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

Department of Computer Science

Assignment # 2, Spring 2020. -- Solution

CS211-Discrete Structures

Instructions: **Max. Points: 75**

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

Solution:
(a) R is reflexive because R contains (a, a), (b, b), (c, c), and (d, d).
(b) R is not symmetric because R contains (a, c) but not (c, a) ∈ R .
(c) R is not antisymmetric because both (b, c) ∈ R and (c, b) ∈ R , but b = c.
(d) R is not Transitive because both (a, c) ∈ R and (c, b) ∈ R , but not (a, b) ∈ R.
(e) R is not irreflexive because R contains (a, a), (b, b), (c, c), and (d, d).
(f) R is not Asymmetric because R is not Antisymmetric.

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

Solution:
(a) R is reflexive: a = a is true for all real numbers.
(b) R is symmetric: suppose a = b ; then b = a .
(c) R is not antisymmetric: we can have aRb and bRa for distinct a and b. For example, 1.1 = 1. 2
(d) R is Transitive because for any real numbers, a, b, and c, if (a, b), (b, c) ∈ R then a = b and b = c. This implies a= c by substitution, so (a, c) ∈ R.
(e) R is not irreflexive because a = a is true for all real numbers.
(f) R is not Asymmetric because R is not Antisymmetric.

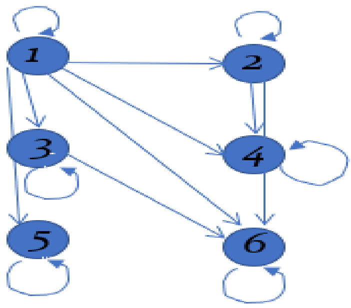
3. List the ordered pairs in the relation R from A = {0, 1, 2, 3, 4} to B = {0, 1, 2, 3}, where (a, b) ∈ R if and only if

a) a = b.	b) a + b = 4.	c) a > b.
d) a | b.	e) gcd(a, b) = 1.	f) lcm (a, b) = 2.

Solution:
a) { (0,0), (1, 1), (2, 2), (3, 3), (4, 4) }
b) { (1, 3), (2, 2), (3, 1), (4, 0) }
c) { (1, 0), (2, 0), (3, 0), (4, 0), (2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3) }
d) { (1, 0), (2, 0), (3, 0), (4, 0), (1, 1), (1,2), (2,2), (1,3), (3,3) }
e) { (1,0), (0,1), (1,1), (1,2), (1,3), (2,1), (3,1), (4,1), (2,3),(3,2),(4,3) }
f) { (1,2), (2,1), (2,2) }

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.
Solution:
R= { (1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (2, 2), (2, 4), (2, 6), (3, 3), (3, 6), (4, 4), (5, 5), (6, 6) }

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



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) }
Solution:
(a) R is not reflexive: It doesn't contain (1,1) and (4,4).
(b) R is not symmetric because R contains (2, 4) but not (4, 2) ∈ R.
(c) R is not antisymmetric: we have (2,3) and (3,2) but 2 ≠ 3.
(d) R is Transitive because for any numbers a, b, and c, if (a, b), (b, c) ∈ R then (a, c) ∈ R.

b) { (1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4) }
Solution:
(a) R is reflexive: It contains (1,1) ,(2,2), (3,3) and (4,4).
(b) R is symmetric because (a,b) and (b,a) ∈ R.
(c) R is not antisymmetric: we have (1,2) and (2,1) but 1 ≠ 2.
(d) R is Transitive because for any numbers a, b, and c, if (a, b), (b, c) ∈ R then (a, c) ∈ R.

c) { (2, 4), (4, 2) }
Solution:
(a) R is not reflexive: It doesn't contain (1,1) ,(2,2), (3,3) and (4,4).
(b) R is symmetric because R contains (2, 4) and (4, 2) ∈ R.
(c) R is not antisymmetric: we have (2,4) and (4,2) but 2 ≠ 4.
(d) R is not Transitive because (2,4), (4, 2) ∈ R but not (2,2) ∈ R.

d) { (1, 2), (2, 3), (3, 4) }
Solution:
(a) R is not reflexive: It doesn't contain (1,1) ,(2,2), (3,3) and (4,4).
(b) R is not symmetric because (1,2) ∈ R but not (2,1) ∈ R.
(c) R is antisymmetric: we have (a,b) but not (b,a) ∈ R.
(d) R is not Transitive because (1,2), (2, 3) ∈ R but not (1,3) ∈ R.

