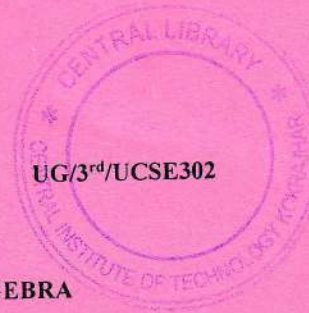


Total number of printed pages:4



2021

NUMBER THEORY AND ALGEBRA

Full Marks: 100

Time: Three hours

The figures in the margin indicate full marks for the questions.

Answer any five questions.

1. (a) Write the Correct option:

5 X 2 = 10

- (i). The number of identity element in a finite group is.....(one/two/four/undefined)
 - (ii). The inverse of any element of a subgroup is the same as the inverse element of the group. (True/False)
 - (iii). Consider the group $(\mathbb{Z}, +)$. Let $H = \{3n: n \text{ is an integer}\}$. Then H is(subgroup of \mathbb{Z} /Normal subgroup of \mathbb{Z} /not a subgroup of \mathbb{Z}).
 - (iv). The ring of integers $(\mathbb{Z}, +, \dots)$ is an(integral domain/field/neither a field nor an integral domain)
 - (v). Consider the ring $(\mathbb{R}, +, \cdot)$. Then $(\{0\}, +, \cdot)$ is a.....(improper subring of \mathbb{R} /proper subring of \mathbb{R} / not a subring of \mathbb{R})
- 1 (b). Show that intersection of two subrings is a ring R is again a subring of R. (3)
- 1 (c). Prove that if any element 'a' has the multiplicative inverse, then 'a' cannot be a divisor of zero, where the underlying set is a ring. (3)
- 1 (d). Prove that every field is an integral domain. (4)

2.

- (a). If G is a cyclic group and N is a subgroup of G then prove that G/N is a cyclic group. (5)
- (b). State and prove the Lagrange Theorem for a finite group. (1+ 5 = 6)
- (c). Prove that every cyclic group is abelian. (5)
- (d) Examine whether the algebraic structure $(\mathbb{Z}, -)$, where '-' denotes the binary operation of subtraction on \mathbb{Z} , is a group or not. (4)

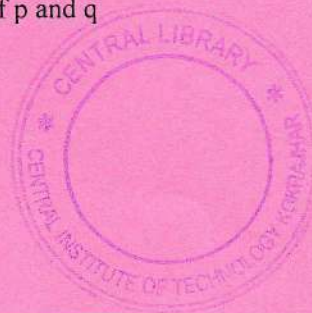
3.

- (a) Show that if every element of a group $(G, *)$ be its own inverse, then it is an abelian group. (5)
- (b) Let $G = \{1, -1, i, -i\}$ be a multiplicative group. Find the order of every element. (4)
- (c) Let H be a subgroup of G and a and b belongs to G . Then, prove that
- (i) $aH = bH$ if and only if $a^{-1}b \in H$ (3+2=5)
- (ii) $aH = H$ if and only if $a \in H$.
- (d) Prove that every subgroup of an abelian group is normal. The converse need not be true. Give an example of such a group. (3+3 = 6)

4. (a) Fill in the blanks

$2 \times 10 = 20$

- (i) An integer n is prime if it is not divisible by any prime less than or equal to _____
- (ii) The integers a and b are _____ if $\gcd(a, b) = 1$.
- (iii) A simple octagon can be triangulated into _____ triangles.
- (iv) In RSA, $\Phi(n) =$ _____ in terms of p and q



- (v) In RSA, we select a value 'e' such that it lies between 0 and $\Phi(n)$ and it is relatively prime to $\Phi(n)$: _____
(TRUE/FALSE).
- (vi) In the RSA algorithm, we select 2 random large values 'p' and 'q' where p and q should be co-prime): _____
(TRUE/FALSE).
- (vii) If $p > 0$ is a prime integer, and a is any unit modulo p, then _____
 $\equiv 1 \pmod{p}$.
- (viii) The RSA is a symmetric encryption / decryption procedure: _____
(TRUE/FALSE).
- (ix) The public key encryption system uses 2 keys: _____
(TRUE/FALSE).
- (x) If a, b are two distinct prime number than a highest common factor of a, b is _____

5.

(a) State Well-Ordering Principle. Using principle of Mathematical Induction, prove that the cube of any integer can be written as the difference of two squares. [8]

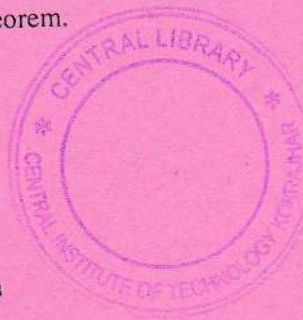
(b) Define Triangulation. Ackermann number is defined as follows for nonnegative integers m and n:

$$A(m, n) = \begin{cases} n + 1 & \text{if } m = 0 \\ A(m - 1, 1) & \text{if } m > 0 \text{ and } n = 0 \\ A(m - 1, A(m, n - 1)) & \text{if } m > 0 \text{ and } n > 0 \end{cases}$$

find $A(2, 2)$

(c) Write the Fermat's Little Theorem.

[4]



- 6.
- (a) Find $\text{GCD}(10764, 2300)$ using the Euclidean algorithm. [5]
 - b) Show that if $a, b, c,$ and m are integers such that $m \geq 2, c > 0,$ and $a \equiv b \pmod{m},$ then $a^c \equiv b^c \pmod{m}.$ [7]
 - c) Prove that if n is an positive integer, then $n^2 \equiv 1 \pmod{8}.$ [8]

