

D 72785

(Pages : 3)

Name.....

Reg. No.....

FIRST SEMESTER M.A./M.Sc./M.Com. DEGREE EXAMINATION
DECEMBER 2019

(CUCSS)

Mathematics

MT 1C 04—NUMBER THEORY

(2016 Admissions)

Time : Three Hours

Maximum : 36 Weightage

Part A

Answer all questions.

Each question carries a weightage of 1.

1. Which are the possible $n \in \mathbb{N}$ such that $\varphi(n) = \varphi(2n)$?
2. Give an example to show that a multiplicative function need not be completely multiplicative. Verify it.
3. If f is multiplicative and not identically 0, show that $f(1) = 1$.
4. Prove that $[x+n] = [x] + n$ for $n \geq 1$.
5. State the Euler summation formula ; and give an asymptotic formula for $\log[x]!$
6. Define the Chebyshev's functions $\psi(x)$ and $\vartheta(x)$.
7. State the prime number theorem. State an equivalent version of it in terms of the n th prime p_n .
8. If $0 < a < b$, prove that there exists x_0 such that for $x \geq x_0$, there is atleast one prime between ax and bx .
9. Define the little o notation. Express $M(x)$ as the little o of a function.
10. Define the Legendre symbol $(n|p)$. What is the value of $(m^2|p)$ for an integer $m \not\equiv 0 \pmod{p}$?
11. Find the value of $(-1|27)$.
12. Prove that 3 is a quadratic non-residue for any p which is 5 mod 12.

Turn over

13. What is an affine map? Define such a map from A to Z and transform the message HELLO.
 14. What is meant by a hash function? What is its significance in a cryptosystem?

(14 × 1 = 14 weightage)

Part B

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

15. Prove that $n = \sum_{d|n} \varphi(d)$ $n \geq 1$.
 16. Prove that for $n \geq 1$, $\log n = \sum_{d|n} \wedge(d)$.
 17. Prove that a multiplicative function f is completely multiplicative if and only if $f^{-1}(n) = \mu(n)$ for $n \geq 1$.
 18. State and prove the Selberg's identity.
 19. Prove that $\lim_{x \rightarrow \infty} \left(\frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \right) = 0$.
 20. If p_n is the n th prime, prove that if $\lim_{x \rightarrow \infty} \frac{\pi(x) \log x}{x} = 1$ then $\lim_{x \rightarrow \infty} \frac{\pi(x) \log \pi x}{x} = 1$.
 21. If $A(x) = \sum_{n \leq x} \frac{\mu(n)}{n}$, prove that the relation $A(x) = o(1)$ as $x \rightarrow \infty$ implies the prime number theorem.
 22. Determine whether 219 is a quadratic residue or non-residue mod 383.
 23. Find the inverse of $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in M_2(\mathbb{Z}/26\mathbb{Z})$. Use it to decipher the message unit "QV".
 24. Explain the working of RSA cryptosystem using an example.

(7 × 2 = 14 weightage)

Part C

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

25. Prove that the set of all multiplicative functions f such that $f(1) \neq 0$ is subgroup of the group of all arithmetic functions.
 26. State and prove Shaprio's theorem.

27. State Gauss lemma. If m is the number defined in Gauss' lemma, prove that

$$m \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p} \right] + (n-1) \frac{p^2-1}{8} \pmod{2}.$$

28. Suppose that we intercept the message "S GNLIKD?KOZQLLIOMKUL.VY" (including the blank after the S) . Suppose that a linear enciphering transformation $C = AP$ is being used with a 30-letter alphabet, in which A-Z have the usual numerical equivalents 0 – 25, blank = 26, . = 27, , = 28, ? = 29. It is also known that the last six letters of the plaintext are the signature KARLA followed by a period. Find the deciphering matrix A^{-1} and the full plaintext message.

(2 × 4 = 8 weightage)