15P205 (Pages:2) Name.....

Reg. No.....

SECOND SEMESTER M.Sc. DEGREE EXAMINATION, JULY 2016

(CUCSS-PG)

(Mathematics)

CC 15P MT2 C10- NUMBER THEORY

(2015 Admission)

Time:Three Hours Maximum: 36 Weightage

Part A

Answer All Questions

Each Question Carries **One** Weightage

1. Show that for $n \geq 1$, $\sum_{d/n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1, if\ n = 1 \\ 0, if\ n > 1 \end{cases}$
2. Prove that if f is multiplicative then $f(1) = 1$
3. For the statement either give a proof or exhibit a counter example,

   "$If\ (a,b) = 1$ then $\big(\varphi(a), \varphi(b)\big) = 1$"
4. Prove that $[3x] - 3[x]$ is either 0 or 1 or 2.
5. Let $(a,m) = d$. Show that the linear congruence $ax \equiv b(mod m)$ has solutions iff d/b.
6. Find all integers n such that $\varphi(n) = 4$.
7. State Chinese Remainder Theorem.
8. Prove that congruence is an equivalence relation.
9. Prove that $\sum_{r=1}^{p-1}(r|p) = 0$ if p is an odd prime.
10. Determine the quadratic residues and non residues modulo 13.
11. Determine whether 219 is a quadratic or non residue mod 383.
12. Find the inverse of $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} (mod 26)$
13. What is a hash function and how it is used in cryptography?
14. Prove that the product of two shift enciphering transformations is again a shift enciphering transformation. (14x1=14)

Part B

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

15. Show that the set of all multiplicative function is a subgroup of the group of all arithmetical function f with $f(1) \neq 0$.

16. Assume f is multiplicative. Prove that $f^{-1}(n) = \mu(n)f(n)$ for every square free n.

17. State Euler's summation formula and deduce $\sum_{n\leq x} \frac{logn}{n} = \frac{1}{2}log^2x + A + O\left(\frac{logx}{x}\right)$, where A is a constant and $x \geq 2$.

18. State and prove Abel's identity.

19. For $n \geq 1$, prove that the nth prime P_n satisfy the inequality:

$\frac{1}{6}nlogn < P_n < 12\left(nlogn + nlog\frac{12}{e}\right)$.

20. State and prove Wolstenholme's theorem.

21. Solve the congruence $25x \equiv 15(mod\ 120)$.

22. If P is an odd positive integer. Show that $(-1|P) = (-1)^{\frac{P-1}{2}}$.

23. Explain how to send a signature in RSA cryptosystem.

24. In 26-letter alphabet, use affine enciphering transformation with key $(a, b) = (7,8)$ to encipher "BLESSME". (7x2=14)

Part C

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

25. State and prove the principle of cross classification.

26. Prove that prime number theorem implies $\lim_{x\to\infty} \frac{M(x)}{x} = 0$.

27. State and prove Lagrange's theorem.

28. Write short notes on:
    (i) Diffie-Hellman key exchange system.
    (ii) ElGamal Cryptosystem. (2x4=8)

****