FAST- National University of Computer and Emerging Sciences, Karachi.

FAST School of Computing
Assignment # 2, Fall 2021.
CS1005-Discrete Structures

<u>Instructions:</u> **Max. Points: 100**

1- This is hand written assignment.
2- Just write the question number instead of writing the whole question.
3- You can only use A4 size paper for solving the assignment.

---

1. Let R be the following relation defined on the set {a, b, c, d}:

   R = {(a, a), (a, c), (a, d), (b, a), (b, b), (b, c), (b, d), (c, b), (c, c), (d, b), (d, d)}.

   Determine whether R is:
   (a) Reflexive (b) Symmetric (c) Antisymmetric
   (d) Transitive (e) Irreflexive (f) Asymmetric

2. Let *R* be the following relation on the set of real numbers:

   $aRb \leftrightarrow \lfloor a \rfloor = \lfloor b \rfloor$, where $\lfloor x \rfloor$ is the floor of x.

   Determine whether R is:
   (a) Reflexive (b) Symmetric (c) Antisymmetric
   (d) Transitive (e) Irreflexive (f) Asymmetric

3. List the ordered pairs in the relation R from A = {0, 1, 2, 3, 4} to B = {0, 1, 2, 3}, where (a, b) ∈ R if and only if
   a) a = b. b) a + b = 4. c) a > b.
   d) a | b. e) gcd(a, b) = 1. f) lcm (a, b) = 2.

4. List all the ordered pairs in the relation R = {(a, b) | a divides b} on the set {1, 2, 3, 4, 5, 6}. Display this relation as Directed Graph(digraph), as well in matrix form.

5. For each of these relations on the set {1, 2, 3, 4}, decide whether it is reflexive, whether it is symmetric, whether it is antisymmetric, and whether it is transitive.

   a) {(2, 2), (2, 3), (2, 4), (3, 2), (3, 3), (3, 4)}
   b) {(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4)}
   c) {(2, 4), (4, 2)}
   d) {(1, 2), (2, 3), (3, 4)}
   e) {(1, 1), (2, 2), (3, 3), (4, 4)}
   f) {(1, 3), (1, 4), (2, 3), (2, 4), (3, 1), (3, 4)}

6. Determine whether the relation R on the set of all people is reflexive, symmetric, antisymmetric, Asymmetric, irreflexive and/or transitive, where (a, b) ∈ R if and only if:

   a) a is taller than b.
   b) a and b were born on the same day.
   c) a has the same first name as b.
   d) a and b have a common grandparent.

7. Give an example of a relation on a set that is
   a) both symmetric and antisymmetric.
   b) neither symmetric nor antisymmetric

8. Consider these relations on the set of real numbers: A= {1,2,3}
R1 = {(a, b) ∈ R | a > b}, the "greater than" relation,
R2 = {(a, b) ∈ R | a ≥ b}, the "greater than or equal to "relation,
R3 = {(a, b) ∈ R | a < b}, the "less than" relation,
R4 = {(a, b) ∈ R | a ≤ b}, the "less than or equal to "relation,
R5 = {(a, b) ∈ R | a = b}, the "equal to" relation,
R6 = {(a, b) ∈ R | a ≠ b}, the "unequal to" relation.

Find:

a) R2 ∪ R4. b) R3 ∪ R6. c) R3 ∩ R6. d) R4 ∩ R6.
e) R3 − R6. f) R6 − R3. g) R2 ⊕ R6. h) R3 ⊕ R5.
i) R2 ◦ R1. j) R6 ◦ R6.

9. (a) Represent each of these relations on {1 , 2 , 3 } with a matrix(with the elements of this set listed in increasing order).
   i) { (1 , 1), (1 , 2), (1 , 3) }
   ii) { (1 , 2), (2 , 1), (2 , 2) ,(3 , 3) }
   iii) { (1 , 1), (1 , 2), (1 , 3) , (2 , 2), (2 , 3) ,(3 , 3) }
   iv) { (1 , 3), (3 , 1) }

(b) List the ordered pairs in the relations on { 1 , 2 , 3 } corresponding to these matrices(where rows and columns correspond to the integers listed in increasing order).

