SPECIFY TYPE OF EXAMINATION

FIRST ATTEMPT ☐
FIRST RESIT ☐
SECOND RESIT ☐
RE-TAKE ☐

JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF IT

2ND YEAR 1ST SEMESTER 2021/2022 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ICB 1209

COURSE TITLE: INTRODUCTION TO NUMBER THEORY

DATE: **TIME:**

TIME: 2 HOURS

Instructions:

Answer question ONE and ANY other TWO questions.

QUESTION 1 (30 MARKS)

(a) State four properties of real numbers. (4 marks)

(b) Suppose a, b and c are integers, prove that
(i) If $a|b$and b|c, then a|c. (3 marks)
(ii) state the steps in RSA encryption scheme (3 marks)
(c) Given that $a = 573$ *and* $b = -16$, find the integers q *and* r such that
$a = bq + r$ *and* $0 < r < b$. (4 marks)
(d) Let 8316 a = and 19800 b = . Express each number in its prime factors and hence find:
(i) gcd(a,b) (2 marks)
(ii) lcm(a,b) (2 marks)
(e) State and prove Fermat's Little Theorem. (4 marks)
(f) Prove that if gcd(a,b)=1 and that a and b both divide c, then ab divides c. (4 marks)
(g) Solve the congruence equation $8x \equiv 12 \pmod{28}$ (4 marks)

QUESTION TWO (20 MARKS)

1. (a) Use the Euclidean algorithm to compute the greatest common divisor (217,161) (5 marks)

   (b) Solve the linear equation 217x − 161y = 21 or explain why there are no solutions. (10marks)

   (c) Let a, b, c, and n be integers. Prove that

   if a≡b(modn) and c≡d(modn), then a−c≡b−d(modn). (5 marks)

QUESTION THREE (20 MARKS)

a. Define the Chinese Remainder Theorem. (2 marks)

b. Use the Chinese Remainder Theorem to solve the simultaneous congruences
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$
$x \equiv -1 \pmod{11}$. (10 marks)

c. Calculate the continued fraction expansion of 4169/3864 (8 marks)

QUESTION FOUR (20 MARKS)

(a) DEFINE the term prime. (1 mark)

(b) PROVE that there are infinitely many primes. (3 marks)

(c) state the Principle of Mathematical Induction (PMI) (2 marks)

(d) Use mathematical induction to prove that, for n $\in$ **N**, we have

$1 + 2 + 3 + \_\,\_\,\_ + (n - 1) + n = \frac{n(n+1)}{2}$ (5 marks)

Can you also prove this formula more directly, without using induction? If so, how? (2 marks)

(e) Find the least common multiple and the greatest common divisor of $2^5 5^6 7^2 11$ and $2^3 5^8 7^2 13$.
Let $a = 2^4 13^2 17$, $b = 2^3 5\ 13$. Find the following:
(a) The prime factorization of (a, b)
(b) The prime factorization of $[a, b]$ (4 marks)

(f) Determine the prime factorization of 13832000 (3 marks)

QUESTION FIVE (20 MARKS)

(a) What is meant by the term 'Cryptography'? (1 mark)
(b) Why is modular arithmetic key to cryptography? (3 marks)
(c) Describe the steps in Diffie-Hellman key exchange algorithm and state why it works. (10 marks)
(d) Suppose that two parties A and B wish to set up a common secret key (D-H key) between themselves using the Diffie Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. Calculate their D-H key. (6 marks)