November 2025
M.Sc.
Third Semester
DISCIPLINE SPECIFIC ELECTIVE – 01
MATHEMATICS
Course Code: MMAD 3.11 (B)
(Number Theory)

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

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

UNIT–I

1. (a) State and prove the division algorithm. 5
   (b) For integers a, b, c, prove that: 5
   (i) $a \mid 0,\ 1 \mid a,\ a \mid a$
   (ii) $a \mid 1$ if and only if $a = \pm 1$
   (iii) If $a \mid b$ and $b \mid c$, then $a \mid c$
   (iv) If $a \mid b$ and $c \mid d$, then $ac \mid bd$
   (c) Using the division algorithm, prove that: 4
   (i) The square of any integer is either of the form $3k$ or $3k + 1$
   (ii) $3a^2 - 1$ is never a perfect square

2. (a) State and prove the Chinese remainder theorem and find the solution of the following system of congruences using Chinese remainder: 6

$$\begin{cases} x \equiv 5 \pmod{4} \\ x \equiv 3 \pmod{7} \\ x \equiv 2 \pmod{9} \end{cases}$$

   (b) State and prove Fermat's little theorem. 4
   (c) Using Fermat's theorem, prove that: 4
   $1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots + (p-1)^{p-1} \equiv -1 \pmod{p}$, and show that
   $1^{p} + 2^{p} + 3^{p} + \ldots + (p-1)^{p} \equiv 0 \pmod{p}$, where p is an odd prime.

UNIT–II

3. (a) If $(a,m)=1$ and let the integer a have order k modulo n. Then prove that $a^h \equiv 1(\bmod n)$ if and only if $k \mid j$. Also, find the order of the integer 2 of modulo 17 and modulo 19. 5

(b) State quadratic residue and quadratic non-residue. Also, prove that the necessary and sufficient condition that a is a non-quadratic residue of (mod m), where m is an odd prime $(a,m)=1$, is $a^{\frac{m-1}{2}} \equiv -1(\bmod m)$. 5

(c) If m is an odd prime and a, b are two integers such that $(a,m)=(b,m)=1$, then show that: 4

(i) $\left(\frac{a}{m}\right) \equiv a^{\frac{m-1}{2}}(\bmod m)$

(ii) $\left(\frac{-1}{m}\right) = \begin{cases} 1, & \text{when } m \equiv 1(\bmod 4) \\ -1, & \text{when } m \equiv 3(\bmod 4) \end{cases}$

4. (a) State and prove Gauss' lemma. If m, n be any two distinct odd primes, then prove that $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2} \times \frac{n-1}{2}}$. 5

(b) Examine whether the quadratic congruence $x^2 \equiv 219(\bmod 419)$ is solvable. 4

(c) Define binary quadratic form and prove that if $f(x,y) = ax^2 + bxy + cy^2$ with discriminant $d = b^2 - 4ac \neq 0$, then $a \neq 0$, $c \neq 0$ then the only solution of the equation $f(x,y) = 0$ in the integer is given by $x = y = 0$. 5

UNIT–III

5. (a) Solve the Diophantine equation $35x + 22y = 1$ and find all integer solutions. 5

(b) Prove that every Pythagorean triple (x,y,z) can be expressed as $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$, where $m > n$ are positive integers. 5

(c) Find five prime numbers p such that $p = n^2 + (n+1)^2$ for some positive integer n. 4

6. (a) State and prove the necessary and sufficient condition for the linear Diophantine equation $ax + by = c$ to have integer solutions. 5

(b) Define primitive Pythagorean triple. Find all primitive Pythagorean triples x, y, z for $x = 40$. 1+3=4

(c) Find all integer solutions of the simultaneous equations: 5

$$\begin{cases} 2x + 3y = 7 \\ 3x + 4y = 10 \end{cases}$$

UNIT–IV

7. (a) Define the Farey sequence of order n and prove that two successive terms $\frac{a}{b}$ and $\frac{c}{d}$ satisfy $bc - ad = 1$. 5

(b) Prove that between any two distinct rational numbers, there exists an irrational number. 5

(c) Prove that for any irrational number $0 < x < 1$ and integer $n > 0$, there exists a fraction $\frac{u}{v}$ in F_n such that $\left| x - \frac{u}{v} \right| < \frac{1}{v(n+1)}$. 4

8. (a) Establish the Binet's formula for $u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ and show that $u_{n+2}^2 - u_n^2 = u_{2n+2}$. 6

(b) Show that the sum of the squares of the first n^{th} Fibonacci is $u_1^2 + u_2^2 + u_3^2 + \ldots + u_n^2 = u_n u_{n+1}$. 4

(c) If $n \geq 2$ and $m = n^{13} - n$. Show that u_m (m^{th} Fibonacci number) is divisible by 30290. 4

UNIT–V

9. (a) Define simple continued fractions and show that every rational number can be expressed as a finite continued fraction. 5

(b) Find the simple continued fraction expansion of $\sqrt{19}$. 5

(c) Prove that if $\alpha = [a_0, a_1, a_2, ...]$, then its convergents provide the best rational approximations to α. 4

10. (a) State Pell's equation and find all integer solutions of $x^2 - 2y^2 = 1$. 5

(b) State Hurwitz's theorem and discuss its application in the approximation of irrational numbers. 5

(c) Show that the continued fraction expansion of $\sqrt{N}$ is periodic for non-square positive integers *N*. 4