(i) $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$ (ii) $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ (iii) $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

10. (a) Suppose that *R* is the relation on the set of strings of English letters such that *aRb* if and only if *l*(*a*) = *l*(*b*), where *l*(*x*) is the length of the string *x*. Is *R* an equivalence relation?

(b) Let *m* be an integer with *m* > 1. Show that the relation *R* = {(*a*,*b*) | *a* ≡ *b* (mod *m*)} is an equivalence relation on the set of integers.

(c) Let m be a positive integer. Show that a ≡ b (mod m) if a mod m = b mod m.

11. What are the quotient and remainder when:
   a) 19 is divided by 7? b) −111 is divided by 11?
   c) 789 is divided by 23? d) 1001 is divided by 13?
   e) 10 is divided by 19? f) 3 is divided by 5?
   g) −1 is divided by 3? h) 4 is divided by 1?

12. (a) Find a div m and a mod m when
   i) a = −111, m = 99. ii) a = −9999, m = 101.
   iii) a = 10299, m = 999. iv) a = 123456, m = 1001.

   (b) Decide whether each of these integers is congruent to 5 modulo 17.
   i) 80 ii) 103 iii) −29 iv) −122

13. (a) Determine whether the integers in each of these sets are pairwise relatively prime.
   i) 11, 15, 19 ii) 14, 15, 21 iii) 12, 17, 31, 37 iv) 7, 8, 9, 11

(b) Find the prime factorization of each of these integers.

i) 88 ii) 126 iii) 729 iv) 1001 v) 1111 vi) 909

14. Use the extended Euclidean algorithm to express gcd (144, 89) and gcd (1001, 100001) as a linear combination.

15. Solve each of these congruences using the modular inverses.

a) $55x \equiv 34 \pmod{89}$ b) $89x \equiv 2 \pmod{232}$

16. (a) Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences.

i) $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, and $x \equiv 3 \pmod 7$.

ii) $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, and $x \equiv 4 \pmod{11}$.

(b) An old man goes to market and a camel step on his basket and crushes the oranges. The camel rider offers to pay for the damages and asks him how many oranges he had brought. He does not remember the exact number, but when he had taken them out five at a time, there were 3 oranges left. When he took them six at a time, there were also three oranges left, when he had taken them out seven at a time, there was only one orange was left and when he had taken them out eleven at a time, there was no orange left. What is the number of oranges he could have had?

17. Find an inverse of *a modulo m* for each of these pairs of relatively prime integers.

a) $a = 2, m = 17$ b) $a = 34, m = 89$

c) $a = 144, m = 233$ d) $a = 200, m = 1001$

18. (a) Encrypt the message STOP POLLUTION by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.

i) $f(p) = (p + 4) \bmod 26$ ii) $f(p) = (p + 21) \bmod 26$

(b) Decrypt these messages encrypted using the Shift cipher. $f(p) = (p + 10) \bmod 26$.

i) CEBBOXNOB XYG ii) LO WI PBSOXN

19. Use Fermat's little theorem to compute $5^{2003} \bmod 7$, $5^{2003} \bmod 11$, and $5^{2003} \bmod 13$.

20. (a) Encrypt the message I LOVE DISCRETE MATHEMATICS by translating the letters into numbers, applying the Caesar Cipher Encryption function and then translating the numbers back into letters.

(b) Decrypt these messages encrypted using the Caesar Cipher.

i) PLG WZR DVVLJQPHQW ii) IDVW QXFHV XQLYHUVLWB

21. (a) Which memory locations are assigned by the hashing function $h(k) = k \bmod 97$ to the records of insurance company customers with these Social Security numbers?

i) 034567981 ii) 183211232 iii) 220195744 iv) 987255335

(b) Which memory locations are assigned by the hashing function $h(k) = k \bmod 101$ to the records of insurance company customers with these Social Security numbers?

i) 104578690 ii) 432222187 iii) 372201919 iv) 501338753

22. What sequence of pseudorandom numbers is generated using the linear congruential generator? $x_n+1 = (4x_n + 1) \bmod 7$ with seed $x_0 = 3$? Do at least 20 iterations.

23. (a) Determine the check digit for the UPCs that have these initial 11 digits.
i) 73232184434 ii) 63623991346

(b) Determine whether each of the strings of 12 digits is a valid UPC code.
i) 036000291452 ii) 012345678903

24. (a) The first nine digits of the ISBN-10 of the European version of the fifth edition of this book are 0-07-119881.What is the check digit for that book?

