3COPY

16P205 (Page: 2) Name……………………

Reg. No……………….

SECOND SEMESTER M.Sc. DEGREE EXAMINATION, MAY-2017

(Regular/Supplementary/Improvement)

(CUCSS - PG)

CC15P MT2 C10 - NUMBER THEORY

(Mathematics)

(2015 Admission Onwards)

Time:Three Hours Maximum: 36 Weightage

Part A

Answer **All** Questions.Each Question Carries **One** Weightage

1. Define the derivative of an arithmetical function, hence find out u'in terms of Mangoldt function $\Lambda(n)$.
2. Prove that the equation $f(n) = \sum_{d/n} g(d)$ implies $g(n) = \sum_{d/n} f(d)\mu\left(\frac{n}{d}\right)$.
3. Show that for $n \geq 1$, $logn = \sum_{d/n} \Lambda(d)$
4. Prove that $[2x] - 2[x]$ is either 0 or 1.
5. Give an example of an arithmetical function which is not multiplicative.
6. State Legendre's identity.
7. Show that, if $(a, b) = d$ then there exists integers x and y such that $ax + by = d$.
8. Find all integers n such that $\varphi(n) = \frac{n}{2}$
9. Check whether Legendre symbol is completely multiplicative.
10. State quadratic reciprocity law and evaluate $(5|383)$.
11. Determine whether 117 is quadratic residue or non residue of 997.
12. Prove that the product of two linear enciphering transformations is again a linear enciphering transformation.
13. Find the inverse of the matrix $A = \begin{pmatrix} 15 & 17 \\ 4 & 9 \end{pmatrix} (mod26)$
14. Find a formula for the number of different affine enciphering transformations on single letter message units in an N-letter alphabet. **(14x1=14 Weightage)**

Part B

Answer Any **Seven** Questions.Each Question Carries **Two** Weightage

15. Show that if $n \geq 1$ then $\sum_{d/n} \varphi(d) = n$
16. Assume f is multiplicative. Prove that $f^{-1}(n) = \mu(n)f(n)$ for every square free n.

17. If $x \geq 1$, prove that $\sum_{n \leq x} \frac{1}{n} = logx + C + O\left(\frac{1}{x}\right)$.

18. Show that $\lim_{x \to \infty} \frac{\pi(x)logx}{x} = 1$ and $\lim_{x \to \infty} \frac{\vartheta(x)}{x} = 1$ are logically equivalent.

19. State Abel's identity and deduce Euler's summation formula.

20. Let p be an odd prime and let $q = \frac{p-1}{2}$, prove that: $(q!)^2 + (-1)^q \equiv 0(modp)$

21. Prove that $(2|p) = (-1)^{\frac{p^2-1}{8}}$, where p is an odd prime.

22. State and prove Euler-Fermat theorem.

23. Solve the following system of simultaneous congruences:

    $9x + 20y \equiv 10(mod29)$

    $16x + 13y \equiv 21(mod29)$.

24. Find the discrete log of 28 to the base 2 in $F_{37}{}^*$ using the Silver-Hellman algorithm.

(7x2=14 Weightage)

Part C

Answer Any **Two** Questions.Each Question Carries **Four** Weightage

25. Prove that the set of all arithmetical functions f with $f(1) \neq 0$ forms an abelian group under Dirchlet multiplication.

26. Prove that the set of lattice points visible from the origin contains arbitrarily large square gaps.

27. State and prove Shapiro's Tauberian theorem.

28. 1) Compare Private Key and Public Key Cryptosystems.

    2) Describe RSA Public key cryptosystem. **(2x4=8 Weightage)**

****