University of Colombo, Sri Lanka

University of Colombo School of Computing

BACHELOR OF SCIENCE IN COMPUTER SCIENCE

Second Year Examination - Semester II - UCSC AY20 [held in March/ April 2024]

SCS 2210 Discrete Mathematics II

(Two (2) Hours)

Answer ALL questions

Number of Pages = 13 Number of Questions = 4

To be completed by the candidate

Index Number: | | | | | | | | |

99

Important Instructions to candidates:

I. Students should answer in the medium of English language only using the space provided in this question paper.

II. Note that questions appear on both sides of the paper. If a page or a part of this question paper is not printed, please inform the supervisor immediately.

III. Write your index number CLEARLY on each and every page of this Question paper.

IV. This paper consists of 4 questions in **13** pages (including the Cover Page).

V. Answer ALL questions. All questions carry equal marks (25 marks).

VI. Calculators and any electronic device capable of storing and retrieving text including electronic dictionaries, smartwatches and mobile phones are **not allowed.**

VII. Do not tear off any part of this answer book. Under no circumstances may this book, used or unused, be removed from the Examination Hall by a candidate

To be completed by the examiners

Question No	Marks
1	
2	
3	
4	
Total	

Index No: ....

Question 1

(a) Let a, b and c be integers and m be a positive integer. If $ac \equiv bc(mod\, m)$ and $gdc(c, m) = 1$ then show that $a \equiv b\ (mod\, m)$.

[6 Marks]

(b) Solve the linear congruence $120x \equiv 52\ mod\ 119$ and show that all possible values of x are in the form $x = t + 119k,\ t, k \in Z$, where Z is the set of all integers.

[7 Marks]

Index No: ....

(c) Solve the following system of congruences:

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 2 \pmod 4 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 3 \pmod 7. \end{aligned}$$

[7 Marks]

Index No: ....

(d) Prove or disprove that both 3 and 4 are primitive roots modulo 7.

[5 Marks]

Question 2

(a) The RSA algorithm is the foundation of the cryptosystem that provides the basis for securing data. Focus on RSA-based encryption and decryption. Subsequently, respond to the following questions.

(i) Utilize the prime numbers 7 and 11 to generate an encryption key.

[4 Marks]

(ii) Employ the aforementioned encryption key to encrypt the plaintext message "9" and derive the corresponding ciphertext.

[6 Marks]

(iii) Formulate an expression to ascertain the appropriate decryption key to decrypt the aforementioned ciphertext.

[5 Marks]

(iv) Utilize the provided decryption key and formulate an expression to deduce the original message.

[4 Marks]

(b) Let $f(x) = \sum_{k=0}^{\infty} a_k x^k$ and $g(x) = \sum_{k=0}^{\infty} b_k\, x^k$ be the generating functions for the sequences $(a_k)_{k=0}^{\infty}$ and $(b_k)_{k=0}^{\infty}$ respectively.

(i) Find the generating function for $f(x).g(x)$ and $f(x) + g(x)$.

[3 Marks]

(ii) Let $f\ (x) = 1/(1 - x)^2$. Find the coefficients of the generating function of $f\ (x)$.

[3 Marks]

Index No: ....

Question 3

(a) Explain how to solve a non-homogeneous recurrence relation.

[4 Marks]

(b) Looking at the recurrence relation $a_n = 2a_{n-1} - a_{n-2} + 2^n \ (n \geq 2)$, state what type of recurrence relation it is and solve it while finding the closed formula when $a_0 = 1 \ and \ a_1 = 2$.

F(n)	Particular Guess
c	C or A
n	cn + d or $A_1 n + A_0$
n^2	$cn^2 + dn + e$ or $A_2 n^2 + A_1 n + A_0$
r^n	Ar^n or Cr^n

[6 Marks]

(c) A person decides to invest in a savings account with an initial deposit of P dollars. The account has an annual interest rate of r (expressed as a decimal). In addition to the interest, the person decides to make an annual deposit of D dollars at the end of each year, starting from the end of the first year. The interest is compounded annually, and the annual deposit is added after the interest is applied. This process can be modeled by a recurrence relation for an Amount A_n in the account after n years.

i. Define a recurrence relation for this scenario. [3 marks]

Index No: ....

ii. Derive the explicit formula for A_n , which is the account balance after n years, based on the defined recurrence relation. [6 Marks]

iii. If the initial deposit is \$1000 (P_0= 1000), and the annual interest rate is 5% (r =0.05) with an annual deposit of \$100, calculate the account balance after 5 years from the explicit formula derived in the part ~~(b)~~ (ii).

[6 Marks]

Index No: ....

Question 4

a) i. A password consists of 3 letters followed by 3 digits. The letters can be any uppercase English alphabet letters, and the digits can be from 0 to 9. How many such distinct passwords can be created if repetition is allowed for both letters and digits?

ii. A club has 12 members. In how many ways can a president, a vice president, and a treasurer be elected if each member can hold only one position?

iii. From a group of 7 men and 5 women, a committee of 5 people is to be formed. How many different committees can be formed if the committee must consist of 3 men and 2 women?

iv. How many ways can 5 distinct rings be placed on 4 fingers if no finger can have more than one ring?

[2x4 Marks]

Index No: ....

b) Expand the binomial $(2 - x)^{-3}$ up to the x^3 term.

[6 Marks]

c) A conference center has a rectangular room that measures 25 meters in length and 20 meters in width. Due to safety regulations:

-Each person requires at least 2 square meters of space.
-An additional buffer zone of 1 meter must be maintained around the edges of the room to ensure clear access to emergency exits.
The center wants to maximize the number of people that can be accommodated for a large meeting while adhering to these conditions. Determine the maximum number of people that can be safely accommodated in the room.

[3 Marks]

Index No: ....

d) A manufacturing company has developed a new production line that involves batches of productions. The output of each production depends on the outputs of three batches plus an external factor that increases linearly with time. Specifically, the number of units produced in any given month n, (P_n) is equal to the sum of the units produced in the three previous months, plus an additional double n units (2n), where n represents the month number (with the process starting at n=1 and the recursion n>3).

The company recorded the following initial outputs:

- In the first month (n=1), 10 units were produced (P_1=10).
- In the second month (n=2), 20 units were produced (P_2=20).
- In the third month (n=3), 30 units were produced (P_3=30).

Determine the number of units produced in the sixth month (P_6)

[3 Marks]

e) Consider a simplified model for the population growth of a certain species in a constrained environment, where the population at time n+1 depends nonlinearly on the population at time n and $n-1$. The model is given by the recurrence relation:

$$P_{n+1} = P_n.(2 - \frac{P_{n-1}}{K})$$

P_n is the population at time n (n>0), K is the environmental carrying capacity (a positive constant that represents the maximum population the environment can sustain), and Initial conditions are $P_0 = 1$ and $P_1 = 2$.

While clearly stating your assumptions, analyze the first few terms to understand how the population changes over time and discuss the impact of the carrying capacity K.

[5 Marks]

****