K25P 2896

Reg. No. : .....

Name : .....

III Semester M.Sc. Degree (C.B.C.S.S. – O.B.E. – Reg./Supple./Imp.) Examination, October 2025
(2023 Admission Onwards)
MATHEMATICS/MATHEMATICS (MULTIVARIATE CALCULUS AND MATHEMATICAL ANALYSIS, MODELLING AND SIMULATION, FINANCIAL RISK MANAGEMENT)
Elective Course
MSMAT03E01/MSMAF03E01 : Number Theory

Time : 3 Hours Max. Marks : 80

PART – A

Answer **any five** questions from the following six questions. **Each** question carries **4** marks.

1. If $n \geq 1$ prove that $\sum_{d/n} \mu(d) = \left[\frac{1}{n}\right]$.
2. Prove that $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$ for p prime and $\alpha \geq 1$.
3. For every odd prime p, prove that $(-1|p) = (-1)^{p-1/2}$.
4. Solve the congruence : $8x \equiv 7 (\text{mod}) 43$.
5. Prove that 5 is irreducible in Z, yet reducible in $Z\left(\sqrt{5}\right)$.
6. Does the number $\theta = \sqrt{-2}$ is an algebraic number ? Justify your answer.

(5×4=20)

PART – B

Answer **any three** from the following five questions. **Each** question carries **7** marks.

7. Prove the following : The algebraic integers form a subring of the field of algebraic numbers.
8. Prove that the ring of integers of $Q\left(\sqrt[3]{175}\right)$ has no Z basis of the form $\{1, \theta, \theta^2\}$.

P.T.O.

9. Prove that 3 is a primitive root mod p if p is a prime of the form $2^n + 1$, $n > 1$.

10. a) Show that 888 is a quadratic nonresidue of 1999.

    b) Show that 219 is a quadratic residue of 383.

11. a) State and prove Euler-Fermat theorem.

    b) If (a, b) = d, prove that there exist integers x and y such that ax + by = d.

(3×7=21)

PART – C

Answer **any three** questions from the following five questions. **Each** question carries **13** marks.

12. a) Prove the following : for $n \geq 1$, $\frac{\phi(n)}{n} = \prod_{p/n}\left(1 - \frac{1}{p}\right)$.

    b) Prove that the Dirchlet multiplication is commutative and associative.

13. a) Prove the following : The set of lattice points in the plane visible from the origin contains arbitrary large square gaps. That is, given any integer $k > 0$ there exist a lattice point (a, b) such that none of the lattice points (a + r, b +s), $0 < r \leq k$, $0 < s \leq k$, is visible from the origin.

    b) State and prove Wolstenholme's theorem.

14. a) State and prove quadratic reciprocity law.

    b) State and prove Euler's criterion.

15. a) Prove that there are no primitive roots (mod 2^α), $\alpha \geq 3$.

    b) Prove the following : if p is an odd prime and $\alpha \geq 1$ there exist odd primitive roots g modulo p^α. Each such g is also a primitive root modulo $2p^\alpha$.

16. Prove the following :

    a) Every subgroup of H a free abelian group G of rank n is free of rank $s \leq n$. Moreover there exist a basis $u_1, u_2, ..., u_n$ for G and positive integers $\alpha_1, \alpha_2, ..., \alpha_s$ such that $\alpha_1 u_1, \alpha_2 u_2, ..., \alpha_s u_s$ is a basis for H.

    b) If K is a number field then $K = Q(\theta)$.

(3×13=39)

———————