19P105A (Pages: 2) Name: ……………………

Reg. No……………………..

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, NOVEMBER 2019

(Supplementary/Improvement)

(CUCSS-PG)

CC17P MT1 C04 – NUMBER THEORY

(Mathematics)

(2017 & 2018 Admissions)

Time: Three Hours Maximum: 36 Weightage

Part A

Answer ***all*** questions. Each question carries 1 weightage.

1. If $n \geq 1$, prove that $\sum_{d/n} \mu(d) = \left[\frac{1}{n}\right]$
2. Prove that $\varphi(n)$ is even for $n \geq 3$
3. Prove that for all ≥ 1, $\log n = \sum_{d/n} \Lambda(d)$
4. Prove that Dirichlet product of two multiplicative functions is multiplicative.
5. Prove that the number of positive divisors of n is odd if and only if n is a square.
6. For any arithmetical functions α and β and for any real or complex valued function F on $(0, \infty)$ such that $F(x) = 0$ for $0 < x < 1$, prove that $\alpha \circ (\beta \circ F) = (\alpha * \beta) \circ F$
7. Prove that $\forall x \geq 1, \sum_{n \leq x} \Lambda(n) \left[\frac{x}{n}\right] = \log([x]!)$
8. Define Chebyshev's ψ- function and ϑ-function and prove that $\psi(x) = \sum_{m \leq x} \vartheta\left(x^{\frac{1}{m}}\right)$
9. Find the quadratic residues and non residues modulo 19
10. Calculate the highest power of 21 that divides 1000!
11. Describe about shift cryptosystem and find a formula for the number of different shift transformations with an N-letter alphabet.
12. Write a note on authentication in public key cryptosystem.
13. Find the cipher text of 'DECEMBER' in the affine cryptosystem with enciphering key (7,3) in the 26 letter alphabet.
14. Find the inverse of $A = \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix} \ (mod\ 26)$

(14 × 1 = 14 Weightage)

Part B

Answer any ***seven*** questions. Each question carries 2 weightage.

15. If f is a multiplicative arithmetical function and $f^{-1}(n) = \mu(n)f(n), \forall n \geq 1$, then prove that f is completely multiplicative.

16. State and prove the Selberg identity.

17. For all $x \geq 1$, prove that $\left|\sum_{n\leq x}\frac{\mu(n)}{n}\right| \leq 1$

18. If $n \geq 1$, prove that $\sum_{n\leq x}\frac{1}{n} = \log x + C + O(\frac{1}{x})$, where C is the Euler's constant.

19. Prove that $\lim_{x\to\infty}\left(\frac{M(x)}{x} - \frac{H(x)}{x\log x}\right) = 0$

20. State and prove Gauss lemma.

21. Let p be an odd prime. Prove that $\sum_{r=1}^{p-1} r(r|p) = 0$ if $p \equiv 1(mod\ 4)$

22. Prove that the Diophantine equation $y^2 = x^3 + k$ has no solutions if k has the form $k = (4n-1)^3 - 4m^2$ where m and n are integers such that no prime $p \equiv -1(mod\ 4)$ divides m.

23. Solve the system of simultaneous congruences

    $x + 3y \equiv 1(mod\ 26)$

    $7x + y \equiv 1(mod\ 26)$

24. (i) Describe about RSA cryptosystem.

    (ii) How to send a digital signature in RSA cryptosystem?

(7×2= 14 Weightage)

Part C

Answer any ***two*** questions. Each question carries 4 weightage.

25. Prove that if both g and $f * g$ are multiplicative then f is also multiplicative and hence show that the set of all multiplicative functions is a subgroup of the group of all arithmetical functions f with $f(1) \neq 0$

26. If a and b are positive real numbers such that $ab = x$, then for any arithmetical functions f and g, prove that

    $$\sum_{\substack{q,d \\ qd\leq x}} f(d)g(q) = \sum_{n\leq a} f(n)\, G\left(\frac{x}{n}\right) + \sum_{n\leq b} g(n)\, F\left(\frac{x}{n}\right) - F(a)G(b) \text{ where}$$

    $F(x) = \sum_{n\leq x} f(n)$ and $G(x) = \sum_{n\leq x} g(n)$

27. State Abel's Identity and deduce Euler's Summation formula from Abel's identity.

28. If p is an odd positive integer show that $(-1|p) = (-1)^{\frac{p-1}{2}}$ and $(2|p) = (-1)^{\frac{p^2-1}{8}}$

(2 × 4 = 8 Weightage)

****