K23P 1408

Reg. No. : ....

Name : ....

III Semester M.Sc. Degree (CBSS – Reg./Supple./Imp.) Examination, October 2023
(2020 Admission Onwards)
MATHEMATICS
MAT3C11 : Number Theory

Time : 3 Hours Max. Marks : 80

PART – A

Answer **any four** questions from Part **A**. **Each** question carries **4** marks.

1. Prove that if $(a, b) = 1$ then $(a^n, b^k) = 1$ for all $n \geq 1, k \geq 1$.

2. Find all integers such that $\phi(n) = \frac{n}{2}$.

3. Find the quadratic residues and non residue modulo 11.

4. Encrypt the message "RETURN HOME" using caeser ciphar.

5. Define an R-module. Find all submodules of $\mathbb{Z}$-module.

6. Check whether $e^{\frac{2\pi i}{23}}$ is algebraic integer or not ?

PART – B

Answer **any four** questions from Part **B** not omitting **any** Unit. **Each** question carries **16** marks.

Unit – 1

7. a) State and prove fundamental theorem of arithmetic.

   b) Given that a and b are integers with $b > 0$. Then prove that there exists a unique pair of integers q and r such that $a = bq + r$, with $0 \leq r < b$ and $r = 0$ if and only if $b|a$.

8. a) If $n \geq 1$, prove that $\sum_{d|n} \phi(d) = n$.

   b) Assume f is multiplicative. Prove that f is completely multiplicative if and only if $f^{-1}(n) = \mu(n) f(n)$ for all $n \geq 1$.

P.T.O.

9. a) State and prove Chinese remainder theorem.

   b) Find all positive integers n for which $n^{13} \equiv n(\text{mod } 1365)$.

Unit – 2

10. a) State and prove Gauss' lemma.

    b) Define Jacobi symbol and prove that $(-1/p) = (-1)^{\frac{p-1}{2}}$ and $(2/p) = (-1)^{\frac{p^2-1}{8}}$.

11. a) Suppose (a, m) = 1. Prove that a is a primitive root modulo m if and only if the numbers a, a^2, ..., $a^{\phi(m)}$ form a reduced residue system modulo m.

    b) If p is an odd prime and $\alpha \leq 1$ then prove that there exist odd primitive roots g modulo p^α and each such g is also a primitive root modulo $2p^\alpha$.

12. a) Explain RSA public key algorithm with an example.

    b) Obtain all solutions of the knapsack problem
    $28 = 3x_1 + 5x_2 + 11x_3 + 20x_4 + 41x_5$.

Unit – 3

13. a) Given R is a ring. Then prove that every symmetric polynomial in $R[t_1,..., t_n]$ is expressible as a polynomial with coefficients in R in the elementary symmetric polynomials $s_1,..., s_n$.

    b) Let G be a free abelian group of rank r and H is a subgroup of G. Then prove that G/H is finite if and only if the rank of G and H are equal.

14. a) Prove that the set A of algebraic numbers is a subfield of the complex field $\mathbb{C}$.

    b) Prove that a complex number θ is an algebraic integer if and only if the additive group generated by all powers 1, θ, θ^2, ... is finitely generated.

15. a) If d is a square-free rational integer, then prove that the integers of $\mathbb{Q}(\sqrt{d})$ are

    $$\mathbb{Z}\left[\sqrt{d}\right] \quad \text{if} \quad d \not\equiv 1(\text{mod } 4)$$

    $$\mathbb{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{d}\right] \quad \text{if} \quad d \equiv 1(\text{mod } 4)$$

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