M.Sc.(Mathematics) (New CBCS Pattern) Semester - I

PSCMTH05(D) - Optional Paper : Number Theory

P. Pages : 2 **GUG/S/23/13744**

Time : Three Hours Max. Marks : 100

Notes : 1. Solve all **five** questions.
2. Each question carries equal marks.

UNIT - I

1. a) Prove that **10**

i) $ax \equiv ay \pmod m$ iff $x \equiv y \left(\operatorname{mod} \dfrac{m}{(a,m)}\right)$

ii) If $ax \equiv ay \pmod m$ & $(a,m)=1$ then $x \equiv y \pmod m$

b) Let $(a,m)=1$, Let $r_1, r_2, ..., r_n$ be a complete, or a reduced, residue system modulo m. Then prove that $ar_1, ar_2 ... ar_n$ is a complete, or a reduced residue system, respectively, modulo m. **10**

OR

c) If $(a,m)=1$ then prove that $a^{\oint(m)} \equiv 1 \pmod m$ **10**

d) Exhibit a reduced residue system modulo 7, composed entirely of powers of 3. **10**

UNIT - II

2. a) State & prove Hensel's Lemma. **10**

b) Solve $x^2 + x + 47 \equiv 0 \left(\operatorname{mod} 7^3\right)$ **10**

OR

c) Prove that the congruence $f(x) \equiv 0 \pmod p$ of degree n has at most n solutions. **10**

d) If p is a prime & (a, p) = 1. Then prove that the congruence $x^4 \equiv a \pmod p$ has (n, p-1) solutions or no solutions according as $a^{(p-1)}/(n, p-1) \equiv 1 \pmod p$ or not . **10**

UNIT - III

3. a) Let p denote an odd prime & a an integer relatively prime to p then prove that. **10**

i) $\left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right) = \left(\dfrac{ab}{p}\right)$

ii) $a \equiv b \pmod p \Rightarrow \left(\dfrac{a}{p}\right) = \left(\dfrac{b}{p}\right)$

iii) $\left(\dfrac{a^2}{p}\right) = 1; \left(\dfrac{a^2 b}{p}\right) = \left(\dfrac{b}{p}\right); \left(\dfrac{1}{p}\right) = 1$ if $(a,p)=1$

b) Let p be a prime integer. Let $(a,p)=1$ & $(b,p)=1$. If $x^2 \equiv a \pmod p$ & $x^2 \equiv b \pmod p$ are not solvable. Then prove that $x^2 \equiv ab \pmod p$ is solvable. **10**

OR

c) State & prove the Gaussian Reciprocity law. **10**

d) Evaluate $\left(\frac{-42}{61}\right)$. **10**

UNIT - IV

4. a) For each positive integer n, prove that **10**

$$d(n) = \prod_{P^{\alpha} \| n} (\alpha+1)$$

b) let f(n) be a multiplicative function & let $F(n) = \sum_{d/n} f(d)$ then prove that F(n) is multiplicative. **10**

OR

c) Find all solutions in positive integers. **10**

$$5x + 3y = 52$$

d) Show that the positive primitive solutions of $x^2 + y^2 = z^2$ with y even are $x = r^2 - s^2$, $y = 2rs$, $z = r^2 + s^2$, where r & s are arbitrary integers of opposite parity with $r > s > 0$ and $(r,s) = 1$. **10**

5. a) If $a \equiv b \pmod m$ & $c \equiv d \pmod m$ then prove that $ac \equiv bd \pmod m$. **5**

b) Find the solution of $x^2 + x + 7 \equiv 0 \pmod{27}$. **5**

c) If a has order $h \pmod m$, b has order $k \pmod m$ & if $(h,k) = 1$ then prove that ab has order hk (mod m). **5**

d) For every positive integer n, prove that $\sigma(n) = \prod_{P^{\alpha} \| n} \left(\frac{p^{\alpha+1} - 1}{p-1}\right)$. **5**

****