e) {(1, 1), (2, 2), (3, 3), (4, 4)}
Solution:
(a) R is reflexive: It contains (1,1) ,(2,2), (3,3) and (4,4).
(b) R is symmetric because R contains (a,b) and (b,a) ∈ R.
(c) R is antisymmetric: we have (a,b) and (b,a) ∈ R then a = b.
(d) R is Transitive because for any numbers a, b, and c, if (a, b), (b, c) ∈ R then (a, c) ∈ R.

f) {(1, 3), (1, 4), (2, 3), (2, 4), (3, 1), (3, 4)}
Solution:

(a) R is not reflexive: It doesn't contain (1,1) ,(2,2), (3,3) and (4,4).
(b) R is not symmetric because (1,4) ∈ R but not (4,1) ∈ R.
(c) R is not antisymmetric: we have (1,3) and (3,1) ∈ R but 1 ≠ 3.
(d) R is not Transitive because we have (1,3) and (3,1) ∈ R but not (1,1) ∈ R.

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.

Solution:

The relation R is **not reflexive**, because a person cannot be taller than himself/herself.

The relation R is **not symmetric**, because if person A is taller than person B, then person B is NOT taller than person A.

The relation R is **antisymmetric**, because $(a, b) \in R$ and $(b, a) \in R$ cannot occur at the same time (as one person is always taller than the other, but not the other way around).

The relation R is **transitive**, because if person A is taller than person B and if person B is taller than person C, then person A needs to be taller than person C as well.

b) a and b were born on the same day.

Solution:

The relation R is **reflexive**, because a person is born on the same day as himself/herself.

The relation R is **symmetric**, because if person A and person B are born on the same day, then person B is also born on the same day as person A.

The relation R is **not antisymmetric**, because if person A and person B are born on the same day and if person B and person A are born on the same day, then these two people are not necessarily the same person.

The relation R is **transitive**, because if person A and person B are born on the same day and if person B and person C are born on the same day, then person A and person C are also born on the same day.

c) a has the same first name as b.

Solution:

The relation R is **reflexive**, because a person has the same first name as himself/herself.

The relation R is **symmetric**, because if person A has the same first name as person B, then person B also has the same first name as person A.

The relation R is **not antisymmetric**, because if person A has the same first name as person B and if person B also has the same first name as person A, then these two people are not necessarily the same person (as there are different people with the same first name).

The relation R is **transitive**, because if person A has the same first name as person B and if person B also has the same first name as person C, then person A also has the same first name as person C.

d) a and b have a common grandparent.

Solution:

The relation R is **reflexive**, because a person has the same grandparents as himself/herself.

The relation R is **symmetric**, because if person A and person B have a common grandparent, then person B and person A also have a common grandparent.

The relation R is **not antisymmetric**, because if person A and person B have a common grandparent and if person B and person A have a common grandparent, then these two people are not necessarily the same person (as there are different people with the same grandparents).

The relation R is **not transitive**, because if person A and person B have a common grandparent and if person B and person C have a common grandparent, then person A and person C do not necessarily have a common grandparent (for example, the common grandparent of A and B can be from person B's father's side of the family, while the common grandparent of B and C can be from person B's mother's side of the family).

(a) Antisymmetric, Irreflexive, Asymmetric and Transitive
(b) Reflexive, Symmetric and Transitive
(c) Reflexive, Symmetric and Transitive
(d) Reflexive and Symmetric

7. **Give an example of a relation on a set that is**

a) both symmetric and antisymmetric.

Solution:

{ (1,1), (2,2), (3,3), (4,4) }

b) neither symmetric nor antisymmetric.

Solution:

{ (1,2), (2,1), (3,4) }

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.**

Solution:

R1= { (2,1), (3,1), (3,2) }
R2= { (1,1), (2,2), (3,3), (2,1), (3,1), (3,2) }
R3= { (1,2), (1,3), (2,3) }
R4= { (1,1), (2,2), (3,3), (1,2), (1,3), (2,3) }
R5= { (1,1), (2,2), (3,3) }
R6= {(1,2), (1,3), (2,1), (2,3), (3,1), (3,2) }

a) R2 ∪ R4 = { (1,1), (2,2), (3,3), (2,1), (3,1), (3,2) (1,2), (1,3), (2,3) } = R^2
b) R3 ∪ R6= {(1,2), (1,3), (2,1), (2,3), (3,1), (3,2) } = R6
c) R3 ∩ R6 = { (1,2), (1,3), (2,3) } = R3
d) R4 ∩ R6 = { (1,2), (1,3), (2,3) } = R3

