DBL-003-1163003 Seat No. ________

M. Sc. (Sem. III) (CBCS) Examination

June – 2022

Mathematics

(3003 - Number Theory 1)

Faculty Code : 003
Subject Code : 1163003

Time : $2\frac{1}{2}$ Hours] [Total Marks : **70**

Instructions :

(1) Attempt any five questions from the following.

(2) There are total ten questions.

(3) Each question carries equal marks.

1 Answer the following : **14**

(a) Find the number of solutions of $x^{48} \equiv 9 \pmod{17}$ if exists.

(b) Find $\sigma(307)$ and $\tau(19610)$.

(c) Prove that, for any two non-zero integers x and $y \exists a$ and b such that $ax + by = 1$.

(d) Define Euler's function for a positive integer m and write down the value of $\phi(139)$.

(e) State, Euclid's Algorithm and verify it by an example.

(f) Define Prime numbers and also give at least four prime numbers more than 155.

(g) For three integers a,b and $n \in \mathbb{N}$, prove that, if $a \mid b$ then $a^n \mid b^n$.

2 Answer the following : **14**

(a) Define L.c.m. with an example and prove that for $a,b \neq 0$ and $m > 0 m[a,b] = [ma,mb]$.

(b) Using standard notation prove that, $\left[\frac{x}{m}\right]=\left[\frac{[x]}{m}\right]$ for any $x \in R$ and $m \geq 1$ be any integer.

(c) Find the number of solutions of $x^{12} \equiv 16 (\bmod 17)$.

(d) Define : (i) Reduced Residue System and (ii) Solution of Congruence Equation.

(e) Is it always true that if $x \mid y$ then $x \mid ty$ for any $t \in Z$. Justify your answer.

(f) Show that, if $a \equiv b (\bmod m) \Rightarrow (a,m)=(b,m)$.

(g) Find the highest power of 61 which divide 38401!.

3 Answer the following : **14**

(a) Prove that, if p is a prime number then p^2 has exactly $(p-1)\phi(p-1)$ primitive roots in (mod p^2). 7

(b) Find the solutions of the congruence equation $x^4 - 1 \equiv 0$ (mod 15) using Chinese Remainder Theorem. 7

4 Answer the following : **14**

(a) For any odd number g prove that 2^α has no primitive roots for $\alpha \geq 3$. 7

(b) (i) If p is a prime number of the form $4k+3$ and $p \mid a^2 + b^2$ then $p \mid a$ and $p \mid b$ for some $a,b \in Z$. 4

(ii) Show that, for a prime number p of the form $4k+3, p$ cannot be expressed as a sum of squares of two integers. 3

5 Answer the following : **14**

(a) (i) State, Fermat's Theorem. **2**

(ii) Find a solution of $x^{11} \equiv 5 (\mathrm{mod}\, 2^5)$ if exists. **5**

(b) (i) State and prove, Mobius Inversion Formulae. **5**

(ii) Prove that, $\sigma(n)$ is a multiplicative function. **2**

6 Answer the following : **14**

(a) State and Prove, Fundamental Theorem of Arithmetic. **7**

(b) Let, $a,b \in Z - \{0\}$ and $m \geq 1$ If $g = \gcd(a,m)$ then the congruence equation $ax \equiv b (\mathrm{mod}\, m)$ has a solution if and only if $g \mid b$. **7**

7 Answer the following : **14**

(a) State, Wilson's Theorem and also verify the theorem for prime number 13. **7**

(b) Prove that, there are infinitely many prime numbers. **7**

8 Answer the following : **14**

(a) State and prove, Hansel's Lemma. **7**

(b) If $\alpha \geq 3$ be any integer then prove that the set $S = \{5, 5^2, 5^3, ...5^{2^{\alpha-2}}\} \cup \{-5, -5^2, -5^3, ...,-5^{2^{\alpha-2}}\}$ is a reduced residue system (mod 2^{α}). **7**

9 Answer the following : **14**

(a) (i) If g is a primitive root of m then show that the set $S = \{1, g, g^2, ..., g^{\phi(m)-1}\}$ is a reduced residue system (mod m). **5**

(ii) Prove that, for any odd number $a, 8 \mid a^2 - 1$. **2**

(b) For a prime number p and $n \geq 1$ with $p \nmid a$ then show that either $x^n \equiv a (\bmod p)$ has no solution or there are $(n, p-1)$ solutions in any C.R.S. (mod p). **7**

10 Answer the following : **14**

(a) Suppose $f(x) \equiv 0 (\bmod p)$ has degree n then prove that the n number of solutions in any C.R.S. (mod m) is $\leq n$. **7**

(b) If $m, m_1, m_2, \ldots\ldots, m_k \geq 1$ are integers with $m = m_1 + m_2 + \cdots \ldots\ldots + m_k$ then prove that **7**

$\dfrac{m!}{m_1! \cdot m_2! \cdot \ldots\ldots \cdot m_k!}$ is an integer.
