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

CLASS: MSC & IMSC **SEMESTER : III & IX**
BRANCH: MATHEMATICS/ MATHEMATICS AND COMPUTING **SESSION : MO/2022**

SUBJECT: MA502 NUMBER THEORY

TIME: 3:00 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.

Q.1(a) State and prove fundamental theorem of arithmetic. [5]

Q.1(b) Obtain integers x and y satisfying $d = (178523,\ 4578) = 178523x + 4578y$ [5]

Q.2(a) Find all the primitive roots of the prime $p = 17$. [5]

Q.2(b) State and prove Wilson's Theorem. [5]

Q.3(a) Find the fundamental solution of $x^2 - 30y^2 = 1$. [5]

Q.3(b) Solve the linear Diophantine equation $56x + 72y = 40$. [5]

Q.4(a) Determine whether -104 is a quadratic residue or nonresidue of the prime 997. [5]

Q.4(b) Prove that $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. [5]

Q.5(a) Explain Public key cryptosystem with the help of an example. [5]

Q.5(b) Alice encrypts the plaintext message $P - 234$ using the RSA cryptosystem with Bob's public key $(n, e) = (2479,37 \times 67,169)$. What is the resulting ciphertext that would be sent to Bob? Find the corresponding decryption key d. [5]

:::::23/11/2022:::::E