e) R3 − R6 = { }   OR Φ
f) R6 − R3 = { (2,1), (3,1), (3,2) } = R1
g) R2 ⊕ R6 = { (1,1), (2,2), (3,3), (1,2), (1,3), (2,3) } = R4
h) R3 ⊕ R5 = { (1,1), (2,2), (3,3), (1,2), (1,3), (2,3) } = R4
i) R2 ◦ R1 = { (2,1), (3,1), (3,2) }
j) R6 ◦ R6 = { (1,1), (2,2), (3,3), (2,1), (3,1), (3,2) (1,2), (1,3), (2,3) } = R^2

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) }

   Solution: $\begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$

   ii) { (1 , 2), (2 , 1), (2 , 2) ,(3 , 3) }

   Solution: $\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

   iii) { (1 , 1), (1 , 2), (1 , 3) , (2 , 2), (2 , 3) ,(3 , 3) }

   Solution: $\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$

   iv) { (1 , 3), (3 , 1) }

   Solution: $\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$

   (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) $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$ Solution: R = { (1,1), (1,3), (2,2), (3,1), (3,3) }

   (ii) $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ Solution: R = { (1,2), (2,2), (3,2) }

   (iii) $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ Solution: R = { (1,1), (1,2), (1,3), (2,1), (2,3), (3,1),(3,2), (3,3) }

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?
    Solution:
    Show that all of the properties of an equivalence relation hold.

- Reflexivity: Because l(a) = l(a), it follows that aRa for all strings a.
- Symmetry: Suppose that aRb. Since l(a) = l(b), l(b) = l(a) also holds and bRa.
- Transitivity: Suppose that aRb and bRc. Since l(a) = l(b),and l(b) = l(c), l(a) = l(a) also holds and aRc.

(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.

Solution:

Recall that a ≡ b (mod m) if and only if m divides a − b.

- **Reflexivity: a ≡ a (mod m) since a − a = 0 is divisible by m since 0 = 0 · m.**
- **Symmetry: Suppose that a ≡ b (mod m). Then a − b is divisible by m, and so a − b = km, where k is an integer. It follows that b − a = (− k) m, so b ≡ a (mod m).**
- **Transitivity: Suppose that a ≡ b (mod m) and b ≡ c (mod m). Then m divides both a − b and b − c. Hence, there are integers k and l with a − b = km and b − c = lm. We obtain by adding the equations: a − c = (a − b) + (b − c) = km + lm = (k + l) m. Therefore, a ≡ c (mod m).**

11. What are the quotient and remainder when:

a) 19 is divided by 7?	**Solution:**	**q = 2;**	**r = 5**
b) −111 is divided by 11?	**Solution:**	**q = -11;**	**r = 10**
c) 789 is divided by 23?	**Solution:**	**q = 34;**	**r = 7**
d) 1001 is divided by 13?	**Solution:**	**q = 77;**	**r = 0**
e) 10 is divided by 19?	**Solution:**	**q = 0;**	**r = 10**
f) 3 is divided by 5?	**Solution:**	**q = 0;**	**r = 5**
g) −1 is divided by 3?	**Solution:**	**q = -1;**	**r = 2**
h) 4 is divided by 1?	**Solution:**	**q = 4;**	**r = 0**

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

Solution:

Proof:(Note: because this theorem is a biconditional, we must prove it in "both directions.")

First, assume a ≡ b (mod m)

then m | (a–b), so there is k ∈ Z such that a – b = mk.

Let a mod m = r.

Then, according to the division algorithm, there is q ∈ Z such that a = mq + r, 0 ≤ r < m.

Using a= mq + r to replace a in a – b = mk. we get

mq + r – b = mk

So

mq – mk + r = b

m (q – k) + r = b

This shows that r is the remainder when b is divided by m, so b mod m = r (= a mod m).We haveproven that if a ≡ b(mod m) then a mod m = b mod m.

Conversely, assume a mod m = b mod m.

Let r = a mod m = b mod m.

Then, according to the division algorithm, there are q_1, q_2 ∈ Z such that

a = mq_1 + r,

b = mq_2 + r, 0 ≤ r < m.

Then a – b = mq_1 + r – (mq_2 + r)

= mq_1 + r – mq_2 – r

= mq_1 – mq_2

= m (q_1 – q_2) **This shows that m|(a–b), so a ≡ b (mod m).**

We have proven that if a mod m = b mod m then a ≡ b (mod m).

