[This question paper contains 4 printed pages.]

Your Roll No.....

E

Sr. No. of Question Paper : 4873

Unique Paper Code : 32357610

Name of the Paper : DSE-4 (Number Theory)

Name of the Course : **CBCS (LOCF) – B.Sc. (H) (Mathematics)**

Semester : VI

Duration : 3 Hours

Maximum Marks : 75

Instructions for Candidates

1. Write your Roll No. on the top immediately on receipt of this question paper.
2. **All** questions are compulsory.
3. Attempt any **two** parts of each question.
4. Question Nos. **1** to **3**, each part carries **6.5** marks and Question Nos. **4** to **6**, each part carries **6** marks.

1. (a) Determine all solutions in the positive integers of the Diophantine equation

$$18x + 5y = 48.$$

P.T.O.

(b) Using Euclidean algorithm and theory of linear Diophantine equation, divide 100 into two summands such that one is divisible by 7 and other by 11.

(c) Write a short note on Prime number theorem.

(d) If $ca \equiv cb \pmod{n}$ then prove that $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

2. (a) Verify that $0, 1, 2, 2^2, 2^3 \ldots\ldots 2^9$ form a complete set of residues modulo 11, but that $0, 1^2, 2^2, 3^2 \ldots\ldots 10^2$ do not.

(b) Find the solutions of the system of congruences :

$3x + 4y \equiv 5 \pmod{13}$

$2x + 5y \equiv 7 \pmod{13}$.

(c) Use Fermat's theorem to verify that 17 divides $11^{104} + 1$.

(d) Find the remainder when $2(26!)$ is divided by 29.

3. (a) Let F and f be two number – theoretic functions related by the formula

$$F(n) = \sum_{d/n} f(d)$$

Prove $f(n) = \Sigma_{d|n}\mu(d)F(n/d) = \Sigma_{d|n}\mu(n/d)F(d)$.

(b) Verify that 1000! terminates in 249 zeros.

(c) Use Euler's theorem for any integer a, to prove that $a^{13} \equiv a \pmod{2730}$

(d) Prove that $\emptyset(2^n - 1)$ is a multiple of n for any $n > 1$.

4. (a) For any positive integer n, prove

$\emptyset(n) = n\Sigma_{d|n}\mu(d)/d$.

(b) Define primitive roots of an integer by an example and show that if $F_n = 2^{2^n} + 1$, $n > 1$, is a prime then 2 is not a primitive root of F_n.

(c) If p is a prime number and d|p–1, then show that there are exactly $\varphi(d)$ incongruent integers having order d modulo p.

(d) Determine all the primitive roots of the primes $p = 11, 19$, and 23, expressing each as a power of one of the roots.

P.T.O.

5. (a) If gcd (m, n) = 1, where $m > 2$ and $n > 2$, then prove that the integer 'mn' has no primitive roots.

(b) Solve the quadratic congruence

$3x^2 + 9x + 7 \equiv 0 \pmod{13}$.

(c) Show that 3 is quadratic residue of 23, but a nonresidue of 31.

(d) Prove that there are infinitely many primes of the form 4k+1.

6. (a) Find the value of Legendre symbol (1234/4567).

(b) Solve the quadratic congruence

$x^2 \equiv 23 \pmod{7^3}$.

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

(d) When the RSA algorithm is based on the key (n, k) = (3233, 37), what is the recovery exponent for the cryptosystem?