2022

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) Find the remainder when the $1^5+2^5+3^5+\ldots+99^5+100^5$ is divided by 4? 4

   (b) Determine all solutions in the positive integers of the Diophantine equation $54x+21y=906$. 5

   (c) State and prove the Wilson's theorem. 1+4=5

2. (a) Prove that there are infinite number of primes. 4

   (b) Find a number that leaves the remainders 2, 3, 2 when divided by 3, 5, 7 respectively. 5

   (c) Using Fermat's theorem, if p is an odd prime, prove that 5

   $$1^{p-1}+2^{p-1}+3^{p-1}+\ldots+(p-1)^{p-1}=-1(\text{mod } p)$$

UNIT–II

3. (a) Prove that for each positive integer $n\geq 1$, 4

   $$\sum_{d|n}\mu(d)=\begin{cases}1 & \text{if } n=1\\ 0 & \text{if } n>1\end{cases}$$

   where d runs through the positive divisors on n.

   (b) If $n=p_1^{k_1}p_2^{k2}\ldots p_r^{k_r}$ is the prime factorization of $n>1$, then prove that $\sigma(n)=\left(\dfrac{p_1^{k_1+1}-1}{p_1-1}\right)\left(\dfrac{p_2^{k_2+1}-1}{p_2-1}\right)\ldots\left(\dfrac{p_r^{k_r+1}-1}{p_r-1}\right)$. 5

(c) Prove that the Dirichlet product is commutative as well as associative. 5

4. (a) For each positive integer n, show that

$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3)=0$ 4

(b) If f and g are multiplicative functions, prove that their Dirichlet product $f*g$ is also multiplicative. 5

(c) Define the Möbius μ-function and prove that the function μ is a multiplicative function. 1+4=5

UNIT–III

5. (a) For $n>2$, prove that $\phi(n)$ is an even integer. 4

(b) Let f and F be number-theoretic functions such that

$F(n)=\sum_{d|n} f(d)$. Prove that $\sum_{n=1}^{N} F(n)=\sum_{k=1}^{N} f(k)\left[\frac{N}{k}\right]$. 5

(c) Using Euler's theorem, evaluate $2^{100000} \pmod{77}$. 5

6. (a) Let x and y be real numbers. Prove that $[x]+[y]\leq[x+y]$. 4

(b) For each positive integer $n \geq 1$, prove that $n=\sum_{d|n}\phi(d)$, the sum being extended over all the positive divisors of n. 5

(c) For $n>1$, prove that the sum of the positive integers less than n and relatively prime to n is $\frac{1}{2}n\phi(n)$. 5

UNIT–IV

7. (a) Determine if the congruence $x^2 \equiv -46 \pmod{17}$ is solvable. 4

(b) Find the four primitive roots of 26 and the eight primitive roots of 25. 5

(c) If p is an odd prime, then prove that $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)=0$. 5

8. (a) Evaluate the following Legendre symbols: 2×2=4

(i) $\left(\frac{-219}{383}\right)$ (ii) $\left(\frac{29}{53}\right)$

(b) If $\gcd(m,n)=1$, where $m>2, n>2$, then the integer mn has no primitive roots. 5

(c) Prove that there are infinitely many primes of the form $4k+1$. 5

UNIT–V

9. (a) The ciphertext *ALXWU VADCOJO* has been enciphered with the cipher

$$C_1 = 4P_1 + 11P_2 \pmod{26}$$

$$C_2 = 3P_1 + 8P_2 \pmod{26}$$

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) Prove that all the solutions of the Pythagorean equation $x^2 + y^2 = z^2$ satisfying the conditions

$$\gcd(x,y,z)=1,\ 2\mid x,\ x>0,\ y>0, z>0$$

are given by

$$x = 2st,\ \ y = s^2 - t^2,\ \ z = s^2 + t^2$$

for integers $s>t>0$ such that $\gcd(s,t)=1$ and $s \not\equiv t \pmod 2$. 8