

M.Sc.(Maths.) Semester - 3 (CBCS) Examination
Nov/Dec-2023 (NEW COURSE)
Number Theory -1 (Core (New))

Time: 2:30 Hours

Marks: 70

Instructions:

1. Figures to the right indicate marks.
2. All questions are compulsory.

Que.1(A) Answer the following. (04)

- 1) Let $g = (a, b)$ if there exist $d > 0$ such that $d|a$ and $d|b$ then

$$g = (a, b) = d \left(\frac{a}{d}, \frac{b}{d} \right).$$

- 2) If $k \neq 0$ then $(a, b) = (a, b + ka)$.

Que.1(B) Attempt any two out of three. (10)

- 1) Let $g = (42823, 6409)$ then find g using Euclidean algorithm. Also find x & y such that $g = 42823x + 6409y$.
- 2) Prove that every integer $n > 1$ can be uniquely expressed as a product of prime numbers, up to the order of factors.
- 3) If a and b are two integers such that $a \neq 0$ or $b \neq 0$ then the G.C.D. of a & b exist and is unique.

Que.2(A) Answer the following. (04)

- 1) Prove that the linear congruence, $ax \equiv b \pmod{m}$ and $d = (a, m)$ with $d | b$ has exactly d in congruent solutions modulo m .

Que.2(B) Attempt any two out of three. (10)

- 1) Calvin Butterball keeps pet meerkats in his backyard. If he divides them into 5 equal groups, 4 are left over. If he divides them into 8 equal groups, 6 are left over. If he divides them into 9 equal groups, 8 are left over. What is the smallest number of meerkats that Calvin could have?
- 2) State and prove Wilson's theorem.
- 3) Let p be a prime number, then $x^2 \equiv -1 \pmod{p}$ has solution if and only if $p = 2$ or $p = 4k + 1$ for some k .

Que.3(A) Answer the following. (04)

- 1) Let $m \geq 1$ and $m = m_1 * m_2$ with $m_1, m_2 \geq 1, (m_1, m_2) = 1$. If $(\phi(m_1), \phi(m_2)) \geq 2$ then m does not have a primitive root.

Que.3(B) Attempt any two out of three. (10)

- 1) Let $m \geq 1$ & order of $a \pmod{m} = h$ and k be any positive integer then order of $a^k \pmod{m} = \frac{h}{(h, k)}$
- 2) Prove that if p is a prime number then p^2 has exactly $(p - 1) \phi(p - 1)$ primitive roots in $(\pmod{p^2})$.
- 3) Let p be a prime number, suppose $p \nmid a$ and $n \geq 1$. then the congruence equation $x^n \equiv a \pmod{p}$ has either $(n, p - 1)$ solutions $(\pmod{p})$ or no solutions $(\pmod{p})$.

Que.4(A) Answer the following. (04)

1) In usual notations prove the following:

(i) Let $x \in \mathbb{R}$ then $[x] \leq x \leq [x] + 1$

(ii) Let $x \in \mathbb{R}$ then $[x] + [-x] = \begin{cases} 0, & \text{if } x \text{ is an integer} \\ -1, & \text{otherwise} \end{cases}$

Que.4(B) Attempt any two out of three. (10)

1) State and prove De Polignac's formula.

2) Let $n \geq 1$ and $n_1, n_2, \dots, n_k \geq 1$. Suppose that

$n = n_1 + n_2 + \dots + n_k$, then $\frac{n!}{n_1! \cdot n_2! \cdot \dots \cdot n_k!}$ is an integer.

3) In usual notations prove that the divisor function $\tau(n)$ is a multiplicative function.

Que.5(A) Answer the following. (04)

1) Find the highest power of 3 which divides 100!.

Que.5(B) Attempt any two out of three. (10)

1) State and prove Hensel's Lemma.

2) If a is an odd integer then $8|a^2 - 1$ and in general for $\alpha \geq 3$ prove that

$$a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$$

3) Prove that the Mobius function $\mu(n)$ is a multiplicative function. Moreover,

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