KISII UNIVERSITY

UNIVERSITY EXAMINATIONS

FOURTH YEAR EXAMINATION FOR THE AWARD OF THE DEGREE OF BACHELOR OF SCIENCE IN APPLIED COMPUTER/INFORMATION TECHNOLOGY
FIRST SEMESTER 2022/2023
[SEPTEMBER-DECEMBER, 2022]

ACMP 455/BIT 400: NUMBER THEORY AND CRYPTOGRAPHY

STREAM: Y4S1 **TIME: 2 HOURS**

DAY: TUESDAY, 9:00 – 11:00 AM **DATE: 20/12/2022**

INSTRUCTIONS

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

QUESTION ONE (30MKS)

a) Using relevant examples, describe the transitivity and linear combination basic properties of divisibility. For the theorem, let a, b, c, x and y be integers ($\mathbb{Z}$). [6marks]

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. $a = 59$, $n = 7$ [2marks]

ii. $a = -100$, $n = 9$ [2marks]

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

$$A = \{n \in \mathbb{N} \mid n.\sin(2n) > 8\}$$ [2marks]

d) By hand determine:

i. Whether $6 \mid b$, where b is 83522349769400598 [2marks]

ii. Whether $7 \mid b$, where b = 16,807 [4marks]

e) Define the Theorem: (Criterion of Divisibility by 3). With an example of your choice explain how it can be improved. [4marks]

f) Find all the positive divisors of 120. [2marks]

g) Answer the following questions in relation to congruences:

i. Describe the reflexivity, symmetry and transitivity properties of congruences. [3marks]

ii. State whether the following congruence is true:

$$11 \equiv 26 \pmod 5$$ [1mark]

QUESTION TWO (20MKS)

1. Answer the following questions regarding the Sieve of Eratosthenes algorithm.
   a) Why is it referred to as a sieve? [1mark]
   b) Discuss in details the four main steps in the Sieve of Eratosthenes algorithm [4marks]
   c) Using the Sieve of Eratosthenes, find all the prime numbers when n = 110. [5marks]
2. Answer the following questions regarding Euclid's algorithm.
   a) Explain the importance of Euclid's algorithm in computer science [2marks]
   b) Using Euclid's algorithm, find the highest common factor of each of the following pairs of integers.
      i. 93 and 21 [4marks]
      ii. 231 and 49 [4marks]

QUESTION THREE (20MKS)

1. 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 70 and 29 and then find integers v and w such that $70v + 29w = d$. [6marks]
2. Does the following 10-digit code satisfy the ISBN congruence check?
   0521683726 [6marks]

QUESTION FOUR (20MKS)

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

QUESTION FIVE (20MKS)

1. Deciphering a message that has been enciphered using an affine cipher. Suppose you receive the enciphered message 3, 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]. [10marks]

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

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