 Student's Copy

2025

(CBCS)

(6th Semester)

MATHEMATICS

TWELFTH (B) PAPER

(Elementary Number Theory)

Full Marks : 75

Time : 3 hours

The figures in the margin indicate full marks for the questions

(SECTION : A—OBJECTIVE)

(*Marks* : 10)

Tick ☑ the correct answer in the boxes provided : 1×10=10

1. The last digit of 2024^{2025} is
   - *(a)* 2 ☐
   - *(b)* 4 ☐
   - *(c)* 6 ☐
   - *(d)* 8 ☐

2. For positive integers m and n, let $m > n$ be such that $\gcd(m, n) = 1$. Which of the following statements is true?
   - *(a)* $\gcd(m-n, m+n) = 1$ ☐
   - *(b)* $\gcd(m-n, m+n)$ can have a prime divisor ☐
   - *(c)* $\gcd(m-n, m+n)$ can be an odd prime ☐
   - *(d)* None of the above ☐

3. Which of the following is a reduced residue system modulo 17?

(a) $\{0, 1, 3, 10, 9, 7, 6, 13\}$ ☐

(b) $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$ ☐

(c) $\{-24, -23, -22, -21, -20, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26\}$ ☐

(d) $\{-24, -23, -22, -21, -20, -19, 16, 18, 19, 20, 21, 22, 23, 24, 25, 26\}$ ☐

4. Let A be the set of polynomials $f(x)$ with integer coefficient satisfying

$$f(x) = 1(\text{mod } x-1) \text{ and } f(x) \equiv 0(\text{mod } x-3)$$

Which of the following statements is true?

(a) The set A is empty ☐

(b) A is a singleton set ☐

(c) A is a non-empty finite set ☐

(d) A is countably infinite ☐

5. The value of $\phi(48756)$ is

(a) 15233 ☐

(b) 15232 ☐

(c) 15436 ☐

(d) 7616 ☐

6. Which of the following are primitive roots of 9?

(a) 2 and 7 ☐

(b) 5 and 6 ☐

(c) 2 and 5 ☐

(d) 2, 3 and 5 ☐

7. Let p be an odd prime and $\left(\frac{a}{p}\right)$ denotes the Legendre symbol. Then

(a) $\left(\frac{a}{p}\right) \equiv a^{p-1} \pmod p$ ☐

(b) $\left(\frac{a}{p}\right) \equiv a^{p} \pmod p$ ☐

(c) $\left(\frac{a}{p}\right) \equiv a^{\frac{p}{2}} \pmod p$ ☐

(d) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$ ☐

8. If $a = 29$ and $p = 53$, then the Legendre symbol $\left(\frac{29}{53}\right)$ is equal to

(a) 1 ☐

(b) −1 ☐

(c) 0 ☐

(d) None of the above ☐

9. Let $\tau(n)$ denotes the number of positive divisors of n. Then $\tau(8736)$ is

(a) 12 ☐

(b) 30 ☐

(c) 48 ☐

(d) 55 ☐

10. Let u_n denote the nth Fibonacci number and $2 | u_n$. Then

(a) $4 | u_{n+1} - u_{n-1}$ ☐

(b) $4 | u_{n+1}^2 - u_{n-1}^2$ ☐

(c) $8 | u_{n+1}^2 - u_{n-1}^2$ ☐

(d) $2 | u_{n+2} - u_{n-2}$ ☐

(SECTION : B—SHORT ANSWERS)

(*Marks* : 15)

Answer the following : $3 \times 5 = 15$

UNIT—I

1. Using the Euclidean algorithm, find the greatest common divisor of 48756 and 7635.

OR

2. Let $a, b, c \in \mathbb{Z}$. If $a|c$ and $b|c$, with $\gcd(a, b) = 1$, then prove that $ab|c$.

UNIT—II

3. Prove that there are infinitely many primes.

OR

4. Consider the set $M = \{r, m + r, 2m + r, 3m + r, 4m + r, \cdots, (n-1)m + r\}$, then show that the set M forms a complete residue system modulo n if $\gcd(m, r) = 1 = \gcd(m, n)$.

UNIT—III

5. Find the remainder when 15! is divided by 17.

OR

6. If n has a primitive root, then show that it has exactly $\phi(\phi(n))$ of them.

UNIT—IV

7. Calculate the value of the Legendre symbol $\left(-\frac{46}{17}\right)$.

OR

8. Let $a, n \in \mathbb{Z}$ with $n > 0$. Prove that there exists an integer solution for the linear congruence $ax \equiv 1 \pmod{n}$ if and only if $\gcd(a, n) = 1$.

UNIT—V

9. For each positive integer n, show that

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

OR

10. Calculate the value of $\sigma(789)$, where $\sigma(n)$ is the sum of all positive divisors of n.

(SECTION : C—DESCRIPTIVE)

(*Marks* : 50)

Answer the following : 10×5=50

UNIT—I

1. *(a)* Find the integers x and y such that $\gcd(456,266) = 456x + 266y$. 5

(b) If p_n is the nth prime number, then prove that $p_n \le 2^{2^{n-1}}$. 5

OR

2. *(a)* State and prove the division algorithm for any integers a and $b > 0$. 7

(b) For any integer $a > 0$ and $b, c \in \mathbb{Z}$ with $\gcd(a, b) = 1$, prove that if $a | bc$, then $a | c$. 3

UNIT—II

3. *(a)* If $p \ge q \ge 5$ and p, q are both primes, then prove that $24 | (p^2 - q^2)$. 8

(b) For any positive integer k, show that there always exists k consecutive composite numbers. 2

OR

4. *(a)* Let k be the smallest positive integer satisfying the condition $a^k \equiv 1 \pmod{n}$, where $\gcd(a, n) = 1$. Prove that for any positive integer $i \ge j$, $a^i \equiv a^j \pmod{n}$ if and only if $i \equiv j \pmod{k}$. 5

(b) If $a \equiv b \pmod{n}$, prove that $\gcd(a, n) = \gcd(b, n)$. 5

UNIT—III

5. *(a)* If p is a prime, prove that $(p-1)! \equiv -1 (\text{mod } p)$. 5

(b) Let p be an old prime. Prove that the quadratic congruence $x^2 + 1 \equiv 0 (\text{mod } p)$ has a solution if an only if $p \equiv 1 (\text{mod } 4)$. 5

OR

6. *(a)* State and prove Euler's generalization of Fermat's little theorem. 6

(b) Verify that 2 is a primitive root of 19 but not of 17. 4

UNIT—IV

7. *(a)* Prove that the linear congruence $ax \equiv b (\text{mod } n)$ has a solution if and only if $\gcd(a, n) \mid b$. 5

(b) Find all integers that satisfy simultaneously 5

$$x \equiv 2 \ (\text{mod } 3), \ x \equiv 3 \ (\text{mod } 5), \ x \equiv 5 \ (\text{mod } 2)$$

OR

8. *(a)* Let p be an odd prime and $\gcd(a, p) = 1$. Then prove that a is a quadratic residue of p if and only if $a^{\frac{p-1}{2}} \equiv 1 \ (\text{mod } p)$. 7

(b) Let $\left(\frac{a}{p}\right)$ denote the Legendre symbol. Prove that $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (\text{mod } p)$. 3

UNIT—V

9. *(a)* If n is a positive integer and p a prime, then prove that the exponent of the highest power of p that divides $n!$ is

$$\sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right]$$ 7

(b) How many zeros does 50! end with? 3

OR

10. (a) Find one solution to the linear Diophantine equation $172x + 20y = 1000$. 5

(b) State and prove the Mobius inversion theorem. 5

★★★