C 83627 (Pages : 3) Name..............................

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

20

SECOND SEMESTER M.Sc. DEGREE EXAMINATION, JUNE 2015

(CUCSS)

Mathematics

MT 2C 10—NUMBER THEORY

Time : Three Hours Maximum : 36 Weightage

Part A

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

1. Find all integers x such that $\varphi(n) = \varphi(2n)$.
2. Show that $\varphi(mn) = \varphi(m)\varphi(n)$ if $(m,n) = 1$.
3. Define completely multiplicative function.
4. Define divisor functions $\sigma_\alpha(n)$ for $n \geq 1$ and show that they are multiplicative.
5. If f and g are arithmetical functions, then show that $(f * g)' = f' * g + f * g'$.
6. Show that if $a > 0$ and $b > 0$, then $\lim_{x\to\infty} \frac{\pi(ax)}{\pi(bx)} = \frac{a}{b}$.
7. Let $(a, m) = 1$. Show that the linear congruence $ax \equiv b \pmod{m}$ has exactly one solution.
8. Determine the quadratic residues and non-residues modulo 11.
9. Determine those odd primes p for which 3 is a quadratic residue.
10. Show that if p is an odd positive integer then $(2/p) = (-1)^{\left(\frac{p^2-1}{8}\right)}$.
11. Prove that the product of two linear enciphering transformations is also a linear enchiphering transformation.
12. Write a short note on enciphering key.
13. What is classical cryptosystem ?
14. State the map coloring problem and translate it to a graph coloring problem.

(14 × 1 = 14 weightage)

Turn over

Part B

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

15. Show that for $n \geq 1, \varphi(n) = n \prod_{p/n} \left(1 - \frac{1}{p}\right)$.

16. Let f be a multiplicative function. Show that f is completely multiplicative
$f^{-1}(n) = \mu(n) f(n)$ for all $n \geq 1$.

17. State and prove Euler's summation formula.

18. Show that for $x \geq 2$; $\sum_{p \leq x} \left[\frac{x}{p}\right] \log p = x \log x - x + 0(\log x)$.

19. Show that for any prime $p \geq 5$; $\sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0 \pmod{p^2}$.

20. Let p be an odd prime. Show that for all n ; $(n/p) \equiv n^{\left(\frac{p-1}{2}\right)} \pmod{p}$.

21. Show that given any integer $k > 0$ there exists a lattice point (a, b) such that none of the la
points $(a+r, b+s)$, $0 < r \leq k, 0 < s \leq k$ is visible from the origin.

22. Find the inverse of $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in M_2\left(\frac{Z}{26\,Z}\right)$.

23. Solve the following system of simultaneous congruences :

$17x + 11y \equiv 7 \pmod{29}$
$13x + 10y \equiv 8 \pmod{29}$.

24. Write a note on the ElGamal cryptosystem.

(7 × 2 = 14 weigh

Part C

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

25. Show that the set of all arithmetical functions f with $f(1) \neq 0$ forms an abelian group with respect to the Dirichlet product.

26. Let p_n deonte the n^{th} prime. Prove that the following are equivalent :

    (i) $\lim_{x \to \infty} \frac{\pi(x) \log x}{x} = 1.$

    (ii) $\lim_{x \to \infty} \frac{\pi(x) \log \pi(x)}{x} = 1.$

    (iii) $\lim_{n \to \infty} \frac{p_n}{n \log n} = 1.$

27. State and prove Quadratic reciprocity law.

28. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2\left(Z/_{NZ}\right)$ and set $D = a$. Prove that the following are equivalent :

    (a) $g \subset d = (D, N) = 1.$

    (b) A has an inverse.

    (c) If x and y are not both 0 in $\frac{Z}{NZ}$, then $A\begin{pmatrix} x \\ y \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$

    (d) A gives a one to one correspondence of $\left(\frac{Z}{NZ}\right)^2$ with itself.

(2 × 4 = 8 weightage)