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

Department of Computer Science
Assignment # 2, Spring 2020.
CS211-Discrete Structures

<u>Instructions:</u>

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^2 | a > b}, the "greater than" relation,
   R2 = {(a, b) ∈ R^2 | a ≥ b}, the "greater than or equal to "relation,
   R3 = {(a, b) ∈ R^2 | a < b}, the "less than" relation,
   R4 = {(a, b) ∈ R^2 | a ≤ b}, the "less than or equal to "relation,
   R5 = {(a, b) ∈ R^2 | a = b}, the "equal to" relation,
   R6 = {(a, b) ∈ R^2 | 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.

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

13. Find a div m and a mod m when
    a) a = −111, m = 99. b) a = −9999, m = 101.
    c) a = 10299, m = 999. d) a = 123456, m = 1001.

14. Decide whether each of these integers is congruent to 5 modulo 17.
    a) 80 b) 103 c) −29 d) −122

15. Determine whether the integers in each of these sets are pairwise relatively prime.
    a) 11, 15, 19 b) 14, 15, 21 c) 12, 17, 31, 37 d) 7, 8, 9, 11

16. Find the prime factorization of each of these integers.

a) 88 b) 126 c) 729 d) 1001 e) 1111 f) 909

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

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

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

19. (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 her 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?

20. 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

21. (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

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

23. (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

24. (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

25. What sequence of pseudorandom numbers is generated using the linear congruential generator?

$x_{n+1} = (4x_n + 1) \bmod 7$ with seed $x_0 = 3$?

26. (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

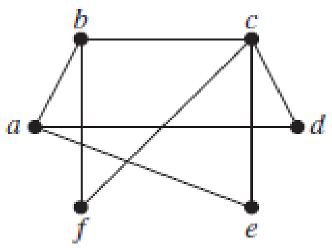
27. (a) The first nine digits of the ISBN-10 of the European version of the fifth edition of this book are 0-07-119881.What is the check digit for that book?

    (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.

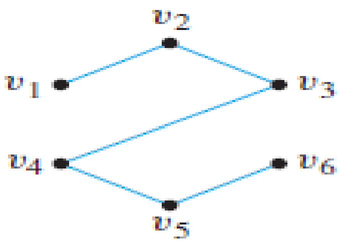
28. Encrypt the message ATTACK using the RSA system with $n = 43 \cdot 59$ and $e = 13$, translating each letter into integers and grouping together pairs of integers.

29. Find which of the following graphs are bipartite. Redraw the bipartite graphs so that their bipartite nature is evident.

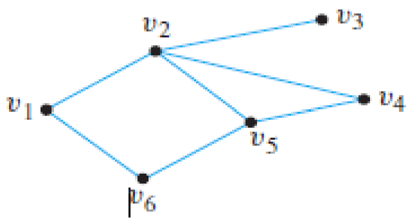
a)



b)

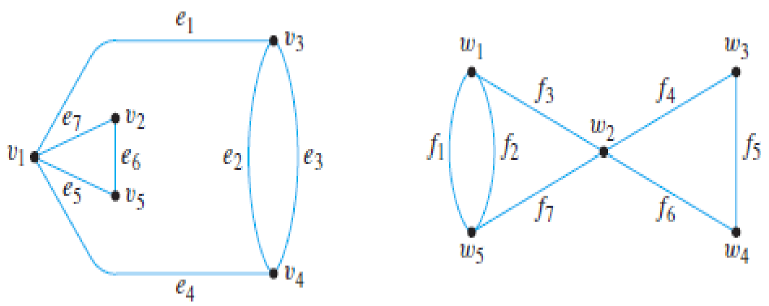


c)

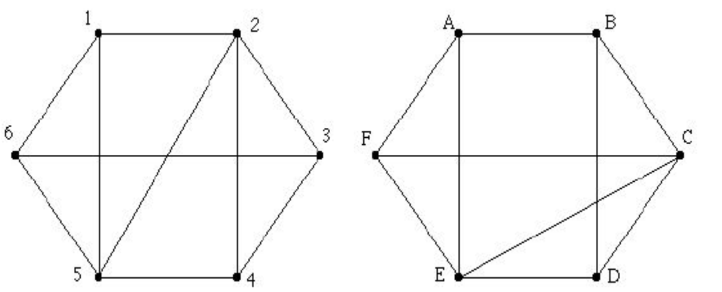


30. Determine whether given two sets of graphs are isomorphic.

a)

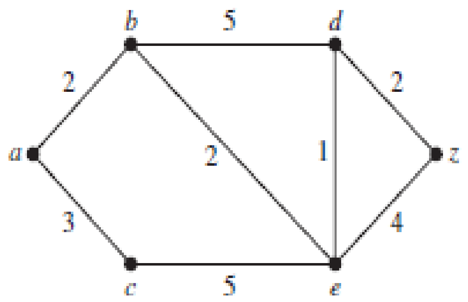


b)

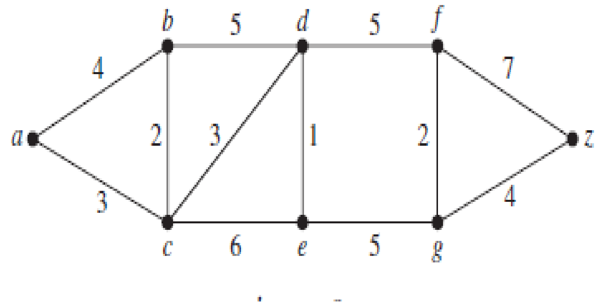


31. Find the length of a shortest path between *a* and *z* in the given weighted graph by using Dijkstra's algorithm.

a)



