003-1163003

Seat No. ______

MASTER OF SCIENCE MATHEMATICS(W.E.F.-2016) MSC MATHS(2016) Semester - 3 Examination

October - 2024

NUMBER THEORY 1

Faculty Code : 003

Subject Code : 003-1163003

**Time : 2.30Hours]** **[Total Marks : 70**



Q.1 Answer the following : (Any seven out of ten, each of 02 marks) 14

1 If $a \equiv b \ (mod\ \ m)$. Show that, $ka \equiv kb \ (mod\ \ m); \ \forall k \in \mathbb{Z}$.

2 State : Euclid's Algorithm. Find $\gcd(2024,1729)$.

3 Define, Complete Residue System of modulo m with an example.

4 Find, total number of primitive roots of $31$ in modulo $31$.

5 Find the number of solutions of $x^6 \equiv 9 \ (mod\ \ 2^3)$ if exists .

6 Define with example : Degree of congruence equation.

7 For $x \in \mathbb{R}, \ m \in \mathbb{Z}$, show that, $[x+m] = [x] + m$.

8 Define : $\sigma$- function. Find, $\sigma(245)$.

9 Using Mobius inversion formula find, $\phi(84)$.

10

Find the highest power of $3$ which divides $200!$.

Q.2 Answer the following : ( Any two out of three, each of 07 marks)

1

For any two non-zero integers $a, b$, prove that, $[a,b] \cdot (a,b) = |ab|$.

2

Prove that, any prime $p$ has a Primitive root. Also show that, $p$ has exactly $\phi(p-1)$ primitive roots in (mod $p$).



3

Let $a$ and $m > 0$ be integers such that, $(a,m) = 1$, and $S$ be any $R.R.S.(mod\ m)$. Prove that, there exist unique $\bar{a} \in S$ such that $a \cdot \bar{a} \equiv 1\ (mod\ m)$.



Q.3 Answer the following : (1 & 2 Both are compulsory, each of 07 marks)

1

Let $m, m_1, m_2$ are positive integers such that $m = m_1 \cdot m_2$, where $(m_1, m_2) = 1$ and $(\phi(m_1), \phi(m_2)) \geq 2$. Prove that, $m$ does not have any primitive root.

2 State and prove: Wilson's theorem.



OR

Answer the following : (1 & 2 Both are compulsory, each of 07 marks)

1 1. State and prove: Hensel's lemma.

2

2. Let order of $a(mod\ m)$ is $h$ and order of $b(mod\ m)$ is $k$. If $(h,k) = 1$. Pove that, order of

$ab(mod\ m)$ is $hk$.

Q.4 Answer the following : 14

1

1. If $a \equiv b\ (mod\ m)$ and $c \equiv d\ (mod\ m)$, then prove that, $a + c \equiv b + d\ (mod\ m)$ and $ac \equiv bd\ (mod\ m)$.

2

2. Let $m$ be positive integer which has primitive root, $a$ be any integer such that $(a, m) = 1$. Then for $n \geq 1$ prove that, $x^n \equiv a(mod\ m)$ either has no solution or it has $(n, \phi(m))$ solutions in $(mod\ m)$.



Q.5 Answer the following : (Any two out of four, each of 07 marks) 14

1

a) Let $n > 2$ be odd integer and $a$ be any odd integer. Then for $\alpha \geq 3$ prove that, $x^n \equiv a\ (mod\ 2^\alpha)$ has a unique solution in $R.R.S.(mod\ 2^\alpha)$.



2

b) Let $m, m_1, m_2, \ldots, m_n$ are positive integers, such that $m = m_1 + m_2 + \cdots + m_n$. Show that, $m_1! \cdot m_2! \cdot \cdots \cdot m_n!$ divides $m!$.

3

c) Define: Mobius function $\mu$. Also show that, $\mu$ is multiplicative function.

4

d) Let $f(n) = \sum_{\substack{d|n \\ d\geq 1}} \phi(d)$, where $\phi$ is Eulers function. Prove that, $f(n) = n,\ \forall n \in \mathbb{N}$.