CENTRAL INSTITUTE OF TECHNOLOGY KOKRAJHAR
(Deemed to be University)
KOKRAJHAR :: BTR :: ASSAM :: 783370

END – SEMESTER EXAMINATION
UG

Session: **July-Dec. 2024** Semester: **III** Time: **3Hrs**. Full Marks: **100**
Course Code: **UCSE302** Title: **Elementary Number Theory & Algebra**

Answer question no. 1 and any 4 from the rest

1. (a) Find the value of **-1 mod 12**.
(b) The minimum prime value is ...?
(c) The number of relatively prime less than 24 is ...?
(d) Ratio of two numbers is 3:4 and their LCM = 60, the GCD is ...?
(e) Find the value of x in **5x = 2 mod 7**
(f) In modular arithmetic : (a/b) = a(b^{-1}). (**True, False**)
(g) GCD(a, b) = GCD(b, a mod b), is this statement is always true?
(h) Identify a generator in the multiplicative group G = {1, ω, ω^2 }, where elements are the cube root of unity.
(i) $< G, * >$ is an abelian group. What criteria are needed to become a ring?
(j) A set of 2x2 matrices forms a group with the multiplicative operation. The identity element of the group is ...?

2 x 10

2. (a) Define Euler's Phi Function $\phi(n)$ with its properties.
(b) Using mathematical induction prove that for any prime p, $\phi(p) = p - 1$, assume that $\phi(1) = 1$.
(c) Find the value of $\phi(99)$.
(d) State the fundamental theorem of arithmetic and explain with an example.

5 + 7 + 4 + 4

3. (a) State the RSA algorithm.
(b) With this algorithm explain the encryption and decryption mechanism for the message ***m = 2*** with ***p = 3, q = 11***.
(c) Explain an efficient approach to check whether a number is prime (can be illustrated with an example).

7 + 7 + 6

4. (a) Consider the following **Cayley table** and show that it forms a group. Is it an abelian group? Identify the inverse of each element.
(b) Show that if G is an abelian group, then $(ab)^2 = a^2b^2$ for all $a, b \in G$.

(c) Define group isomorphism. Is the group $(\mathbb{Z}, +_3)$ isomorphic with the given group in the Cayley table?

$*$	**e**	**a**	**b**
e	e	a	b
a	a	b	e
b	b	e	a

$8 + 6 + 6$

5. (a) Define Subgroup and Coset.
(b) State the Lagrange Theorem.
(c) Define the Ring with zero divisors.
(d) What are the additional criteria for a ring to become an Integral domain?

$5 + 5 + 5 + 5$

6. Answer any five:
(a) If divide a number by 5 the remainder is 3, and if divide it by 7 the remainder is 5. Find the number.
(b) If you divide a number by 7 the remainder is 5. What will be the remainder when *three times that number* is divided by 7?
(c) Define **Mobious function** and find the value of $\mu(6)$
(d) Find the value of 4^{99} **mod 35**.
(e) Define Group homomorphism.
(f) State the difference between Rind and Field.
(g) In $\mathbb{Z}_3[x]$, $f(x) = 1 + x$ and $g(x) = 2 + x$. Find the value of $f(x) + g(x)$.

4 x 5

( )

Central Institute Of Technology
Kokrajhar : : Bodoland
ESTD. : 2006
असतो मा सत गमय
तमसो मा ज्योतिर्गमय