647510 **MSC3MatC303x** **Seat No :_____**

M.Sc.(Maths.) Semester - 3 (*CBCS*) Examination
Oct/Nov-2022 (NEW COURSE)
Number Theory -1 (Core (New))

Time: 2:30 Hours **Marks: 70**

Instructions:

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

Question-1(A): Answer the following. **(04)**

(i) Let $g = (a, b)$. If there exist $d > 0$ such that $d|a$ and $d|b$ then prove that $g = (a, b) = d\left(\frac{a}{d}, \frac{b}{d}\right)$.

(ii) If $k \neq 0$ then prove that $(a, b) = (a, b + ka)$.

Question-1(B): Attempt any two out of three. **(10)**

(i) Let $g = (42823,6409)$ then find g using Euclidean algorithm. Also find x & y such that $g = 42823x + 6409y$.

(ii) Prove that every integer $n > 1$ can be uniquely expressed as a product of prime numbers, up to the order of factors.

(iii) If a and b are two integers such that $a \neq 0$ or $b \neq 0$ then show that the G.C.D. of a & b exist and is unique.

Question-2(A): Answer the following question. **(04)**

(i) Prove that the linear congruence, $ax \equiv b(mod\ m)$ and $d = (a, m)$ with $d \mid b$ has exactly d in congruent solutions modulo m.

Question-2(B): Attempt any two out of three. **(10)**

(i) 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?

(ii) State and prove Wilson's theorem.

(iii) Let p be a prime number, then show that $x^2 \equiv -1\ (mod\ p)$ has solution if and only if $p = 2\ or\ p = 4k + 1$ for some k.

Question-3(A): Answer the following question. **(04)**

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

Question-3(B): Attempt any two out of three. **(10)**

(i) Let $m \geq 1$ & order of $a(mod\ m) = h$ and k be any positive integer then show that order of $a^k(mod\ m) = \frac{h}{(h,k)}$

(ii) Prove that if p is a prime number then p^2 has exactly $(p - 1)\ \phi(p - 1)$ primitive roots in $(mod\ p^2)$.

(iii) Let p be a prime number, suppose $p \nmid a$ and $n \geq 1$. then the congruence equation $x^n \equiv a\ (mod\ p)$ has either $(n, p - 1)$ solutions $(mod\ p)$ or no solutions $(mod\ p)$.

Question-4(A): Answer the following questions. **(04)**

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 $[x] + [-x] = \begin{cases} 0\ , & if\ x\ is\ an\ integer \\ -1, & otherwise \end{cases}$

Question-4(B): Attempt any two out of three. **(10)**

(i) State and prove De Polignac's formula.

(ii) Let $n \geq 1$ and $n_1, n_2, \dots, n_k \geq 1$. Suppose that $n = n_1 + n_2 + \cdots + n_k$, then $\frac{n!}{n_1! \cdot n_2! \cdot \dots \cdot n_k!}$ is an integer.

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

Question-5(A): Answer the following question: **(04)**

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

Question-5(B): Attempt any two out of three. **(10)**

(i) State and prove Hensel's Lemma.

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

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

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

****