**Assignment -2 (DAA)**

**Assignment should be submitted in loose sheet physically. [Deadline: 2078/08/26 (December 12, 2021)]**

**(Refer book: Introduction to Algorithms, 3rd Edition by Thomas H. Cormen ; page number 926 to 972. You may follow other resources but focus on book)**

a) Write short notes on following number theoretic notations
   i. Divisibility and divisors
   ii. Prime and composite numbers
   iii. The division theorem, remainders, and modular equivalence
   iv. Common divisors and greatest common divisors
   v. Relatively prime integers
   vi. Unique factorization
   vii. Modular linear equations
   viii. The Chinese remainder theorem
b) Write the recursive Euclidian algorithm to find GCD and analyze it's complexity
c) Write the Extended Euclidian algorithm and analyze it's complexity
d) Discuss about the use of Extended Euclidian algorithm to solve modular linear equation. Write the algorithm and analyze it. (Algorithm: MODULAR-LINEAR-EQUATION-SOLVER)
e) What do you mean by primality testing? Define pseudoprimality testing.
f) Discuss about the Miller-Rabin randomized primality test with algorithm and analysis.