K16P 1043

Reg. No. :

Name :

Third Semester M.A./M.Sc./M.Com. Degree (Reg./Supple./Imp.)

Examination, November 2016

MATHEMATICS

MAT 3 C 11 : Number Theory

(2014 Admission Onwards)

Time: 3 Hours

A Prove that the page of integrals of K is ALS.

Max. Marks: 60

PART-A

Answer any four questions from this Part. Each question carries 3 marks.

- 1. If (a, b) = 1, prove that $(a + b, a^2 ab + b^2)$ is either 1 or 3.
- 2. Prove that the Mobius function is multiplicative but not completely multiplicative.
- 3. Find the quadratic residues and non residues modulo 13.
- 4. Define a primitive root modulo m and show that 2 is a primitive root modulo 11.
- 5. Express the polynomials in terms of the elementary symmetric polynomials

i)
$$t_1^2 + t_2^2 + t_3^2$$
 (n = 3) ii) $t_1^3 + t_2^3$ (n = 2)

6. Let $K = Q(\xi)$, where $\xi = e^{2\pi i/5}$. Calculate $N_K(\alpha)$ and $T_K(\alpha)$ where $\alpha = \xi + \xi^2$.

PART-B

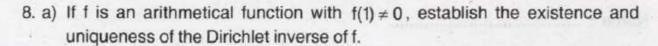
Answer any four questions from this Part without omitting any Unit. Each question carries 12 marks.

Unit - I

- 7. a) Prove that every integer n > 1 is either a prime or a product of prime numbers.
 - b) Prove that $n^4 + 4$ is composite if n > 1.
 - c) State and prove the fundamental theorem of arithmetic.







- b) If both g and the Dirichlet product f * g are multiplicative, prove that f is multiplicative. Deduce that the Dirichlet inverse of a multiplicative function is multiplicative.
- 9. a) State and prove Lagrange's theorem on polynomial congruences.
 - b) For any prime $p \ge 5$, prove that $\sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0 \pmod{p^2}$.

Unit - II

- 10. a) If p is an odd prime, then prove that for all n, $(n \mid p) \equiv n^{(p-1)/2} \pmod{p}$.
 - b) State the quadratic reciprocity law and apply it to determine those odd primes p for which 3 is a quadratic residue and those for which it is a non residue.
- 11. a) Prove that there are no primitive roots mod 2^{α} if $\alpha \ge 3$.
 - b) Let p be an odd prime. If g is a primitive root mod p then prove that g is also a primitive root mod p^{α} for all $\alpha \ge 1$ if and only if $g^{p-1} \not\equiv 1 \pmod{p^2}$.
- 12. a) Use the Hill cipher $C_1 \equiv 5P_1 + 2P_2 \pmod{26}$

$$C_2 \equiv 3P_1 + 4P_2 \pmod{26}$$

to encipher the message GIVE THEM TIME.

Explain how the encryption key (n, k) is selected in the RSA cryptosystem.
 Also explain the encryption and decryption procedure of this cryptosystem.

Unit - III

- a) Prove that every subgroup H of a free abelian group G of rank n is free of rank s ≤ n.
 - b) Prove that every finitely generated abelian group with n generators is the direct product of a finite abelian group and a free group of k generators where $k \le n$.



- a) Prove that the set B of algebraic integers form a subring of the field A of algebraic numbers.
 - b) Prove that every number field K possesses an integral basis, and the additive group of the ring of integers of K is free abelian of rank n equal to the degree of K.
- 15. Let $K = Q(\xi)$, where $\xi = e^{2\pi i/p}$ and p is an odd prime.
 - a) Prove that the ring of integers of K is $\mathbb{Z}[\xi]$
 - b) Prove that $\alpha \in \mathbb{Z}[\xi]$ is a unit if and only if $N_{\kappa}(\alpha) = \pm 1$.