Exam Date & Time: 02-Jan-2025 (09:30 AM - 12:30 PM)

Make-up Q.P.

# MANIPAL ACADEMY OF HIGHER EDUCATION

Elementary Number Theory

## ELEMENTARY NUMBER THEORY [MAT 2137]

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

**A**

**Answer all the questions.** Section Duration: 180 mins

Answer all questions

1A) State and prove the division algorithm. (4)

1B) Find GCD(12378, 3054) and express it as linear combination of 12378 and 3054. (3)

1C) Determine all solutions of the Diophantine equation, 172x + 20y = 1000. (3)

2A) State and prove Fermat's Little Theorem. (4)

2B) Solve the system of congruences using Chinese Remainder Theorem $x \equiv 1 \; mod \; 2$ ,

$x \equiv 2 \; mod \; 3$, (3)

$x \equiv 3 \; mod \; 5$

2C) Using generalized Fermat's factorization, factor 141467. (3)

3A) Show that $18! \equiv -1 (mod \; 437)$. (4)

3B) Prove that $[x] + [y] \leq [x + y]$ (3)

3C) If $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots . p_r^{\alpha_r}$, for n>1, then prove that

$1 > \frac{n}{\sigma(n)} > \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots ..(1 - \frac{1}{p_r})$. (3)

4A) Find square root of 186 modulo 401 using the least non-residue modulo 401. (5)

4B) What is Euler phi-function $\varphi(n)$. If $\varphi(3589) = 3456$, factor 3589 into product of two primes. (3)

4C) Evaluate Legendre symbol $\left(\frac{7411}{9283}\right)$ (2)

5A) Send the message "SELL" using ElGamal Cryptosystem to the user with public key $K_E$ =(p, g, $g^a$ )=(43, 3, 22) by selecting k=23. Also decipher the message to verify, if the secret key of user is a=15. (4)

5B) Police could find out that the word "LOVE", was an encryption of the word "KILL" using an affine mapping of digraphs over 31 letters alphabet with 26=blank, 27=&, 28=@, 29=! and 30=?. But the police could not decode the word "YUKA" which was encrypted by the same group of criminals escaped last week. Help the police by decoding it. (3)

5C) Using RSA cryptosystem to encrypt plaintexts in digraphs to ciphertexts in trigraphs, send the message "DONE" over 26 letter alphabets, to your friend who has the public key $(n, e) = (899, 7)$. Also verify whether your friend can read the message. (3)

-----End-----