13. Find a div m and a mod m when

		q = *a* div *m*		*r* = *a* mod *m*
a) a = −111, m = 99.	**Solution:**	**−2 = −111 div 99**	**;**	**87 = −111 div 99**
b) a = −9999, m = 101.	**Solution:**	**−99 = −9999 div 101**	**;**	**0 = −9999 div 101**
c) a = 10299, m = 999.	**Solution:**	**10 = 10299 div 999**	**;**	**309 = 10299 div 999**
d) a = 123456, m = 1001.	**Solution:**	**113= 123456 div 1001**	**;**	**333 = 123456 div 1001**

14. Decide whether each of these integers is congruent to 5 modulo 17.

a) 80

SOLUTION

(a)

$$5 \,\mathbf{mod}\ 17$$

Since 80 is larger than 5, we should be able to obtain 80 by consecutively adding 17 to 5 if $80 \equiv 5 \,\mathbf{mod}\ 17$.

$$\begin{gathered} 5 \,\mathbf{mod}\ 17 \\ \equiv 5+17 \,\mathbf{mod}\ 17 \\ \equiv 22 \,\mathbf{mod}\ 17 \\ \equiv 22+17 \,\mathbf{mod}\ 17 \\ \equiv 39 \,\mathbf{mod}\ 17 \\ \equiv 39+17 \,\mathbf{mod}\ 17 \\ \equiv 56 \,\mathbf{mod}\ 17 \\ \equiv 56+17 \,\mathbf{mod}\ 17 \\ \equiv 73 \,\mathbf{mod}\ 17 \\ \equiv 73+17 \,\mathbf{mod}\ 17 \\ \equiv 90 \,\mathbf{mod}\ 17 \end{gathered}$$

We then note that $5 \,\mathbf{mod}\ 17$ is equivalent with 73 and 90. $5 \,\mathbf{mod}\ 17$ is then not equivalent with 80, since $73 < 80 < 90$.

Note: $80 \,\mathbf{mod}\ 17 \equiv 12 \,\mathbf{mod}\ 17$

b) 103

Since 103 is larger than 5, we should be able to obtain 103 by consecutively adding 17 to 5 if $103 \equiv 5 \,\mathbf{mod}\ 17$.

$$\begin{gathered} 5 \,\mathbf{mod}\ 17 \\ \equiv 5+17 \,\mathbf{mod}\ 17 \\ \equiv 22 \,\mathbf{mod}\ 17 \\ \equiv 22+17 \,\mathbf{mod}\ 17 \\ \equiv 39 \,\mathbf{mod}\ 17 \\ \equiv 39+17 \,\mathbf{mod}\ 17 \\ \equiv 56 \,\mathbf{mod}\ 17 \\ \equiv 56+17 \,\mathbf{mod}\ 17 \\ \equiv 73 \,\mathbf{mod}\ 17 \\ \equiv 73+17 \,\mathbf{mod}\ 17 \\ \equiv 90 \,\mathbf{mod}\ 17 \\ \equiv 90+17 \,\mathbf{mod}\ 17 \\ \equiv 107 \,\mathbf{mod}\ 17 \end{gathered}$$

We then note that $5 \,\mathbf{mod}\ 17$ is equivalent with 73 and 90. $5 \,\mathbf{mod}\ 17$ is then not equivalent with 80, since $73 < 80 < 90$.

Note: $103 \,\mathbf{mod}\ 17 \equiv 1 \,\mathbf{mod}\ 17$

c) −29

Since -29 is smaller than 5, we should be able to obtain -29 by consecutively subtracting 17 from 5 if $-29 \equiv 5 \ \mathbf{mod}\ 17$.

$$\begin{gathered} 5 \ \mathbf{mod}\ 17 \\ \equiv 5-17 \ \mathbf{mod}\ 17 \\ \equiv -12 \ \mathbf{mod}\ 17 \\ \equiv -12-17 \ \mathbf{mod}\ 17 \\ \equiv -29 \ \mathbf{mod}\ 17 \end{gathered}$$

Thus we then note that $-29 \equiv 5 \ \mathbf{mod}\ 17$.

d) −122

Since -122 is smaller than 5, we should be able to obtain -122 by consecutively subtracting 17 from 5 if $-122 \equiv 5 \ \mathbf{mod}\ 17$.

