F-41/2110 10053/NJ

NUMBER THEORY-303
SEM-III
Syll-Dec-17

Time- 3hrs **M.M. 75**

Section A

1. a) If $\gcd(a, m) = 1$, then prove that $a^{\phi(m)} \equiv 1 \ (mod\ m)$

b) Solve the system of congruences:

$$x \equiv 2 \ (mod\ 3), \quad x \equiv 3\ mod(5), \quad x \equiv 5\ (mod\ 2)$$

2. State and prove the fundamental theorem of arithmetic.

3. a) For an integer $n > 1$, Show that

$$\prod_{d|n} d = n^{d(n)/2}$$

where $d(n)$ denotes the number of positive divisors of n.

b) Define Mobius function μ and prove that

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

4. a) Using Wilson's theorem, prove that for any odd prime p,

$$1^2 . 3^2 . 5^2 \ldots\ldots\ldots\ldots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} (mod\ p)$$

b) Use Fermat's theorem to prove that if p is an odd prime, then

$$1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots \ldots\ldots\ldots + (p-1)^{p-1} \equiv -1 (mod\ p)$$

Section B

5. Let p be an odd prime and a be any integer such that $\gcd(a, p) = 1$. If n denotes the number of integers in the set

$$S = \left\{a, 2a, 3a, \ldots\ldots\ldots \frac{1}{2}(p-1)a\right\}$$

whose reminders upon divisors by p exceed $p/2$. Then show that $\left(\frac{a}{p}\right) = (-1)^n$

6. Find all solutions in positive integers of the equation $56x + 72y = 40$

7. a) Determine whether 3422 is a quadratic residue or non-residue of the prime 5683.

b) Show that if, for $n > 1$, $F_n = 2^{2^n} + 1$ is prime, then 2 is not a primitive root of F_n.

8. Find all the primitive Pythagorean triple for which $x = 40$.

Section C

9. Write in brief:

a) If $\gcd(a, b) = 2$, then find $\gcd(a, b + 3a)$.

b) If x and y are odd integers, prove that $x^2 + y^2$ is even but not divisible by 4.

c) Using congruence, show that $2^{15}.14^{40} + 1$ is divisible by 11.

d) Using induction method, show that $8|5^{2n+7}$.

e) For every integer $n > 1$, show that $n^4 + 4$ is a composite.

f) Find the following (succeeding) fraction of $\frac{4}{9}$ in F_{20}.

g) Define the arithmetic functions $\phi(n), d(n), \sigma(n)$.

h) Define the Legendre symbol $\left(\frac{a}{p}\right)$.

i) Find the smallest integer x for which $d(x) = 6$

j) Show that the system $x \equiv 5(mod\ 6)$ and $x \equiv 7(mod\ 15)$ does not possess a solution.