Name of Course	: **CBCS B.Sc. (H) Mathematics**
Unique Paper Code	: **32357610**
Name of Paper	: **DSE4: Number Theory**
Semester	: **VI**
Duration	: **3 hours**
Maximum Marks	: **75 Marks**

Attempt any four questions. All questions carry equal marks.

1. Using the theory of linear Diophantine Equation, divide 299 into two summands such that one is divisible by 12 and the other by 17.

If p is an odd prime divisor of (n^2+1), then prove that $p \equiv 1 \pmod 4$.

Find all primitive Pythagorean triples x, y, z in which x = 20.

2. Solve the following set of simultaneous congruences:

$x \equiv -1 \pmod{27}$

$x \equiv -2 \pmod{16}$

$x \equiv 0 \pmod{25}$

Using the theory of congruences show that the sum $1^5 + 2^5 + 3^5 + 4^5 + \ldots\ldots\ldots\ldots\ldots + 100^5$ is divisible by 4.

3. Mobius pair is a pair of functions {f(n), g(n)} such that $f(n) = \sum_{d|n} g(d)$ where the sum runs over all positive divisors of the positive integer n. Prove that if one of the functions of the Mobius pair is multiplicative, then so is the other.

Using the Mobius Inversion formula, deduce that for all n>=1,

$\sum_{d|n} \mu\left(\frac{n}{d}\right) \tau(d) = 1$ and $\sum_{d|n} \mu\left(\frac{n}{d}\right) \sigma(d) = n$

4. Find the last two digits in decimal representation of 13^{1010} .

Find the sum of positive integers less than 1001 and relatively prime to 1001.

Also show that $\frac{(a+b)!}{a!\,b!}$ is an integer for any positive integers a and b.

5. Find all positive integers less than 37 having order 6 (mod 37).

Determine whether the quadratic congruence $x^2 \equiv -72 \pmod{131}$ is solvable.

Find all odd primes $p \neq 3$ having 3 as quadratic residue.

6. The ciphertext VKYAQ VAKEC has been enciphered with the Linear Cipher

$$C \equiv 17P + 10 \pmod{26}$$

Derive the plaintext. When the RSA algorithm is based on the key (n, k) = (2419, 11), what is the recovery exponent for the cryptosystem?