2023
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) Prove that the linear Diophantine equation $ax + by = c$ has a solution if and only if $d|c$, where $d = gcd(a, b)$. If x_0, y_0 is any particular solution, derive a formula to obtain all the other solutions. 3+2=5

   (b) If p and q are distinct primes with $a^p \equiv a \pmod{q}$ and $a^q \equiv a \pmod{p}$, prove that $a^{pq} \equiv a \pmod{pq}$. 5

   (c) If $ca \equiv cb \pmod{n}$, then show that $a \equiv b\left(\mathrm{mod}\ \frac{n}{d}\right)$, where $d = gcd(c, n)$. 4

2. (a) Solve the linear congruence $140x \equiv 133 \pmod{301}$. 5

   (b) If p is an odd prime, prove that $1^p + 2^p + \ldots + (p-1)^p \equiv 0 \pmod{p}$. 5

   (c) If p is a prime and $p|ab$, then prove that $p|a$ or $p|b$. 4

UNIT–II

3. (a) If f is a multiplicative function and F is defined by $F(n) = \sum_{d|n} f(d)$, then show that F is also multiplicative. 5

(b) If both g and the Dirichlet product of f and g, $f * g$, are multiplicative, then prove that f is also multiplicative. 5

(c) Show that the functions τ and σ are multiplicative functions. 4

4. (a) If F and f are two number theoretic functions related by the formula

$F(n) = \sum_{d|n} f(d)$, then show that $F(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$. 5

(b) If n is a square free integer, prove that $\tau(n) = 2^r$, where r is the number of prime divisors of n. 5

(c) The Liouville λ-function is defined by $\lambda(1) = 1$ and

$\lambda(n) = (-1)^{k_1+k_2+\ldots+k_r}$, if the prime factorization of n is

$n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$. Prove that λ multiplicative. 4

UNIT–III

5. (a) If n and r are positive integers with $1 \leq r \leq n$, then prove that the binomial coefficient ${}^nC_r$ is also an integer. 5

(b) If $n \geq 1$ and $gcd(a, n) = 1$, then prove that $a^{\phi(n)} \equiv 1 \pmod{n}$. 5

(c) Show that if $gcd(a, n) = gcd(a-1, n) = 1$, then

$1 + a + a^2 + \ldots + a^{\phi(n)-1} \equiv 0 \pmod{n}$. 4

6. (a) If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{kr}$,

then show that $\sum_{d|n} \mu(d)\phi(d) = (2-p_1)(2-p_2)\ldots(2-p_r)$. 5

(b) Prove that $n = \sum_{d|n} \phi(d)$, for each positive integer $n \geq 1$. 5

(c) For what value of n does $n!$ terminate in 37 zeros? 4

UNIT–IV

7. (a) If the integer a has order k modulo n and $h > 0$, then prove that the

order of a^h modulo n is $\dfrac{k}{\gcd(h,k)}$. 5

(b) Show that the integer 2^k has no primitive roots for $k \geq 3$. 5

(c) Evaluate the Legendre symbol $\left(\frac{-219}{383}\right)$ and the Jacobi symbol $\left(\frac{21}{221}\right)$. 4

8. (a) If p is an odd prime, then show that

$$\left(\frac{2}{p}\right)=\begin{cases}1 & \text{if } p\equiv 1 \pmod 8 \text{ or } p\equiv 7 \pmod 8\\ -1 & \text{if } p\equiv 3 \pmod 8 \text{ or } p\equiv 5 \pmod 8\end{cases}$$ 5

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

(c) If p is an odd prime, show that $x^{p-2}+x^{p-3}+\ldots+x+1\equiv 0 \pmod p$ has exactly $p-2$ incongruent solutions. 4

UNIT–V

9. (a) The ciphertext BS FMX KFSGR JAPWL is known to have resulted from a Vigenere cipher whose keyword is YES. Obtain the deciphering congruences and write the message. 5

(b) Prove that the radius of the inscribed circle of a Pythagorean triangle is always an integer. 5

(c) If x, y, z is a primitive Pythagorean triple, prove that $x + y$ and $x - y$ are congruent modulo 8 to either 1 or 7. 4

10. (a) The ciphertext message produced by the RSA algorithm with key (n, k) = (2573, 1013) is 0464 1472 0636 1262 2111. Determine the original message. 5

(b) Prove that the area of a Pythagorean triangle can never be equal to a perfect (integral) square. 5

(c) If x, y, z is a primitive Pythagorean triple, then one of the integers x or y is even, while the other is odd. 4