$$\begin{gathered} 5 \ \mathbf{mod}\ 17 \\ \equiv 5-17 \ \mathbf{mod}\ 17 \\ \equiv -12 \ \mathbf{mod}\ 17 \\ \equiv -12-17 \ \mathbf{mod}\ 17 \\ \equiv -29 \ \mathbf{mod}\ 17 \\ \equiv -29-17 \ \mathbf{mod}\ 17 \\ \equiv -46 \ \mathbf{mod}\ 17 \\ \equiv -46-17 \ \mathbf{mod}\ 17 \\ \equiv -63 \ \mathbf{mod}\ 17 \\ \equiv -63+17 \ \mathbf{mod}\ 17 \\ \equiv -80 \ \mathbf{mod}\ 17 \\ \equiv -63+17 \ \mathbf{mod}\ 17 \\ \equiv -80 \ \mathbf{mod}\ 17 \\ \equiv -80+17 \ \mathbf{mod}\ 17 \\ \equiv -97 \ \mathbf{mod}\ 17 \\ \equiv -97+17 \ \mathbf{mod}\ 17 \\ \equiv -114 \ \mathbf{mod}\ 17 \\ \equiv -114+17 \ \mathbf{mod}\ 17 \\ \equiv -131 \ \mathbf{mod}\ 17 \end{gathered}$$

We then note that $5 \ \mathbf{mod}\ 17$ is equivalent with -114 and -131. $5 \ \mathbf{mod}\ 17$ is then not equivalent with -122, since $-131 < -122 < -114$.

Note: $-122 \ \mathbf{mod}\ 17 \equiv 14 \ \mathbf{mod}\ 17$

15. Determine whether the integers in each of these sets are pairwise relatively prime.

a) 11, 15, 19
Solution: Yes
gcd (11,15) = 1, gcd (11,15) = 1, gcd (11,19) = 1

b) 14, 15, 21
Solution: No
gcd (14, 15) = 1, gcd (14, 21) = 7, gcd (15, 21) = 3

c) 12, 17, 31, 37
Solution: Yes
gcd (12, 17) = 1, gcd (12, 31) = 1, gcd (12, 37) = 1, gcd (17, 31) = 1, gcd (17, 37) = 1, gcd (31, 37) = 1

d) 7, 8, 9, 11
Solution: Yes
gcd (7, 8) = 1, gcd (7, 9) = 1, gcd (7, 11) = 1, gcd (8, 9) = 1, gcd (8, 11) = 1, gcd (9, 11) = 1

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

a) 88	Solution: 88 = 2^3 * 11
b) 126	Solution: 126 = 7 * 13 * 11
c) 729	Solution: 729 = 2 * 7 * 3^2
d) 1001	Solution: 1001 = 7 * 13 * 11
e) 1111	Solution: 1111 = 11 * 101
f) 909	Solution: 909 = 3^2 * 101

17. **Use the extended Euclidean algorithm to express gcd (144, 89) and gcd (1001, 100001) as a linear combination.**
Solution:
Gcd(144,89) = (144)(34) + (89)(−55) = 1
gcd (1001, 100001) = (10)(100001) + (−999)(1001) = 1

18. **Solve each of these congruences using the modular inverses.**
a) 55x ≡ 34 (mod 89)
Solution:
Gcd(55,89) = (55)(34) + (89)(−21) = 1
So, inverse ā = 34.
Multiply 34 both side
55 * 34 x ≡ 34 * 34 (mod 89)
x = 1156 (mod 89) = 88.

b) 89x ≡ 2 (mod 232)
Solution:
Gcd(89,232) = (73)(89) + (232)(−28) = 1
So, inverse ā = 73,
Multiply 73 both side
89 * 73 x ≡ 2 * 73 (mod 232)
x = 146 (mod 232) = 146.

19. **(a) Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences.**
i) x ≡ 1 (mod 5), x ≡ 2 (mod 6), and x ≡ 3 (mod 7).
Solution:
We will follow the notation used in the proof of the Chinese remainder theorem.
We have $m=m_1 * m_2 * m_3$ = 5 * 6 * 7 = 210.
M_1= 210/5 = 42, M_2 = 210/6 = 35, and M_3 = 210/7 = 30
Also, by simple inspection we see that:
y_1 = 3 is an inverse for M_1 = 42 modulo 5,
y_2 = 5 is an inverse for M_2 = 35 modulo 6 and
y_3 = 4 is an inverse for M_3 = 30 modulo 7.
The solutions to the system are then all numbers x such that
$x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 \bmod m$
= ((1 * 42 * 3) + (2*35*5) + (3*30*4)) mod 210
= 826 (mod 210) = 206.

