17P207 (Pages: 2) Name……………………….

Reg. No……………………

SECOND SEMESTER M.Sc. DEGREE EXAMINATION, MAY 2018

(Supplementary/Improvement)

(CUCSS - PG)

CC15P MT2 C10 – NUMBER THEORY

(Mathematics)

(2015 & 2016 Admissions)

Time: Three Hours Maximum: 36 Weightage

Part A

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

1. State the relation between φ and μ.
2. Define a multiplicative function. Give an arithmetical function which is not multiplicative.
3. If the integer n has r distinct odd prime factors, then prove that $2^r|\varphi(n)$.
4. Find $\varphi^{-1}(12)$.
5. Define big oh notation and show that $\frac{x-[x]}{x} = O\left(\frac{1}{x}\right)$.
6. Verify that $50!$ terminates in 12 zeros.
7. Find $\pi(14)$.
8. Solve the linear congruence $5x \equiv 2(mod\ 26)$.
9. Show that $n^7 - n$ is divisible by 42.
10. Determine the quadratic residues and non residues modulo 11.
11. State quadratic reciprocity law for Legendre symbol and evaluate $(5|71)$.
12. Find a formula for the number of different affine enciphering transformations there are with an N-letter alphabet.
13. Prove that any sequence of positive integers $\{v_i\}$ with $v_{i+1} \geq 2v_i$, is super increasing.
14. Define the discrete logarithm problem.

(14 x 1 = 14 Weightage)

Part B

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

15. Assume f is multiplicative. Prove that $f^{-1}(n) = \mu(n)f(n)$ for every square free n.
16. Let $f(n) = [\sqrt{n}] - [\sqrt{n-1}\,]$. Prove that f is multiplicative but not completely multiplicative.
17. State and prove Euler's summation formula. Deduce that $\sum_{n\leq x}\frac{1}{n^\alpha} = \frac{x^{\alpha+1}}{\alpha+1} + O(x^\alpha)$, if $\alpha \geq 0$.

18. If $m|n$, prove that $\varphi(m)|\varphi(n)$.

19. 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.

20. Prove that $(2|p) = (-1)^{(p^2-1)/8}$, where p is an odd prime. Also find all odd primes, for which 2 is a quadratic non-residue.

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

22. Solve the following system of simultaneous congruence

$$x + 4y \equiv 1(mod 9)$$

$$5x + 8y \equiv 2(mod 9)$$

23. Working in the 26 letter alphabet with enciphering matrix $\begin{pmatrix} 15 & 17 \\ 4 & 9 \end{pmatrix}$, decipher the cipher text "FWMDIQ".

24. Find the discrete log of 153 to the base of 2 in $\mathbb{F}_{181}^*$.

(7 x 2 = 14 Weightage)

Part C

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

25. Given integers r,d and k such that $d|k$, also k≥ 1 and gcd$(r, d) = 1$. Show that the number of elements in the set

$$S = \left\{r + td, t = 1,2, \dots, \frac{k}{d}\right\}$$

which are relatively prime to k is $\frac{\varphi(k)}{\varphi(d)}$.

26. With usual notations, prove that there is a constant A such that

$\sum_{p\leq x}\left(\frac{1}{p}\right) = \log(\log x) + A + O\left(\frac{1}{\log x}\right)$ for all $x \geq 2$.

27. State and prove the Gauss Lemma and deduce the formula for finding the value of m in the lemma.

28. Write short notes on the following with examples

(a) RSA Cryptosystem.

(b) Diffie-Hellman key exchange system.

(2 x 4 = 8 Weightage)

****