 64, 78-79
  - public key, 85
  - RSA, 22, 92-93, 106, 125, 137, 153
  - structure, 56
  - symmetric, 88
- cyclic group, 34
- Cyrillic, 63, 78
  
- Data Encryption Standard, 101
- deciphering, 54
  - key, 83
  - transformation, 54
- decryption, 54
- determinant, 67
- deterministic algorithm, 127
  - encryption, 89
- Diffie-Hellman assumption, 99, 121
  - key exchange, 98-99, 181-182
- Digital Signature Standard, 101-102
- digits, 1
  - binary (bit), 3
  - number of, 3
- digraph, 54, 59
  - transformation, 59
- Dirichlet  $L$ -series, 134
- discrete log, 97-98
  - algorithms for, 102-106
  - on elliptic curve, 180
- divisibility, 12
  - exact, 12
- division points, 173
- divisor, 12
  - nontrivial, 12
  - proper, 12
  
- ElGamal cryptosystem, 100-101, 109, 182
  - signature, 109-110
- elliptic curve, 167-168
  - addition law, 168-170
  - complex points, 171
  - cryptosystem, 181-182
  - factorization, 191-192, 195-198
  - global, 183
  - nonsupersingular, 181
  - over finite field, 174
  - primality test, 188-190
  - rank, 173
  - real points, 176-177, 227
  - reduction, 184, 193-194
  - supersingular, 181
  - torsion subgroup, 173, 185
  - Weil pairing, 180-181
  - zero element, 169
  - zeta-function, 175
- elliptic function, 173
- enciphering, 54
  - key, 56, 83
  - matrix, 71-72
  - transformation, 54
- encoding, 179
- encryption, 54
- Euclidean algorithm, 13
  - for Gaussian integers, 18
  - for polynomials, 17
- Euler phi-function, 15, 21-22
  - pseudoprime, 129
- exponentiation, 23, 97
  
- factor base, 145
  - algorithm, 103, 148
- factoring, 27-29, 92
  - continued fraction method, 158-159
  - with elliptic curves, 191-192, 195-198