

M.Sc.(Mathematics) (New CBCS Pattern) Semester-I
PSCMTH05(D) - Optional Paper - Number Theory

P. Pages : 2

Time : Three Hours



GUG/W/24/13744

Max. Marks : 100

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

UNIT – I

1. a) Let p be a prime number. Then prove that $x^2 \equiv 1 \pmod{p}$ iff $x \equiv \pm 1 \pmod{p}$. 10
- b) State and prove Wilson theorem. 10

OR

- c) If p be a prime number and $p \equiv 1 \pmod{4}$ then show that there exists positive integers a and b such that $a^2 + b^2 = p$. 10
- d) Show that 1763 is composite. 10

UNIT – II

2. a) Solve $x^3 + x^2 - 4 \equiv 0 \pmod{7^3}$. 10
- b) Solve $x^2 + 5x + 24 \equiv 0 \pmod{36}$. 10

OR

- c) Prove that the congruence $f(x) \equiv 0 \pmod{p}$ of degree n has at most n solutions. 10
- d) Show that the congruence $x^5 \equiv 6 \pmod{101}$ has 5 solutions. 10

UNIT – III

3. a) If p is an odd prime and $(a, 2p) = 1$ then show that $\left(\frac{a}{p}\right) = (-1)^t$ where $t = \sum_{j=1}^{(p-1)/2} \left[\frac{ja}{p} \right]$ 10
- b) Prove that if p is an odd prime then $x^2 \equiv 2 \pmod{p}$ has solutions iff $p \equiv 1$ or $7 \pmod{8}$. 10

OR

- c) If p and q are distinct odd primes, then show that **10**

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\{(p-1)/2\}\{(q-1)/2\}}$$
- d) Prove that there are infinitely many primes of each of the forms $3n+1$ and $3n-1$. **10**

UNIT – IV

4. a) Show that $\sum_{d|n} \phi(d) = n$ where n is any positive integer. **10**
- b) Find all integers x and y such that $147x + 258y = 369$ **10**

OR

- c) Find all solution of $999x - 49y = 5000$. **10**
- d) Show that the equation $y^2 = x^3 + 7$ has no solution in integers. **10**
5. a) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then prove that $ac \equiv bd \pmod{m}$. **5**
- b) If $(a, m) = 1$, then show that the order of a modulo m divides $\phi(m)$. **5**
- c) Show that 3 is a quadratic residue of 13 but a quadratic nonresidue of 7. **5**
- d) Show that the equation $15x^2 - 7y^2 = 9$ has no solution in integers. **5**
