

Total number of printed pages-7

1 (Sem-4) MAT 4

2025

MATHEMATICS

Paper : MAT0400404

(Number Theory-I)

Full Marks : 60

Time : 2½ hours

The figures in the margin indicate full marks for the questions.

1. Answer the following questions : $1 \times 8 = 8$

(a) State Well-Ordering Principle.

(b) If a and b are integers with $b \neq 0$, then there exist unique integers q and r such that $a = qb + r$ where

(i) $0 < r \leq b$

(ii) $0 \leq r < |b|$

(iii) $0 \leq r \leq b$

(iv) $0 \leq r \leq |b|$

(Choose the correct option)

- (c) Which of the following Diophantine equation cannot be solved ?

(i) $6x + 51y = 22$

(ii) $24x + 138y = 18$

(iii) $158x - 57y = 7$

(iv) $221x + 35y = 11$

- (d) Give an example to show that $a^2 \equiv b^2 \pmod{n}$ need not imply that $a \equiv b \pmod{n}$.

- (e) Without performing the division, determine whether the integer 176, 521, 221, is divisible by 9.

- (f) If p is a prime number, then

(i) $(p-1)! \equiv 1 \pmod{p}$

(ii) $(p-1)! \equiv -1 \pmod{p}$

(iii) $(p+1)! \equiv 1 \pmod{p}$

(iv) $(p+1)! \equiv -1 \pmod{p}$

(Choose the correct option)

- (g) Find $\sigma(180)$.

- (h) Define Möbius μ -function.

2. Answer the following questions : $2 \times 6 = 12$

- (a) If $a|c$ and $b|c$ with $\gcd(a,b)=1$, then prove that $ab|c$.

- (b) Prove that $\gcd(a+b, a-b)=1$ or 2 if $\gcd(a,b)=1$.

- (c) Use Fermat's theorem to show that $5^{38} \equiv 4 \pmod{11}$.

- (d) Show that 41 divides $2^{20} - 1$.

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

- (f) For $n > 2$, prove that $\phi(n)$ is an even integer.

3. Answer **any four** of the following questions :

$$5 \times 4 = 20$$

(a) State and prove Archimedean property.

$$1 + 4 = 5$$

(b) Use the Euclidean Algorithm to obtain integers x and y satisfying

$$\gcd(12378, 3054) = 12378x + 3054y$$

(c) Use Chinese Remainder Theorem to solve the simultaneous congruences

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

(d) If n and r are positive integers with $1 \leq r < n$, then prove that the binomial coefficient

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

is also an integer.

(e) Prove that every positive integer $n > 1$ can be expressed uniquely as a product of primes a part from the order in which the factors occur.

(f) If p and q are distinct primes, prove that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$

(g) If f is a multiplicative function and F

be defined by $F(n) = \sum_{d|n} f(d)$, then

prove that F is also multiplicative.

(h) If $n \geq 1$ and $\gcd(a, n) = 1$, then prove that

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

4. Answer **any two** of the following questions :

$$10 \times 2 = 20$$

(a) (i) Prove that for given integers a and b , with $b > 0$, there exist unique integers q and r satisfying

$$a = bq + r, \quad 0 \leq r < b \quad 6$$

(ii) Establish the following formula by Mathematical induction.

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}$$

for all $n \geq 1$ 4

(b) (i) Given integers a and b , not both of which are zero, prove that there exist integers x and y such that $\gcd(a, b) = ax + by$. 5

(ii) Determine all solutions in the positive integers of the Diophantine equation $172x + 20y = 1000$ 5

(c) (i) Prove that if p is a prime and $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Is the converse of it true? Justify. 5+1=6

(ii) Solve : $9x \equiv 21 \pmod{30}$. 4

(d) (i) Prove that there is an infinite number of primes.

(ii) Prove that the quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$ where p is an odd prime has a solution if and only if $p \equiv 1 \pmod{4}$. 6

(e) (i) If $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ is the prime factorization of $n > 1$, then prove that

$$(II) \quad \tau(n) = (k_1 + 1)(k_2 + 1) \dots (k_r + 1)$$

$$(III) \quad \sigma(n) = \left(\frac{p_1^{k_1+1} - 1}{p_1 - 1} \right) \left(\frac{p_2^{k_2+1} - 1}{p_2 - 1} \right) \dots \left(\frac{p_r^{k_r+1} - 1}{p_r - 1} \right)$$

6

(ii) For each positive integer $n \geq 1$, prove that

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } n > 1 \end{cases} \quad 4$$