
Index

- 15 Puzzle, 30
 - and permutations, 31
- Adleman, Leonard, 4
- Advanced Encryption Standard, 11
- AES, 11
- asymmetric cryptosystem, 11
- biconditional statement, 89
- bijection, 57
- Binet's Formula, 74
- binomial theorem
 - for real numbers, 9
- cases, proof using, 100
- check digits
 - ISBN-10, 17
 - Luhn algorithm, 17
 - Verhoeff scheme, 18
- choose-an-element method, 93
- cipher
 - Caesar's's, 12
 - Hill, 13
 - shift, 12
 - stretch, 12
- Cocks, Clifford, 4
- complement of a set, 88
- complex number
 - argument, 118
 - norm, 118
 - trigonometric form, 118
- composite function, 59
- composite number, 88
- composition of functions, 59
- compound statement, 89
- conditional, 89
- congruent modulo n , 88
- conjunction, 89
- contrapositive, 94
- counterexample, 90, 92
- cryptography, 2
- cryptosystem
 - asymmetric, 11
 - symmetric, 11
- cubic formula, 111
- De Morgan's Laws
 - for statements, 89
- definition, 87
- difference of two sets, 88
- disjunction, 89
- distributive laws
 - for statements, 89
- divides, 87
- Division Algorithm
 - using cases, 101–102
- divisor, 88
- encryption
 - public key, 4
 - RSA, 4
- equal sets, 88
- Euler's formula, 121
- Euler's identity, 121
- even integer, 87
- Extended Principle of Mathematical Induction,
 - 72
- factor, 88
- Fermat's Little Theorem, 10
- Freshman's Dream, 10
- function
 - bijective, 57
 - composite, 59
 - composition, 59
 - injective, 56
 - inverse of, 61
 - invertible, 63
 - one-to-one, 56
 - onto, 57
 - surjective, 57
- golden ratio, 75
- implication, 89
- Induction
 - Extended Principle, 72
 - Principle of, 70

- Strong Form, 74
- injection, 56
- integers, 87
- intersection
 - of two sets, 88
- inverse of a function, 61
- invertible function, 63
- irrational numbers, 99, 103
- logically equivalent, 89
- mod n function, 2
- multiple, 88
- National Institute of Standards and Technology, 11
- natural numbers, 87
- negation, 89
- NIM, 25
 - strategy for playing, 29
- NIM sum, 26
- NIST, 11
- odd integer, 87
- one-to-one function, 56
- onto function, 57
- partially ordered set, 78
- prime number, 88
- Principle of Mathematical Induction, 70
- product
 - semidirect, 41
- proof
 - by contradiction, 97
 - contrapositive, 94
 - using cases, 100
- proper subset, 88
- Pythagorean Theorem, 96, 103
- quotient, 101
- rational numbers, 99, 103
- relation, 78
- relative complement, 88
- remainder, 101
- Rivest, Ron, 4
- roots of unity, 122
 - primitive, 123
- RSA encryption, 4
- semidirect product, 41
- semidirect product of groups, 41
- set
 - complement, 88
 - difference, 88
 - equality, 88
 - intersection, 88
 - partially ordered, 78
 - relative complement, 88
 - totally ordered, 78
 - union, 88
 - well-ordered, 79
- set equality, 88
- Shamir, Adi, 4
- statement, 89
 - biconditional, 89
 - compound, 89
- Strong Form of Mathematical Induction, 74
- subset, 88
 - proper, 88
- surjection, 57
- symmetric cryptosystem, 11
- symmetric groups
 - application to 15 Puzzle, 31
- totally ordered set, 78
- totient, 5
- union
 - of two sets, 88
- well-ordered set, 79
- Well-Ordering Principle, 79
- whole numbers, 87