ii) $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, and $x \equiv 4 \pmod{11}$.
Solution:
We will follow the notation used in the proof of the Chinese remainder theorem.
We have $m=m_1 * m_2 * m_3 * m_4 = 2 * 3 * 5 * 11 = 330$.
$M_1 = 330/2 = 165$, $M_2 = 330/3 = 110$, $M_3 = 330/5 = 66$ and $M_4= 330/11 = 30$
Also, by simple inspection we see that:
$y_1 = 1$ is an inverse for $M_1= 165$ modulo 2,
$y_2 = 2$ is an inverse for $M_2 = 110$ modulo 3,
$y_3= 1$ is an inverse for $M_3 = 66$ modulo 5 and
$y_4 = 7$ is an inverse for $M_4 = 30$ modulo 11.

The solutions to the system are then all numbers x such that
$x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 + a_4M_4y_4 \bmod m$
$= ((1 * 165 * 1) + (2 * 110 *2) + (3 * 66 *1) + (4 * 30 *7)) \bmod 330$
$= 1643 \pmod{330} = 323$.

(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?
Solution:
We will follow the notation used in the proof of the Chinese remainder theorem.
We have $m=m_1 * m_2 * m_3 * m_4 = 2310$.
Also, by simple inspection we see that:
$y_1 = 3$ is an inverse for $M_1 = 462$ modulo5,
$y_2 = 1$ is an inverse for $M_2 = 385$ modulo 6,
$y_3 = 1$ is an inverse for $M_3 = 330$ modulo 7 and
$Y_4 = 1$ is an inverse for $M_3 = 210$ modulo 11.
The solutions to the system are then all numbers x such that
$x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 + a_4M_4y_4 \bmod m$
$= (3 * 462 * 3) + (3* 385* 1) + (1* 330* 1) + (0*210*1) = 5643 \pmod{2310} = 1023$.
He could have 1023 oranges.

20. Find an inverse of a modulo m for each of these pairs of relatively prime integers.
a) $a = 2$, $m = 17$
Solution:
$\gcd(2,17) = (1)(17) + (-8)(2) = 1$
So, $-8 + 17 =9$
Hence inverse, $\bar{a} = 9$.

b) $a = 34$, $m = 89$
Solution:
$\gcd(34,89) = (13)(89) + (-34)(34) = 1$
So, $-34 + 89 = 55$
Hence inverse, $\bar{a} = 55$.

c) a = 144, m = 233
Solution:
gcd(144,233) = (89)(144) + (−55)(233) = 1
Hence inverse, ā = 89.

d) a = 200, m = 1001
Solution:
gcd(200,1001) = (1)(1001) + (−5)(200) = 1
So, −5 + 1001 = 996
Hence inverse, ā = 996.

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) mod 26
Solution:
S T O P P O L L U T I O N
18 19 14 15 15 14 11 11 20 19 8 14 13
After applying function:
22 23 18 19 19 18 15 15 24 23 12 18 17
W X S T T S P P Y X M S R will be encrypted message.

ii) f (p) = (p + 21) mod 26
Solution:
S T O P P O L L U T I O N
18 19 14 15 15 14 11 11 20 19 8 14 13
After applying function:
13 14 09 10 10 09 06 06 15 14 03 09 08
N O J K K J G G P O D J I will be encrypted message.

(b) Decrypt these messages encrypted using the Shift cipher. f (p) = (p + 10) mod 26.
i) CEBBOXNOB XYG
Solution:
" SURRENDER NOW " will be decrypted message.

ii) LO WI PBSOXN
Solution:
" BE MY FRIEND " will be decrypted message.

22. Use Fermat's little theorem to compute 5^{2003} mod 7, 5^{2003} mod 11, and 5^{2003} mod 13.
Solution:
(i) 5^{2003} mod 7
Solution: Since $5^6 = 1$ mod 7
$= (5^6)^{333} . 5^5$ mod 7 $= 5^5$ mod 7 = 3.

(ii) 5^{2003} mod 11
Solution: Since $5^{10} = 1$ mod 11
$= (5^{10})^{2000} . 5^3$ mod 11 $= 5^3$ mod 11 = 4.

