
Index

- abelian, 76
- affine space, 148
- associative, 74

- basis, 32
- binary operation, 73
- birthday paradox, 119

- Cayley table, 128
- Chinese Remainder Theorem, 70
- ciphertext, 63
- closed, 31
- collision, 118
- commutative, 74
- composite, 55
- congruence modulo n , 80
- conic, 40
- coprime, 51
- cubic, 40
- cyclic, 134

- degree, 40
- dihedral group, 132
- dimension, 32
- direct product, 136
- discriminant, 179
- divides, 47
- division algorithm, 47

- elliptic curve, 3
- equivalence class, 79

- equivalence relation, 79
- Euler's totient function, 86

- forward secrecy, 143
- Fundamental Theorem of Finite Abelian Groups, 139
- Fundamental Theorem of Arithmetic, 23, 41, 55

- genus, 28
- greatest common divisor, gcd, 51
- group, 75

- hash function, 114
- homogenization, 154
- homomorphism, 130

- identity, 74
- inverse, 75
- irreducible, 41
- isomorphic, 128
- isomorphism, 130

- keyspace, 64

- Lagrange interpolation, 168
- line, 40
- linear combination, 29, 32

- modulus, 108
- multiplicity, 38, 223

natural numbers, 46

one-way function, 118

order of a group, 88

order of an element, 88

partition, 80, 81

plaintext, 63

preimage resistance, 118

prime, 55

Prime Number Theorem, 237

primitive Pythagorean triple, 16

primitive root, 141

projective plane, 151

projective n -space, 152

projective line, 149

pseudoprime, 91

quadratic nonresidue, 186

quadratic residue, 186

rational curve, 40

reflexive, 78

relatively prime, 16, 51

ring, 76

safe prime, 144

second preimage resistance, 118

shift cipher, 64

symmetric, 78

symmetric group, 131

textbook RSA, 108, 112

torsion point, 178

transitive, 78

vector spaces, 30

well-defined, 83

well-ordered, 48

zero set, 39