KISII UNIVERSITY

UNIVERSITY EXAMINATIONS

FOURTH YEAR EXAMINATION FOR THE AWARD OF THE DEGREE OF BACHELOR OF SCIENCE IN APPLIED COMPUTING SCIENCE

SECOND SEMESTER 2023/2024

[JAN – APRIL, 2024]

COMP 471/SOEN 490: NUMBER THEORY AND CRYPTOGRAPHY

STREAM: Y4 S2 **TIME: 2 HOURS**

DAY: FRIDAY, 12:00 - 2:00 P.M. **DATE: 19/04/2024**

INSTRUCTIONS

1. ***Do not write anything on this question paper.***
2. ***Answer question ONE (Compulsory) and any other TWO questions.***

QUESTION ONE [30MKS]

a) Describe commutative, associativity, identity and distributivity properties of multiplication of integers for all $a, b, and\ c \in \mathbb{Z}$ [4 marks]

b) For each of the following numbers a and n, find the quotient q and the remainder r when you divide a by n, and write down the equation

$$a = qn + r.$$

i.) $a = 0, n = 11$ [2 marks]

ii.) $a = -58, n = 5$ [2 marks]

c) Consider the following set and state whether they have the well-ordering principle. Explain your answer.

If $A=\{n \in \mathbb{N} | n^2 + 3n - 200 > 0\}$ [2marks]

d) By hand determine:

i.) whether $6 | b$, where b is 835223497694005987. [4 marks]

ii.) Whether $7 | b$, where b = 117,649 [4 marks]

e) Define the Theorem: (Criterion of Divisibility by 8). With an example of your choice explain why it is the simplest criterion. [2 marks]

f) Find all the positive divisors of 100. [2 marks]

g) Which of the following congruences are true? Work it out to justify your answer.
   i.) $11 \equiv 26 \pmod 5$ [1mark]
   ii.) $38 \equiv 0 \pmod{13}$ [1mark]
h) Find the least residue of 17 x 14 modulo 19. [2 marks]
i) Plot the residue class of -1 modulo 4 on a number line. [4 marks]

QUESTION TWO [20MKS]

a) Answer the following questions regarding the Sieve of Eratosthenes algorithm.
   i.) Why is it referred to as a sieve? [1 mark]
   ii.) Discuss in details the four main steps in the Sieve of Eratosthenes algorithm [4 marks]
   iii.) Using the Sieve of Eratosthenes, find all the prime numbers when n = 200. [5 marks]
b) Answer the following questions regarding Euclid's algorithm.
   i.) Explain the importance of Euclid's algorithm in computer science [2 marks]
   ii.) Using Euclid's algorithm, find the highest common factor of each of the following pairs of integers.
      i.) 93 and 21 [4marks]
      ii.) 138 and 61 [4 marks]

QUESTION THREE [20MKS]

a) Using the Bézout's theorem to find integers v and w with $av + bw = d$ when a and b are both positive. Find the highest common factor d, of 93 and 42 and then find integers v and w such that $93v + 42w = d$. [6 marks]
b) Does the following 10-digit code satisfy the ISBN congruence check?
   0521683726 [6 marks]
c) For each of the following values of a and n, determine whether a multiplicative inverse of a modulo n exists and, if it does, find one.
   i.) $a = 84, n = 217$
   [4mks]
   ii.) $a = 43, n = 96$ [4 marks]

QUESTION FOUR [20MKS]

a) In your understanding, explain how the various Number theory concepts have been used to ensure that information is secure. [8 marks]
b) Explain the following processes with examples as they are used in Number Theory & Cryptography.
   i.) Enciphering [6 marks]

ii.) Deciphering [6 marks]

QUESTION FIVE [20MKS]

a) Deciphering a message that has been enciphered using an affine cipher. Suppose you receive the enciphered message 5, 17, 18, 7, which you know has been created using the affine cipher

$$E(x) \equiv 9x + 21 \pmod{26}$$

What does the message say? [Use the conversation table for letters and number below – (**Table 1**). [10 marks]

b) In detail discuss history, applications, impact, and real-life use of number theory in cryptography. [10 marks]

Table 1. Conversion table for letter and numbers.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25