

BIRLA INSTITUTE OF TECHNOLOGY, MESRA, RANCHI  
(END SEMESTER EXAMINATION)

CLASS: I MSc  
BRANCH: MATHEMATICS AND COMPUTING

SEMESTER : IX  
SESSION : MO/2025

SUBJECT: MA502 NUMBER THEORY

TIME: 3 Hours

FULL MARKS: 50

**INSTRUCTIONS:**

1. The question paper contains 5 questions each of 10 marks and total 50 marks.
  2. Attempt all questions.
  3. The missing data, if any, may be assumed suitably.
  4. Before attempting the question paper, be sure that you have got the correct question paper.
  5. Tables/Data hand book/Graph paper etc. to be supplied to the candidates in the examination hall.
- 

		CO	BL
Q.1(a) Find all such $n$ with $\phi(n) = 8$ . Explain properly.	[5]	1	3
Q.1(b) Let $a$ and $b$ be coprime, then find the possible values of $(a+b, a-b)$ .	[5]	1	2
Q.2(a) Find the solution(s) of the following equations.	[5]	2	2
(i) $10x \equiv 15 \pmod{35}$			
(ii) $x \equiv 2 \pmod{4}$ and $x \equiv 6 \pmod{9}$			
Q.2(b) Find the integer in the unit place of $2^{2^{10}}$ .	[5]	2	4
Q.3(a) Generate the convergents of the expressions of $\sqrt{13}$ .	[5]	3	3
Then find the least positive solutions of $x^2 - 13y^2 = -1$ and			
$x^2 - 13y^2 = 1$ .			
Q.3(b) Define units in $Z[\sqrt{D}]$ in terms of the norm value, where $D > 0$ is a square-free integer. Is 41 prime in $Z[i]$ ? Explain.	[5]	4	2
Q.4(a) Use Pollard's rho method to find a factor of 2491.	[5]	4	2
Q.4(b) Is 561 to base 2 a pseudoprime number? Is it a Carmichael number? Justify your answer.	[5]	4	3
Q.5(a) Find $(-123   1009)$ .	[5]	1	3
Q.5(b) Explain the Diffie-Hellman key exchange algorithm. How does it enable two parties to establish a shared secret over an insecure channel?	[5]	5	1

:::21/11/2025:::E