C 63093 (Pages : 3) N me..................................

Reg. No..............................

# SECOND SEMESTER M.Sc. DEGREE EXAMINATION, JUNE 2014

(CUCSS)

Mathematics

MT 2C 10—NUMBER THEORY

Time : Three Hours Maximum : 36 Weightage

## Part A

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

1. Let (m, n) = $d$. Prove that, for the Euler totient function $\phi$, $\phi(m$ n $\phi$ (m) • $\phi$ (n) · d $\phi(d)$

2. Prove that the equation f (n) = $\sum_{d/n} g(d)$ implies $g(\mathrm{n}) = \sum_{d/n} \mathrm{f}(d) \cdot \mu\left(\frac{r}{d}\right)$.

3. If $f$ and $g$ are arithmetical functions, show that :

$$(f * g)' = *g + f * g \cdot$$

4. For x > 1, prove that :

$$\sum \wedge(n)\left[\frac{x}{n}\right] = \log\,[x]!$$

5. State Abel's identity.

6. Prove that congruence is an equivalence relation.

7. For any integer a and any prime $p$, prove that :

$$a' \equiv a \pmod p \cdot$$

8. State Chinese remainder theorem.

9. Let $p$ be an odd prime. Prove that every reduced residue system mod $p$ contains exactly $(p-1)/2$ quadratic residues and exactly $(p\ -1)12$ quadratic non-residues mod $p$.

**Turn over**

10. If P is an odd positive integer, prove that :

$$(-1/p) = (-1)^{(p-1)/2}.$$

11. In the 27-letter alphabet (with blank = 26) use the affine enciphering transformation with key a = 13, *b* = 9 to encipher the message "HELP ME".

12. What do you mean by an enciphering matrix ?

13. Explain how to send a signature in RSA cryptosystem ?

14. What is oblivious transfer ?

**(14 x 1 = 14 weightage)**

## Part B

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

**15. If n ≥ 1, prove that :**

$$\phi(n) = n \cdot \prod_{p/n} \left(1 - \frac{1}{p}\right)$$

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

**17. If $x \geq 1$, prove that :**

$$\sum_{n \leq x} \frac{1}{n} = \log x + C + O\left(\frac{1}{x}\right)$$

**18. For n > 1, prove that the nth prime $P_n$ satisfy the inequality :**

$$\frac{1}{6} n \log n < p_n < 12\left(n \log n + n \log \frac{12}{e}\right)$$

**19. Let *p* be an odd prime and let $q = \frac{p-1}{2}$. Prove that :**

$$(q!)^2 + (-1)^q \equiv 0 \pmod{p}.$$

20. Solve the congruence :

$25x \equiv 15 \pmod{120}$.

21. Let $p$ be an odd prime. Prove that :

$$\sum_{\substack{r\,p=)=1 \\ (r/}} r \quad \frac{p(p}{4} \text{ if } p \quad 1(\text{mod} \quad .$$

22. **Find the inverse of the matrix $\begin{vmatrix} 15 & 17 \\ 4 & 9 \end{vmatrix}$ mod 26**

23. **Find the discrete log of 28 to the base 2 in $\mathbf{F}_{37}^{*}$, using the Silver-Pohlig-Hellman algorithm. (2 is a generator of $\mathbf{F}_{37}^{*}$).**

24. **Briefly describe a method to construct the Knapsack cryptosystem.**

**(7 x 2 = 14 weightage)**

## Part C

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

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

26. **Let $\{a(n)\}$ be a non-negative sequence such that :**

$$\sum_{n \le x} a(n)\left[\frac{x}{n}\right] = x \log x + 0\,(x) \text{ for all } x \quad .$$

**Prove that there is a constant B > 0 such that :**

$$\sum_{n \le x} a(n) \le B(x) \text{ for all } x \ge 1 .$$

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

28. Explain the advantages and disadvantages of public key cryptosystem as compared to classical cryptosystems.

(2 x 4 = 8 weightage)