End Sem Q.P.

Exam Date & Time: 27-Nov-2024 (09:30 AM - 12:30 PM)

MANIPAL ACADEMY OF HIGHER EDUCATION

MAT 2187 ELEMENTARY NUMBER THEORY

ELEMENTARY NUMBER THEORY [MAT 2137]

Marks: 50 **Duration: 180 mins.**

Descriptive

Answer all the questions. Section Duration: 180 mins

Answer ALL the questions.Assume missed data suitably.

1A) Find GCD(423, 198) and express it as linear combination of 423 and 198. (3)

1B) Determine all solutions in the integers of the Diophantine equation, 12x + 25y = 331. (3)

1C) Express the prime 3877 as a sum of two squares if $3877 \mid (15^6 + 1)$ (4)

2A) Solve the system of congruences using Chinese Remainder Theorem
$x \equiv 5\ (mod\ 6),\ x \equiv 4\ (mod\ 11),\ x \equiv 3\ (mod\ 17)$ (3)

2B) Using generalized Fermat's factorization, factor 17018759. (3)

2C) State and prove Wilson's Theorem (4)

3A) Prove that $\sum_{d|n} \frac{1}{d} = \frac{\sigma(n)}{n}$ for all n>0. (3)

3B) Find the highest power of 5 dividing $1000!$ and the highest power of 7 dividing $2000!$ (3)

3C) Prove that $a^{\phi(m)} \equiv 1\ (mod\ m)$ (Generalization of FLT) (4)

4A) Evaluate Legendre symbol: $\left(\frac{3083}{3911}\right)$ (2)

4B) Compute Euler phi function, $\phi(9968)$ (2)

4C) Find square root of 432 modulo 673 using the least non-residue modulo 673. (6)

5A) You have received a trigraph message “BBI” which was encryption of a digraph plaintext in 26-letter alphabet using RSA cryptosystem. Suppose your public key is K_E =(1073, 275), read the message. (3)

5B) If the investigating team revealed the plaintext “TAKE” by decrypting the ciphertext “EUXT” which was due to encryption using an affine mapping of digraphs over 27-letters alphabet with 26=blank. Help the team by decoding the word “FUYT” which was encrypted by the same group of criminals escaped last week. (3)

5C) The message "REPLYTODAY" must be encrypted in ElGamal Cryptosystem in 26 letter alphabet, and forwarded to the user with public key K_E =(p,g,g^a)=(47,5,10). Select k=13 and encrypt the message. Also decipher the message to verify, if the secret key of the user is a=19. (4)

-----End-----