WEST BENGAL STATE UNIVERSITY

B.Sc. Honours 5th Semester Examination, 2021-22

MTMADSE02T-MATHEMATICS (DSE1/2)

NUMBER THEORY

Time Allotted: 2 Hours Full Marks: 50

The figures in the margin indicate full marks.
Candidates should answer in their own words and adhere to the word limit as practicable.
All symbols are of usual significance.

Answer Question No. 1 and any *five* from the rest

1. Answer any ***five*** questions from the following: 2×5 = 10

(a) If ϕ denotes the Euler's phi function, then prove that $\phi(n) \equiv 0 \pmod 2$, $\forall\, n \geq 3$.

(b) Solve $140x \equiv 133 \pmod{301}$.

(c) Check if Goldbach's conjecture is true for $n = 2022$.

(d) If n has a primitive root, prove that it has exactly $\phi(\phi(n))$ primitive roots.

(e) Find all solutions to the Diophantine equation $24x + 138y = 18$.

(f) In RSA encryption, is $e = 20$, a valid choice for $N = 11 \times 13$?

(g) List down the quadratic non-residues in $\mathbb{Z}_{10}^{*}$, with proper explanation.

(h) Prove that $(p-2)! \equiv 1 \pmod p$, where p is a prime.

(i) Find the number of positive divisors of $2^{2020} \times 3^{2021}$.

2. (a) If f is a multiplicative function and F is defined as $F(n) = \sum_{d\,|\,n} f(d)$, then prove F to be multiplicative as well. 5

(b) Prove that there exists a bijection between the set of positive divisors of p_1^{α} and p_2^{β}, if and only if $\alpha = \beta$, where p_1 and p_2 are distinct primes. 3

3. (a) For each positive integer n, show that 3

$$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$$

(b) Let x and y be real numbers. Prove that the greatest integer function satisfies the following properties: 3+2

(i) $[x+n] = [x] + n$ for any integer n

(ii) $[x] + [-x] = 0$ or -1 according to x is an integer or not

4. (a) Solve the congruence $72x \equiv 18 \pmod{42}$. 5

(b) Let a, b and m be integers with $m > 0$ and $\gcd(a, m) = 1$. Then prove that the congruence $ax \equiv b \pmod{m}$ has a unique solution. 3

5. (a) Prove that, in $\mathbb{Z}_n^*$, the set of all quadratic residues form a subgroup of $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{\bar{0}\}$. 4

(b) Prove that $\mathbb{Z}_{15}^*$ is not cyclic where $\mathbb{Z}_n^*$ is the collection of units in $\mathbb{Z}_n$. 4

6. (a) Suppose, c_1 and c_2 are two ciphertexts of the plaintexts m_1 and m_2 respectively, in an RSA encryption, using the same set of keys. Prove that, c_1c_2 is an encryption of m_1m_2. 3

(b) Prove that, in RSA encryption, the public key may never be even. 3

(c) Find $\phi(2021)$. 2

7. (a) Prove that there are no primitive roots for $\mathbb{Z}_8^*$. 2

(b) Let $\bar{g}$ be a primitive root for $\mathbb{Z}_p^*$, p being an odd prime. Prove that $\bar{g}$ or $\overline{g+p}$ is a primitive root for $\mathbb{Z}_{p^2}^*$. 6

8. (a) Prove that the Mobius μ-function is multiplicative. 6

(b) State the Mobius inversion formula. 2

9. (a) Show that Goldbach Conjecture implies that for each even integer $2n$ there exist integers n_1 and n_2 with $\Phi(n_1) + \Phi(n_2) = 2n$. 4

(b) Prove that the equation $\Phi(n) = 2p$, where p is a prime number and $2p+1$ is composite, is not solvable. 4

10. (a) Determine whether the following quadratic congruences are solvable: 2+2

(i) $x^2 \equiv 219 \pmod{419}$

(ii) $3x^2 + 6x + 5 \equiv 0 \pmod{89}$.

(b) Show that 7 and 18 are the only incongruent solutions of 4

$$x^2 \equiv -1 \pmod{5^2}$$

N.B. : *Students have to complete submission of their Answer Scripts through E-mail / Whatsapp to their own respective colleges on the same day / date of examination within 1 hour after end of exam. University / College authorities will not be held responsible for wrong submission (at in proper address). Students are strongly advised not to submit multiple copies of the same answer script.*

——×——