(iii) 5^{2003} mod 13

Solution: Since $5^{12} = 1$ mod 13

$= (5^{12})^{166} . 5^{11}$ mod 13 $= 5^{11}$ mod 13 = 8.

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.
Solution:
The encrypted message will be " L ORYH GLVFUHWH PDWKHPDWLFV "

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

i) PLG WZR DVVLJQPHQW
Solution:
" MID TWO ASSIGNMENT " will be decrypted message.

ii) IDVW QXFHV XQLYHUVLWB
Solution:
" FAST NUCES UNIVERSITY " will be decrypted message.

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

i) 034567981
Solution:
= 034567981 mod 97 = 91

ii) 183211232
Solution:
= 183211232 mod 97 = 57

iii) 220195744
Solution:
= 220195744 mod 97 = 21

iv) 987255335
Solution:
= 987255335 mod 97 = 5

(b) Which memory locations are assigned by the hashing function h(k) = k mod 101 to the records of insurance company customers with these Social Security numbers?
i) 104578690
Solution:
= 104578690 mod 101 = 58.

ii) 432222187
Solution:
= 432222187 mod 101 = 60.

iii) 372201919
Solution:
= 372201919 mod 101 = 32.

iv) 501338753
Solution:
= 501338753 mod 101 = 3.

25. What sequence of pseudorandom numbers is generated using the linear congruential generator?
$x_n+1 = (4x_n + 1)$ mod 7 with seed $x_0 = 3$?
Solution:
$X_1 = (4 * 3 + 1)$ mod 7 = 6.
$X_2 = (4 * 6 + 1)$ mod 7 = 4.
$X_3 = (4 * 4 + 1)$ mod 7 = 3.
$X_4 = (4 * 3 + 1)$ mod 7 = 6.
$X_5 = (4 * 6 + 1)$ mod 7 = 4
Sequence: 6,4,3,6,4,…….

26. (a) Determine the check digit for the UPCs that have these initial 11 digits.

i) 73232184434
Solution:
7*3 + 3 + 2 *3 + 3 + 2 *3 + 1 + 8 *3 + 4 + 4*3 + 3 + 4*3 + x_{12} = 0 mod 10
21 + 3 + 6 + 3 + 6 +1 + 24 + 4 + 12 + 3 + 12 + x_{12} = 0 mod 10
95 + x_{12} = 0 mod 10
Check digit is x_{12} = 5.

ii) 63623991346
Solution:
6*3 + 3 + 6 *3 + 2 + 3 *3 + 9 + 9 *3 + 1 + 3*3 + 4 + 6*3 + x_{12} = 0 mod 10
18 + 3 + 18 + 2 + 9 + 9 + 27 + 1 + 9 + 4 + 18 + x_{12} = 0 mod 10
118 + x_{12} = 0 mod 10
Check digit is x_{12} = 2.

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

i) 036000291452
Solution:
0*3 + 3 + 6 *3 + 0 + 0 *3 + 0 + 2 *3 + 9 + 1*3 + 4 + 5*3 + 2 = 0 mod 10
0 + 3 + 18 + 0 + 0 + 0 + 6 + 9 + 3 + 4 + 15 + 2 = 0 mod 10
60 = 0 mod 10
It's a valid UPC code.

ii) 012345678903
Solution:
0*3 + 1 + 2 *3 + 3 + 4 *3 + 5 + 6 *3 + 7 + 8*3 + 9 + 0*3 + 3 = 0 mod 10
0 + 1 + 6 + 3 + 12 + 5 + 18 + 7 + 24 + 9 + 0 + 3 = 0 mod 10
88 ≠ 0 mod 10
It's not a valid UPC code.

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?

Solution:

1*0 + 2*0 + 3*7 + 4*1 + 5*1 + 6*9 + 7*8 + 8*8 + 9*1 + x_{10} = 0 mod 11

0 + 0 + 21 + 4 + 5 + 54 + 56 + 64 + 9 + x_{10} = 0 mod 11

213 + x_{10} = 0 mod 11

Check digit , x_{10} = 4.

(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.

