Total number of printed pages: **Programme(UZG)/3rd Sem (Back)/UCSE302**

2024

Elementary 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)	Define Euler's Phi Function. Write the properties of this function. Write some utilities of this function. Calculate the value of $\Phi(30)$.	12 + 8
	b)	Write the RSA algorithm.	
2.	a)	State the principle of mathematical induction. Using the principle of mathematical induction, prove that $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \ldots\ldots + n(n+1) = (1/3)\{n(n+1)(n+2)\}$.	15 + 5
	b)	The LCM of two numbers are 1200, which must not be a factor of GCD? i) 600 ii) 300 iii) 500 iv) 400	
3.	a)	Covert the Binary number to Decimal number: (i)100011.110 (ii)1011101111	4 x 5
	b)	Covert the Octal number to Decimal number: (i)147.110 (ii) 1756	
	c)	Covert the Hexadecimal number to Decimal number: (i) ABA (ii) 15CA	
	d)	Covert the Decimal number to Binary number: (i) 0.125 (ii) 11.10	
4.	a)	Define Cyclic group. Is the cyclic group is abelian group? Explain your answer.	10+10
	b)	Show that $\{1, \omega, \omega^2\}$ is a cyclic group under multiplication. Find the generator of the group. [ω is the cube root of unity]	
5.	a)	State the Chinese Remainder Theorem. Write its applications.	5 + 15
	b)	Using this theorem find the value of x from, $2x = 1 (\text{mod } 5)$ $3x = 9 (\text{mod } 6)$ $4x = 1 (\text{mod } 7)$ $5x = 9 (\text{mod } 11)$	
6.		Write the short note on	4 x 5
		i) Plain text and Cipher text ii) Public key and Private key iii) Encryption and Decryption iv) Symmetric key and Asymmetric key	