

## AlgoLab 2

1. (CLRS page no. 879) Write a C or a C++ program for modular exponentiation in  $O(\log n)$  time. You have to find the value of  $a^x \bmod n$  where  $a, x$  and  $n$  are integer. You should not multiply  $a, n$  times. This way it takes  $O(n)$  time.
2. Write a C or a C++ program to find GCD of two numbers. Write a C or a C++ program for function GCD for more than two arguments by the recursive equation  $\text{GCD}(a_1, a_2, a_3, \dots, a_n) = \text{gcd}(a_1, \text{gcd}(a_2, a_3, \dots, a_n))$ .
3. The numbers  $x$  and  $y$  are relatively prime and therefore there must exist integers  $a$  and  $b$  such that  $xa + yb = 1$ . Write a program to find such a pair of integers  $(a, b)$  with the smallest possible  $a > 0$ . Given this pair, can you determine the inverse of  $x \bmod y$ ? (<https://en.wikipedia.org/wiki/ExtendedEuclideanAlgorithm>)
4. Randomized algorithms : algorithm which may return wrong answer with some non-negligible probability. Miller Rabin algorithm is primality testing algorithm ( whether the number  $n$  is prime or not ) which is based on Fermat's theorem. You have to write a program for Miller Rabin algorithm. Check  $n = 2047 = 23 \times 89$  with  $a = 2$ . (CLRS page no. 891)

Note: Find the time complexity of all above algorithms.