(b) The ISBN-10 of the sixth edition of Elementary Number Theory and Its Applications is 0-321-500Q1-8, where Q is a digit. Find the value of Q.

25. Encrypt the message ATTACK using the RSA system with $n = 43 \cdot 59$ and $e = 13$, translating each letter into integers and grouping together pairs of integers.

26. (a) Find the first five terms of the sequence for each of the following general terms where $n > 0$.
(i) $2^n - 1$ (ii) $10 - \frac{3}{2}n$ (iii) $\frac{(-1)^n}{n^2}$ (iv) $\frac{3n+4}{2n-1}$

(b) Identify the following Sequence as Arithmetic or Geometric Sequence then find the indicated term.
(i) -15, -22, -29, -36, ……; 11th term. (ii) a - 42b, a - 39b, a - 36b, a - 33b, ….; 15th term.
(iii) 4, 3, $\frac{9}{4}$, ...; 17th term (iv) 32, 16, 8, ….; 9th term

27. (a) Find the G.P in which:
(i) $T_3 = 10$ and $T_5 = 2\frac{1}{2}$ (ii) $T_5 = 8$ and $T_8 = -\frac{64}{27}$

(b) Find the A.P in which:
(i) $T_4 = 7$ and $T_{16} = 31$ (ii) $T_5 = 86$ and $T_{10} = 146$

28. (a) How many numbers are there between 256 and 789 that are divisible by 7? Also find their sum.
(b) Find the sum to n terms of an A.P whose first term is $\frac{1}{n}$ and the last term is $\frac{n^2-n+1}{n}$.

29. (a) Use summation notation to express the sum of the first 100 terms of the sequence $\{a_j\}$, where $a_j = \frac{1}{j}$ for $j = 1, 2, 3\ldots.$

(b) What is the value of:
(i) $\sum_{k=4}^{8}(-1)^k$ · (ii) $\sum_{j=1}^{5}(j)^2$ ·

30. Find the first six terms of the sequence defined by each of these recurrence relations and initial conditions.

a) $a_n = -2a_{n-1}$, $a_0 = -1$ b) $a_n = a_{n-1} - a_{n-2}$, $a_0 = 2$, $a_1 = -1$
c) $a_n = 3a^2_{n-1}$, $a_0 = 1$ d) $a_n = na_{n-1} + a^2_{n-2}$, $a_0 = -1$, $a_1 = 0$

31. (a) Prove the statement: There is an integer $n > 5$ such that $2^n - 1$ is prime.
    (b) Prove that for any integer a and any prime number p, if $p \mid a$, $P \nmid (a + 1)$.

32. (a) Prove the statement: There are real numbers a and b such that $\sqrt{(a+b)} = \sqrt{a} + \sqrt{b}$.
    (b) Prove that if $|x| > 1$ then $x > 1$ or $x < -1$ for all $x \in R$.

33. (a) Find a counter example to the proposition: For every prime number n, n + 2 is prime.
    (b) Show that the set of prime numbers is infinite.

34. (a) Prove by contradiction method, the statement: If n and m are odd integers, then n + m is an even integer.
    (b) Prove the statement by contraposition: For all integers m and n, if m + n is even then m and n are both even or m and n are both odd.

35. (a) Prove by contradiction that $6 - 7\sqrt{2}$ is irrational.
    (b) Prove by contradiction that $\sqrt{2} + \sqrt{3}$ is irrational.

36. By mathematical induction, prove that following is true for all positive integral values of n.

    (a) $1^2 + 2^2 + 3^2 + \ldots\ldots + n^2 = (n(n+1)(2n+1))/6$
    (b) $1 + 2 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$ for all integers $n \geq 0$
    (c) $1^3 + 2^3 + 3^3 + \ldots + n^3 = \frac{1}{4} n^2(n+1)^2$

37. As we have discussed, the practical application of all the topics in the class. Now you are required to submit at least two real world applications of the following topics.

    (a) Propositional Logic
    (b) Predicates and quantifiers
    (c) Sets
    (d) Functions
    (e) Relations
    (f) Sequence and Series
    (g) Proof methods and Mathematical Induction

Best of Luck!