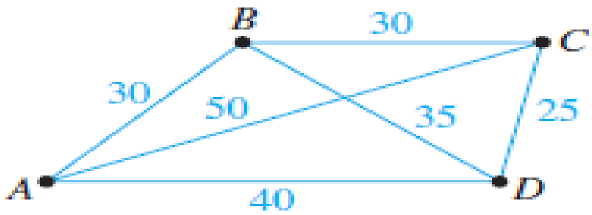
b)



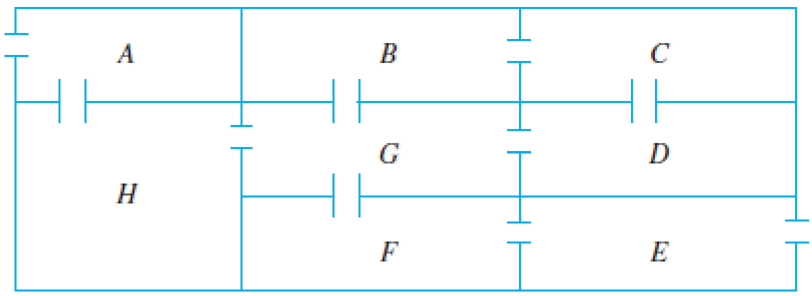
32. a) In a group of 15 people, is it possible for each person to have exactly 3 friends? Explain. (Assume that friendship is a symmetric relationship: If x is a friend of y, then y is a friend of x.)

b) In a group of 4 people, is it possible for each person to have exactly 3 friends? Why?

33. Imagine that the drawing below is a map showing four cities and the distances in kilometers between them. Suppose that a salesman must travel to each city exactly once, starting and ending in city A. Which route from city to city will minimize the total distance that must be traveled?

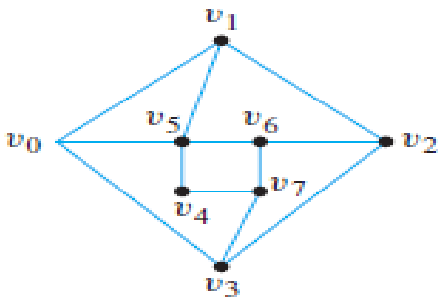


34. The following is a floor plan of a house. Is it possible to enter the house in room A, travel through every interior doorway of the house exactly once, and exit out of room E? If so, how can this be done?

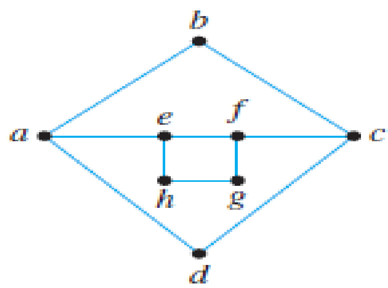


35. Find Hamiltonian circuits AND Path for those graphs that have them. Explain why the other graphs do not.

a)

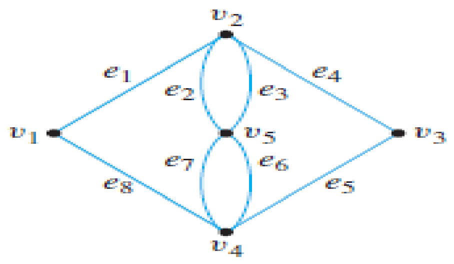


b)

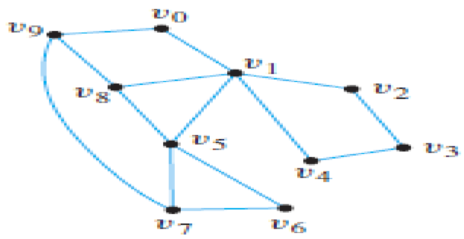


36. a) Determine which of the graphs have Euler circuits. If the graph does not have an Euler circuit, explain why not. If it does have an Euler circuit, describe one.

i)

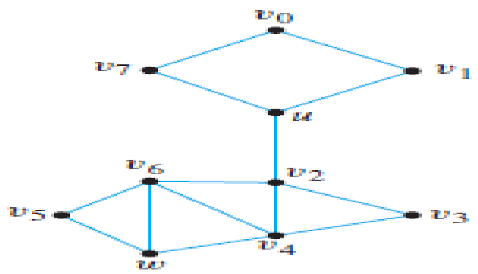


ii)

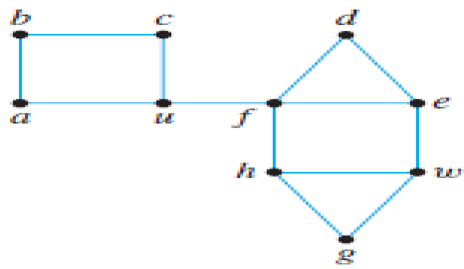


b) Determine whether there is an Euler path from u to w. If there is, find such a path.

i)

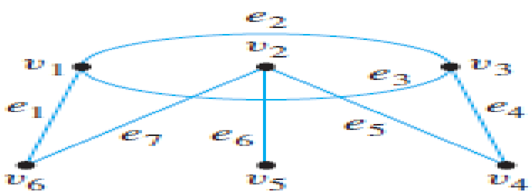


ii)

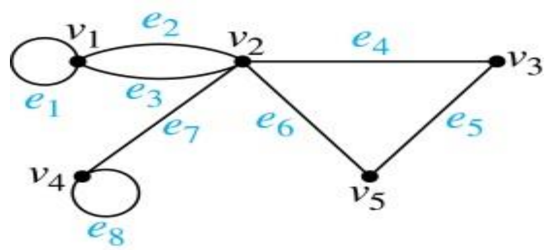


37. Use an incidence matrix to represent the graph shown below.

a)



b)



38. Draw a graph using below given incidence matrix.

a)

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

b)

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Best of Luck!