M.Sc. - Mathematics
I Semester End Examination - May 2022
ELEMENTARY NUMBER THEORY

Course Code: MM106S | **QP Code: 11006**
Time: 3 hours | **Total Marks: 70**

Instructions: 1) **All** questions carry **equal** marks.
2) Answer **any five** full questions.

1. a) Prove that given integers a and b with $b > 0$, there exist unique integers q and r satisfying $a = qb + r,\ 0 \leq r < b$.
   b) Find the $\gcd(a, b)$, where $a = -427, b = 616$ and express $\gcd(a, b) = ax + by$.
   (7 + 7)
2. a) State and prove fundamental theory of arithmetic.
   b) If $m > 1$ and $p = 2^m - 1$ is prime then prove that m is prime.
   c) Prove that an integer $n > 1$ is composite if and only if it is divisible by some prime $p \leq \sqrt{n}$.
   (6 + 5 + 3)
3. a) State and prove the necessary and sufficient condition for existence of solution for linear congruence $ax \equiv b \pmod n$.
   b) If m is a positive integer and a is any integer such that $\gcd(a, m) = 1$, prove that $a^{\phi(m)} \equiv 1 \pmod m$. Hence deduce $a^{p-1} \equiv 1 \pmod p$, where p is prime which does not divide a.
   (7 + 7)
4. a) Given a prime p, let $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$ be a polynomial of degree n with integer coefficient such that $c_n \not\equiv 0 \pmod p$, then prove that the polynomial congruence $f(x) \equiv 0 \pmod p$ has atleast n solutions.
   b) Solve the system of linear congruences
   $$x \equiv 1 \pmod 3,\ \ x \equiv 2 \pmod 4,\ \ x \equiv 3 \pmod 5.$$
   (7 + 7)
5. a) Define Legendre symbol. State and prove Euler's criterion for Legendre symbol.
   b) State and prove Gauss lemma.
   (7 + 7)
6. a) Evaluate the Legendre symbol $(504|23)$.
   b) State and prove quadratic reciprocity law for Jacobi symbol.
   (6 + 8)
7. a) Prove that there is no prime p of the form $4k + 3$ is a sum of two squares.
   b) Prove that an odd prime p expressible as sum of two squares if and only if $p \equiv 1 \pmod 4$.
   (7 + 7)
8. a) Prove that any positive integer can be expressed as sum of four squares.
   b) State and prove Fermat's last theorem for the case $n = 4$.
   (6 + 8)

***