October 2025
B.A./B.Sc.
Fifth Semester
DISCIPLINE SPECIFIC ELECTIVE – 1
MATHEMATICS
Course Code: MAD 5.11
(Number Theory)

Total Mark: 70 *Pass Mark: 28*
Time: 3 hours

Answer five *questions, taking* one *from each unit.*

UNIT–I

1. (a) Solve the linear Diophantine equation $24x + 138y = 18$ and describe all integer solutions. 5

   (b) Show that: 2½+2½=5

   (i) The only prime of the form $n^3 - 1$ is 7.

   (ii) Any integer of the form $8^n + 1$, where $n \geq 1$, is composite.

   (c) Find the remainder when $1^5 + 2^5 + 3^5 + \cdots ... + 99^5 + 100^5$ is divided by 4. 4

2. (a) Solve using the Chinese remainder theorem, $x \equiv 5 (\text{mod} 11)$, $x \equiv 14 (\text{mod} 29)$, $x \equiv 15 (\text{mod} 31)$. 5

   (b) For any integer a, verify that a^5 and a have the same unit digit. 4

   (c) Show that the quadratic congruence $x^2 + 1 \equiv 0 (\text{mod } p)$, where p is an odd prime, has a solution if and only if $p \equiv 1 (\text{mod } 4)$. 5

UNIT–II

3. (a) Prove that the function τ and σ are both multiplicative functions. 4

   (b) Establish the following assertions: 3×2=6

   (i) For any positive integer n, $\frac{\sigma(n!)}{n!} \geq 1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n}$

(ii) If $n>1$ is a composite number, then $\sigma(n)>n+\sqrt{n}$

(c) For each positive integer *n*, show that
$\mu(n)\cdot\mu(n+1)\cdot\mu(n+2)\cdot\mu(n+3)=0$. 4

4. (a) Prove that $\sigma(n)$ is an odd integer if and only if *n* is a perfect square or twice a perfect square. 5

(b) For any positive integer *n*, prove that $\sum_{d|n}\tau(d)^3=\left(\sum_{d|n}\tau(d)\right)^2$. 4

(c) Define the Mangoldt function Λ. Prove that
$\Lambda(n)=\sum_{d|n}\mu(d)\log\frac{n}{d}$. 5

UNIT–III

5. (a) Let *x* and *y* be real numbers. Prove that: 3+3=6

(i) $[x+n]=[x]+n$, for any integer *n*

(ii) $[nm/k]\geq n[m/k]$ for positive integer *n*, *m*, *k*.

(b) Verify that 1000! terminates in 249 zeros. 4

(c) Prove that the equation $\phi(n)=\phi(n+2)$ is satisfied by $n=2(2p-1)$, whenever *p* and $2p-1$ are both odd primes. 4

6. (a) If *m* and *n* are relatively prime positive integers, prove that
$m^{\phi(n)}+n^{\phi(m)}\equiv 1(\text{mod } mn)$. 5

(b) Find the units digit of 3^{100} by means of Euler's theorem. 4

(c) If *n* is a square-free integer, prove that $\sum_{d|n}\sigma(d^{k-1})\phi(d)=n^k$ for all integers $k\geq 2$. 5

UNIT–IV

7. (a) If the integer *a* has order *k* modulo *n*, then prove that
$a^i\equiv a^j(\text{mod } n)$ if and only if $i\equiv j(\text{mod } n)$. 4

(b) Prove that $\phi(2^n-1)$ is a multiple of *n* for $n>1$. 4

(c) If p is an odd prime, prove that: 6

(i) The only incongruent solutions of $x^2 \equiv 1 \pmod{p}$ are 1 and $p-1$

(ii) The congruence $x^{p-2} + \ldots + x^2 + x + 1 \equiv 0 \pmod{p}$ has exactly $p-2$ incongruent solutions, and they are the integers 2, 3, …, $p-1$.

8. (a) Prove that if $\gcd(m,n)=1$, where $m>2$ and $n>2$, then the integer mn has no primitive roots. 5

(b) Find the index of 5 relative to each of the primitive roots of 13. 4

(c) Let p be an odd prime and $\gcd(a,p)=1$. Prove that a is a quadratic residue of p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$. 5

UNIT–V

9. (a) 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 plaintext. 6

(b) Prove that the Diophantine equation $x^4 - y^4 = z^2$ has no solution in positive integers x, y, z. 8

10. (a) Encrypt the plaintext message GOLD MEDAL using the RSA algorithm with key (2561,3). 6

(b) Verify that the only solution in relatively prime positive integers of the equation $x^4 + y^4 = 2z^2$ is $x = y = z = 1$. 8