JBZ-003-1163003 Seat No. ______

M. Sc. (Sem. III) Examination

December - 2019

Mathematics - 3003

(Number Theory - I)

Faculty Code : 003
Subject Code : 1163003

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

Instructions : (1) There are five questions.
(2) All questions are compulsory.
(3) Each question carries 14 marks.

1 Do as directed : (Answer any **seven**) **14**

(a) Find the number of solution of $x^2+1\equiv 0(\text{mod } p)$ for p is of the form $4k+3$.

(b) Define Totally Multiplicative Function with example.

(c) Find all solutions of $6x\equiv 2(\text{mod } 8)$.

(d) Prove that if p be a prime number and p does not divides a then $a^p \equiv a(\text{mod } p)$.

(e) State Euclid's Algorithm.

(f) Prove that g.c.d is always unique for any two real numbers.

(g) State Division Algorithm.

(h) State De-Poignac's Formulae.

(i) Find $\phi(63*625*49)$.

2 Answer any **two** of the following : **14**

(a) State and prove Chinese Remainder Theorem. **7**

(b) (i) Prove that for g = g.c.d (a, b) if d is a positive integer of a and b such that $d|a$ and $d|b$ then $\frac{g}{d}=\left(\frac{a}{d},\frac{b}{d}\right)$. **3**

(ii) For $n\geq 1$ and p be a prime number then **4**

$$\left[\frac{n}{p^j}\right]=\left[\frac{n-1}{p^j}\right]+1 \text{ or } 0.$$

(c) Let a and b are non-zero integers then prove that g.c.d of a and b exists and if g = g.c.d (a, b) then g = $ax + by$ for some integers x and y. **7**

3 Answer the following : **14**

(a) If $m_1, m_2, m_3, \ldots\ldots\ldots\ldots m_k \geq 1$ with the condition $m = m_1 + m_2 + m_3 + \ldots\ldots\ldots + m_n$ then prove that $\frac{m!}{m_1!\, m_2!\, m_3! \ldots\ldots\ldots m_n!}$ is an integer. **7**

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

OR

(b) 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**

4 Answer the following : **14**

(a) State and Prove Euler's Theorem.

OR

(a) State and Prove Fundamental Theorem of Arithmetic.

(b) Suppose $f(x)$ is a polynomial with integer coefficients, p is a prime number and $f(x) \equiv 0 (\text{mod } p)$ has degree n. Prove that $f(x) \equiv 0 (\text{mod } p)$ has atmost n solutions in any completer residue system (mod p).

5 Answer the following : **14**

(a) Prove that $\sigma(n)$ and $\Im(n)$ is a multiplicative function. **4**

(b) If $m_1, m_2 \geq 1$ and $m = m_1 \cdot m_2$ provided m_1 and m_2 are relatively prime with $(\phi(m_1), \phi(m_2)) \geq 2$ then show that m does not have a primitive root. **5**

(c) Prove that if order of a(mod m) = h and order of b(mod m) = j with (h, j) = 1 then order of ab (mod m) = hj. **5**

OR

(c) Prove that for a prime number $p = 2$ or $4k+1$ there is a solution of $f(x) \equiv 0 (\text{mod } p)$ where $f(x) = x^2 + 1$ for some k. **5**