Number Theory for Competitive Programming

Last Updated : 12 Jul, 2021

Read Discuss Courses Practice

Topics:

Basics:

1. GCD and LCM
2. Factorial
3. Prime factors
4. Binomial Coefficient
5. Catalan numbers
6. Euclid’s Lemma
7. Basic and Extended Euclidean algorithms
8. Integer sequences: Fibonacci, Padovan, OESIS

Modular Arithmetic :

1. Euler’s Totient Function
2. Euler’s Totient function for all numbers smaller than or equal to n
3. Modular Exponentiation (Power in Modular Arithmetic)
4. Find remainder without using modulo operator
5. Modular multiplicative inverse
6. Multiplicative order
7. Compute nCr % p | Set 1 (Introduction and Dynamic Programming Solution)
8. Compute nCr % p | Set 2 (Lucas Theorem)
9. Compute nCr % p | Set 3 (Using Fermat Little Theorem)

10. Chinese Remainder Theorem – Set 1 (Introduction), Set 2 (Inverse Modulo based Implementation)
11. Find Square Root under Modulo p | Set 1 (When p is in form of 4*i + 3)
12. Find Square Root under Modulo p | Set 2 (Shanks Tonelli algorithm)
13. Modular Division
14. Cyclic Redundancy Check and Modulo-2 Division
15. Primitive root of a prime number n modulo n
16. Euler's criterion (Check if square root under modulo p exists)
17. Using Chinese Remainder Theorem to Combine Modular equations
18. Multiply large integers under large modulo
19. Compute n! under modulo p
20. Wilson's Theorem

Number Theory :

1. Primality Test | Set 1 (Introduction and School Method)
2. Primality Test | Set 2 (Fermat Method)
3. Primality Test | Set 3 (Miller–Rabin)
4. Primality Test | Set 4 (Solovay-Strassen)
5. Legendre's formula (Given p and n, find the largest x such that p^x divides n!)
6. Carmichael Numbers
7. number-theoryGenerators of finite cyclic group under addition
8. Sum of divisors of factorial of a number
9. GFact 22 | (2^x + 1 and Prime)
10. Sieve of Eratosthenes
11. Goldbach's Conjecture
12. Pollard's Rho Algorithm for Prime Factorization

Coding Problems :

1. Searching for Patterns | Set 3 (Rabin-Karp Algorithm)
2. Measure one litre using two vessels and infinite water supply
3. Program to find last digit of n'th Fibonnaci Number
4. GCD of two numbers when one of them can be very large
5. Find Last Digit Of a^b for Large Numbers
6. Remainder with 7 for large numbers
7. Find (a^b)%m where 'a' is very large
8. Find sum of modulo K of first N natural number
9. Count all sub-arrays having sum divisible by k
10. Partition a number into two divisble parts
11. Find power of power under mod of a prime

12. Rearrange an array in maximum minimum form | Set 2 (O(1) extra space)
13. Subset with no pair sum divisible by K
14. Number of substrings divisible by 6 in a string of integers

Misc :

1. How to compute mod of a big number?
2. BigInteger Class in Java
3. Modulo 10^9+7 (1000000007)
4. How to avoid overflow in modular multiplication?
5. RSA Algorithm in Cryptography

Game Theory:

1. Minimax
2. Nim Game
3. Sprague – Grundy Theorem

Quick Links :

1. 'Practice Problems' on Modular Arithmetic
2. 'Practice Problems' on Number Theory
3. Ask a Question on Number theory

If you like GeeksforGeeks and would like to contribute, you can also write an article and mail your article to review-team@geeksforgeeks.org. See your article appearing on the GeeksforGeeks main page and help other Geeks.

Please write comments if you find anything incorrect, or you want to share more information about the topic discussed above