0150328

K19P 1186

Reg. No. : ....

Name : ....

III Semester M.Sc. Degree (CBSS-Reg./Suppl./Imp.)
Examination, October - 2019
(2017 Admission Onwards)
Mathematics
MAT3C11 : NUMBER THEORY

Time : 3 Hours Max. Marks : 80

PART - A

Answer any **Four** questions. Each question carries 4 marks. (4×4=16)

1. Prove the following statement or exhibit a counter example: if F is multiplicative, then $F(n) = \prod_{d|n} f(d)$ is multiplicative.
2. If n > 1 and $(n-1)! + 1 \equiv 0 \pmod{n}$, then prove that n is a prime.
3. Find the quadratic residues and nonresidues module 13.
4. If P and Q are odd positive integers, then prove that $(n \mid PQ) = (n|P)(n|Q)$.
5. State Newton's theorem on symmetric polynomials. Express the polynomial $t_1^3 + t_2^3$ in terms of elementary symmetric polynomial in t_1, t_2.
6. Show that an algebraic integer is a rational number if and only if it is a rational integer.

PART - B

Answer any **Four** questions without omitting any unit. Each question carries 16 marks. (4×16=64)

UNIT - I

7. a) State and prove the Euclidean algorithm.
   b) Define Euler function $\varphi(n)$ and derive a product formula for. $\varphi(n)$.
   c) Prove that $\varphi(n)$ is even for $n \geq 3$.

P.T.O.

8. a) If f and g are multiplicative, prove that so is their Dirichlet product $f * g$.

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) With usual notations, prove that $\varphi^{-1}(n) = \prod_{P|n}(1-P)$.

9. a) Assume $(a, m) = d$ and $d|b$. Prove that the linear congruence $ax \equiv b \pmod m$ has exactly d solutions modulo m.

b) Solve the congruence $25x \equiv 15 \pmod{120}$.

c) Let $P \geq 5$ be a prime and wirte $1+\frac{1}{2}+\frac{1}{3}+....+\frac{1}{P}=\frac{r}{PS}$. Then prove that $P^3|r-s$.

UNIT - II

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

b) Determine whether 888 is a quadratic residue or nonresidue of the prime 1999.

11. a) Let p be an odd prime. Prove that there exists at least one primitive root mod p^α if $\alpha \geq 2$.

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. Prove that there are no primitive roots mod m.

12. a) Using the linear cipher $C \equiv 5P + 11 \pmod{26}$, encrypt the message NUMBER THEORY is EASY.

b) Decrypt the message FDHVDU ZDV JUHDV which was enciphered using the caesar cipher.

c) Solve the knapsack problem $118 = 4x_1 + 5x_2 + 10x_3 + 20x_4 + 41x_5 + 99x_6$.

UNIT - III

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

b) Let θ be a complex number satisfying a monic polynomial equation whose coefficients are algebraic integers. Them prove that θ is an algebraic integer.

14. a) Prove that every number field K possesses an integral basis, and the additive subgroup of the ring of integers of K is free abelian of rank n equal to the degree of K.

b) Compute an integral basis and discriminant of $Q(\sqrt{2},\sqrt{3})$.

15. a) Let d be a squarefree rational integer. Prove that the integers of $Q(\sqrt{d})$ are

i) $\mathbb{Z}[\sqrt{d}]$ if $d \not\equiv 1 \pmod 4$

ii) $\mathbb{Z}\left[\frac{1}{2}+\frac{1}{2}\sqrt{d}\right]$ if $d \equiv 1 \pmod 4$

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