K18P 1032

Reg. No. : ....

Name : ....

Third Semester M.Sc. Degree (Reg.) Examination, October 2018
MATHEMATICS
(2017 Admn. Onwards)
MAT3C11 : Number Theory

Time : 3 Hours Max. Marks: 80

PART – A

Answer **any four** questions. **Each** question carries **4** marks.

1. Prove that every number of the form $2^{a-1}(2^a-1)$ is perfect if $2^a - 1$ is prime.
2. Solve the congruence $5x \equiv 3 \pmod{24}$.
3. If p is an odd prime, prove that $\sum_{r=1}^{p-1} r(r|p) = 0$, if $P \equiv 1 \pmod 4$.
4. If $m \geq 1$, $(a, m) = 1$ and $f = \exp_m(a)$, then prove that $a^k \equiv a^h \pmod m$ if and only if $k \equiv h \pmod f$.
5. Let $\mathbb{Z}$ be a $\mathbb{Z}$– module with the obvious action. Find all the submodules.
6. Let $K = \mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/p}$ for a rational prime p. In the ring of integers of $\mathbb{Z}[\zeta]$, show that $\alpha \in \mathbb{Z}[\zeta]$ is a unit if and only if $N_K(\alpha) = \pm 1$. **(4×4=16)**

PART – B

Answer **any four** questions without omitting any Unit. **Each** question carries **16** marks.

Unit – I

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

   b) Define the Euler totient function $\varphi(n)$ and derive a product formula for it.

P.T.O.

8. a) Define the Dirichlet product $f*g$ of two arithmetic functions. If both g and $f*g$ are multiplicative, prove that f is also multiplicative.

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

   c) Prove that $\varphi^{-1}(n) = \sum_{d|n} d\mu(d)$

9. a) State and prove Lagrange's theorem on polynomial congruences.

   b) State the principle of cross classification. Given integers r, d and k such that $d|k$, $d > 0$, $k \geq 1$ and $(r, d) = 1$. Then prove that the number of elements of the set $S = \{r + td : t = 1, 2, ..., k/d\}$ which are relatively prime to k is $\varphi(k)/\varphi(d)$.

Unit – II

10. a) State and prove the quadratic reciprocity law.

    b) Determine whether 219 is a quadratic residue or non-residue modulo 383.

11. a) Let p be an odd prime and let d be any positive divisor of $p - 1$. Prove that in every reduced residue system modulo p there are $\varphi(d)$ numbers a such that $\exp_p(a) = d$.

    b) If $\alpha \geq 3$, prove that there are no primitive roots mod 2^α.

12. a) Encipher the message HAVEANICETRIP using a Vigenere cipher with the keyword MATH.

    b) The ciphertext ALXWU VADCOJO has been enciphered with the cipher

    $C_1 \equiv 4P_1 + 11P_2 \pmod{26}$, $C_2 \equiv 3P_1 + 8P_2 \pmod{26}$. Derive the plain text.

    c) Find the unique solution of the knapsack problem

    $51 = 3x_1 + 5x_2 + 9x_3 + 18x_4 + 37x_5$.

Unit – III

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. Prove that the elements $y_i = \sum_{j=1}^{n} a_{ij} x_j$, $(i = 1, \ldots, n)$ form a basis of G if and only if (a_{ij}) is unimodular.

    b) Prove that every subgroup H of a free abelian group of rank n is free of rank $s \leq n$.

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

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

15. a) Prove that the ring of integers of the cyclotomic field $\mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/p}$, p an odd prime is $\mathbb{Z}[\zeta]$.

    b) Prove that the discriminant of $\mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/p}$, p an odd prime is $(-1)^{(p-1)/2} p^{p-2}$. **(4×16=64)**

____