Total No. of printed pages = 3

19/3rd Sem/UCSE302

2021

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. (i) Discuss Mathematical Induction in details. 10

   (ii) Use Mathematical Induction to prove that sum of the first n odd positive integer is n^2. 10

2. (i) Discuss Eular's Phi function. What is value of $\Phi(240)$? 5+5=10

   (ii) Discuss Fermat's little theorem. Using Fermat's little theorem, find the remainder when you divide $3^{100,000}$ by 53. 10

[Turn over

3. Using Chinese remainder theorem solve the value of x : 20

$3x \equiv 1 \pmod{5}$

$4x \equiv 6 \pmod{14}$

$5x \equiv 11 \pmod{3}$.

4. (i) Discuss properties of a group in details. 8

(ii) Prove that $Z_4 = \{0,1,2,3\}$ is an Abelian group with respect to 'addition modulo 4'. 12

5. (i) What is the full form of RSA ? 2

(ii) Write RSA algorithm. 8

(iii) In an RSA cryptosystem, a particular A uses to prime numbers 13 and 17, to generate the public key and private key. 10

6. (i) Explain various types of active attack and passive attack in details. 10

(ii) Discuss Well Ordering Principles in details. 10

7. Write short notes on any *four* : 5×4=20

(i) Symmetric key and Asymmetric key cryptography.

(ii) Active attack and Passive attack

(iii) Rings

(iv) Cayley's theorem

(v) Euclidean's algorithm.