<u>Unit-1</u>

1) Find g.c.d(252,198) by Euclidean Algorithm.
2) Find the inverse of 3 mod 5.
3) Define Euler Tuotient function. Find (32).
4) State Euler's criteria for quadratic residue mod prime. Verify whether 2 is a quadratic residue mod 13.
5) Find the quadratic residue mod 5.
6) State Law of Quadratic Reciprocity.
7) Find the value of $3^{31} \pmod 7$ by applying Fermat's Little theorem.
8) Show that 8 is a Quadratic residue mod 17.
9) Find an x between 0 and 19 such that $x^2 \equiv 5 \pmod{19}$.
10) Find $\varphi(125)$, where $\varphi(n)$ is Euler 'Phi" function of an integer "n".
11) Explain Euclidean Algorithm. Write the g.c.d(1547,560) as linear combination of 1547 and 560.
12) Distinguish between Legendre Symbol and Jacobi Symbol. Find $\left(\frac{1999}{2315}\right)$.
13) Find the remainder when 24^{1947} is divided by 17 by using Fermat's Little theorem.
14) Express the G.C.D of (726, 275) in the form of $m726+n275$, where m and n are any integers and find the values of m and n.
15) Suppose a and n are relatively prime such that g.c.d(a, n)=1, prove that
    - **a)** If $x^2 \equiv a \pmod n$ has a solution then $\left(\frac{a}{n}\right)=1$.
    - **b)** If $\left(\frac{a}{n}\right)=1$, we cannot conclude that $x^2 \equiv a \pmod n$ has solutions.
16) State and Prove Fermat's Theorem.
17) State and Prove Chinese Remainder Theorem.
18) Explain Miller-Rabin Algorithm. Test the primality of 561.
19) Using Chinese Remainder Theorem solve the following congruence's $x \equiv 1 \pmod 3$, $x \equiv 1 \pmod 4$, $x \equiv 1 \pmod 5$ and $x \equiv 0 \pmod 7$.
20) Solve $x \equiv 3 \pmod 4$, $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 3$ by using Chinese Remainder theorem.