QP CODE: 21000687 21000687 **Reg No** : ....

Name : ....

M Sc DEGREE (CSS) EXAMINATION, JULY 2021

Fourth Semester

Faculty of Science

CORE - ME010402 - ANALYTIC NUMBER THEORY

M Sc MATHEMATICS,M Sc MATHEMATICS (SF)

2019 Admission Onwards

B052CF42

Time: 3 Hours Weightage: 30

Part A (Short Answer Questions)

Answer any **eight** questions.

Weight **1** each.

1. Define Euler Totient function $\phi(n)$. Also prove that $\phi(n)$ is even for $n \geq 3$.

2. State Euler's summation formula and define Riemann zeta function.

3. Explain the mutual visible lattice points. State a necessary and sufficient condition for two lattice points (a, b) and $(m, n)$to be mutually visible.

4. Derive Euler's summation formula from Abel's identity.

5. Write any four equivalent forms of the prime number theorem.

6. (a) If $ac \equiv bc(mod\ m)$ and if $d = (m, c)$, then prove that $a \equiv b(mod\frac{m}{d})$.
   (b) If $c > 0$ then prove that $a \equiv b(mod\, m)$ if and only if $ac \equiv bc(mod\, mc)$.

7. Define residue class $a\ modulo\, m$ and prove that for a given modulus m the m residue classes $\hat{1}, \hat{2}, \ldots, \hat{m}$ are disjoint and their union is the set of all integers.

8. If $\{a1, a2, \ldots. a_{\phi(m)}\}$ is a reduced residue system modulo m and if $(k, m) = 1$ then prove that $\{ka1, ka2, \ldots ka_{\phi(m)}\}$ is also a reduced residue system modulo m.

9. Define quadratic residues. Find the quadratic nonresidues for p = 13.

10. (a) Define $exp_m(a)$.
    (b) Let $m \geq 1$ and $(a, m) = 1$. Then prove that $a^k \equiv a^h(mod\, m)$ if and only if $k \equiv h(mod\, m)$,where$f = exp_m(a)$.

(8×1=8 weightage)

Part B (Short Essay/Problems)

Answer any **six** questions.

Weight **2** each.

11. Prove that if both g and $f*g$ are multiplicative then f is multiplicative.

12. (a) Prove that if f is multiplicative then $\sum_{d|n}\mu(d)f(d) = \Pi_{p|n}(1-f(p))$.
(b)State and prove the associative property relating $\circ$ and $*$.

13. Show that the n^{th}prime P_n satisfies the inequality $\frac{1}{6}n\, log\, n < P_n < 12(n\, log\, n + n\, log\frac{12}{e}), \forall\, n \geq 1$.

14. Show that $(i)\sum_{n\leq x}\psi(\frac{x}{n}) = x\, log\, x - x + O(log\, x)$ and $(ii)\sum_{n\leq x}\vartheta(\frac{x}{n}) = x\, log\, x - x + O(x)$.

15. Given a prime p,let $f(x) = c_0 + c_1x + \ldots c_nx^n$ be a polynomial of degree n with integer coefficents such that $c_n \not\equiv 0(mod\, p)$. Then prove that polynomial congruence $f(x) \equiv o(mod\, p)$has at most n solutions.

16. Find all x which simultaneously satisfy the system of congruences $x \equiv 1(mod\, 3), x \equiv 2(mod\, 4), x \equiv 3(mod\, 5)$.

17. Prove that $(-1|p) = -1$ if $p = 4m + 3$for some integer m. Also write a formula for $(2|p)$when p is an odd prime.

18. Let g be a primitive root mod p, where p is an odd prime. Then prove that the even powers $g^2, g^4, \ldots, g^{p-1}$are the quadratic residues and the odd powers $g, g^3, \ldots, g^{p-2}$are the quadratic nonresidues mod p.

(6×2=12 weightage)

Part C (Essay Type Questions)

Answer any **two** questions.

Weight **5** each.

19. (a)For $x \geq 1$ prove that $\left|\sum_{n\leq x}\frac{\mu(n)}{n}\right| \leq 1$ with equality holding only if $x < 2$.

(b)Prove that for every $x \geq 1, [x]! = \Pi_{p\leq x}p^{\alpha(p)}$,where the product is extended over all primes $\leq x,\ and\ \alpha(p) = \sum_{m=1}^{\infty}[\frac{x}{p^m}]$.

(c) If $x \geq 2$,prove that $log[x]! = x\, log\, x - x + O(log\, x)$.

20. Let $\{a(n)\}$ be a nonnegative sequence such that $\sum_{n\leq x}a(n)[\frac{x}{n}] = x\, log\, x + O(x) for\ all\ x \geq 1$. Then prove the following

(a) $\forall\, x \geq 1, we\ have \sum_{n\leq x}\frac{a(n)}{n} = log\, x + O(1)$.

(b) There is a constant B such that $\sum_{n\leq x}a(n) \leq Bx, \forall\, x \geq 1$.

(c) There is a constant $A > 0$and an $x_0 > 0$ such that $\sum_{n\leq x}a(n) \geq Ax, \forall\, x \geq x_0$.

21. (a) Prove that for a given integer $k > 0$ there exist a lattice point (a, b) such that none of the lattice points $(a + r, b + s)$,$0 < r \leq k$,$o < s \leq k$, isvisible from the origin.
(b) Let f be a polynomial with integer coefficients, let $m_1, \ldots, m_r$ be positive integers relatively prime in pairs, and let $m = m_1m_2 \ldots m_r$.Prove that the congruence $f(x) \equiv 0(mod\, m)$ has a solution if and only if each of the congruences $f(x) \equiv o(mod\, m_i)$ $(i = 1, \ldots, r)$ has a solution. Also show that if $v(m)$ and $v(m_i)$ denote the number of solutions of $f(x) \equiv 0(mod\, m)$and $f(x) \equiv o(mod\, m_i)$for $i = 1, \ldots, r$, respectively, then $v(m) = v(m_1)v(m_2) \ldots v(m_r)$.

22. Assume n is not congruent to $0(modp)$ and consider the least positive residues mod p of the following $\frac{p-1}{2}$multiples of $n : n, 2n, 3n, \ldots, \frac{p-1}{2}n$. Then if m denotes the number of these residues which exceed $\frac{p}{2}$, prove that $(n|p) = (-1)^m$.

(2×5=10 weightage)