K24P 3339

Reg. No. : ....

Name : ....

III Semester M.Sc. Degree (C.B.S.S. – Supple./Imp.)
Examination, October 2024
(2021 and 2022 Admissions)
MATHEMATICS
MAT3C11 : Number Theory

Time : 3 Hours Max. Marks : 80

PART – A

Answer **any four** questions from Part **A. Each** question carries **4** marks. **(4×4=16)**

1. If (a, b) = 1, then (a + b, a – b) is either 1 or 2.
2. State and prove Euler-Fermat theorem.
3. Determine whether 219 is a quadratic residue or nonresidue mod 383.
4. Prove that m is prime if and only if $\exp_m(a) = m - 1$ for some a.
5. Express the polynomial $t_1^2 + t_2^2 + t_3^2$ in terms of elementary symmetric polynomials.
6. Given $K = \mathbb{Q}(\sqrt[4]{2})$. Find all monomorphisms $\sigma : K \to \mathbb{C}$ and the minimum polynomials (over $\mathbb{Q}$) and field polynomials (over K) of $\sqrt[4]{2}$.

PART – B

Answer **any four** questions from Part **B not** omitting **any** Unit. **Each** question carries **16** marks. **(16×4=64)**

Unit – 1

7. a) Prove that the infinite series $\sum_{n=1}^{\infty} \frac{1}{p_n}$ diverges.

 b) State and prove division algorithm .

P.T.O.

8. a) Show that the set of all arithmetical functions with $f(1) \neq 0$ forms an abelian group with respect to the Dirichlet product.

   b) State and prove Mobius inversion formulae.

9. a) State and prove Lagrange's theorem.

   b) Find all x which simultaneously satisfy the system of congruences.

   $x \equiv 1 \pmod 3$

   $x \equiv 2 \pmod 4$

   $x \equiv 3 \pmod 5$

Unit – 2

10. a) State and prove Euler's criterion.

    b) Determine those odd primes p for which 3 is a quadratic residue and those for which it is a nonresidue.

11. a) Given x be an odd integer. If $\alpha \geq 3$, then prove that

    $x^{\frac{\phi(2^\alpha)}{2}} \equiv 1 \pmod{2^\alpha}$ and there are no primitive roots modulo 2^α.

    b) Given $m \geq 1$, where m is not of the form $m = 1, 2, 4, p^\alpha$ or $2p^\alpha$, where p is an odd prime. Then prove that for any a with $(a, m) = 1$ we have

    $a^{\frac{\phi(m)}{2}} \equiv 1 \pmod m$, so there are no primitive roots mod m.

12. a) Compare private key and public key crypto systems.

    b) Encrypt the message "HAVE A NICE DAY" using caeser ciphar.

Unit – 3

13. a) Let G be a free abelian group of rank n with basis $\{x_1, \ldots, x_n\}$. Suppose (a_{ij}) is an $n \times n$ matrix with integer entries. Then prove that the elements

$$y_i = \sum a_{ij} x_j$$ form a basis of G if and only if a_{ij} is unimodular.

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

14. a) If K is number field then prove that $K = \mathbb{Q}(\theta)$ for some algebraic number θ.

b) Prove that the algebraic integers form a subring of the field of algebraic numbers.

15. a) Prove that the minimum polynomial of $\zeta = e^{\frac{2\pi i}{p}}$, where p is an odd prime. over $\mathbb{Q}$ is $f(t) = t^{p-1} + t^{p-2} + \ldots + t + 1$ and the degree of $\mathbb{Q}(\zeta)$ is $p - 1$.

b) Prove that the ring $\mathfrak{D}$ of integers $\mathbb{Q}(\zeta)$ is $\mathbb{Z}[\zeta]$.