Solution:

$$\begin{aligned} x_{10} &= 1\cdot 0+2\cdot 3+3\cdot 2+4\cdot 1+5\cdot 5+6\cdot 0+7\cdot 0+8\cdot Q+9\cdot 1 \bmod 11 \\ &= 0+6+6+4+25+0+0+8Q+9 \bmod 11 \\ &= 8Q+50 \bmod 11 \end{aligned}$$

The check digit is known to be 8.

$$8Q+50 \bmod 11 = 8$$

Since $50 \bmod 11 = 6$

$$8Q+6 \bmod 11 = 8$$

Subtract 6 from each side of the equation:

$$8Q \bmod 11 = 2$$

Since the inverse of 8 mod 11 is 7 mod 11, we should multiply both sides of the equation by 7:

$$\begin{aligned} 7\cdot 8Q \bmod 11 &= 7\cdot 2 \bmod 11 \\ 56Q \bmod 11 &= 14 \bmod 11 \\ Q \bmod 11 &= 3 \end{aligned}$$

Since Q is a digit (between 0 and 9), Q then has to be equal to 3.

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

Solution:

A	T	T	A	C	K
00	19	19	00	02	10

- n = 43 · 59 = 2537
- k = (43 − 1) (59 − 1) = 2436
- e = 13

Encryption Function: $C = M^e \bmod n$

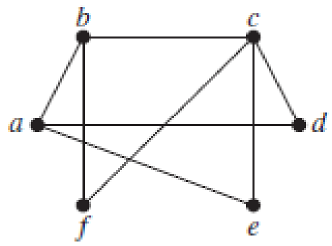
$C = 0019^{13} \bmod 2537$

$C = 1900^{13} \bmod 2537$

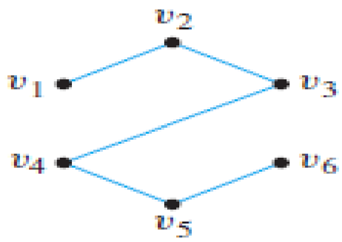
$C = 0210^{13} \bmod 2537$

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

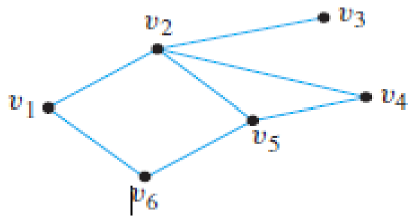
a)



b)



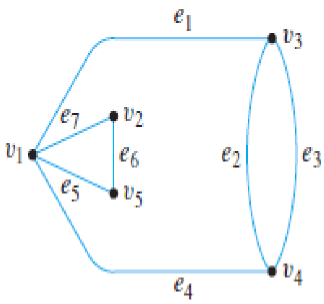
c)

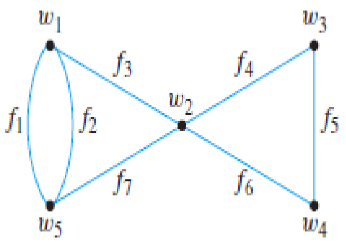


(a) Not bipartite (since b & f are adjacent vertices)
(b) Bipartite (A (V_1, V_3, V_5) & B (V_2, V_4, V_6))
(c) Not bipartite (since V_4 & V_5 are adjacent vertices)

30. **For given pair of graph G and G/. Determine whether G and G/ are isomorphic. If they are, give function g: V (G) →V (G/) that define the isomorphism. If they are not, give an invariant for graph isomorphism that they do not share.**

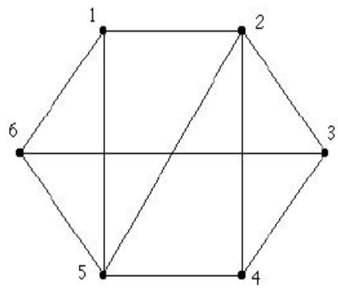
a) Solution:

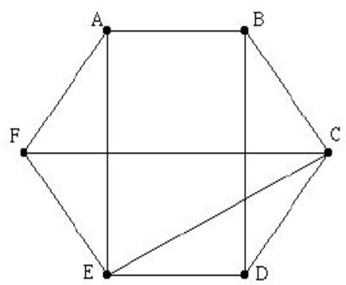




Both graph are isomorphic.
$f(V_1) = W_2$
$f(V_2) = W_3$
$f(V_3) = W_1$
$f(V_4) = W_5$
$f(V_5) = W_4$

b) Solution:

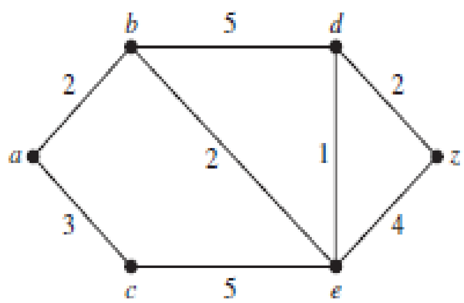




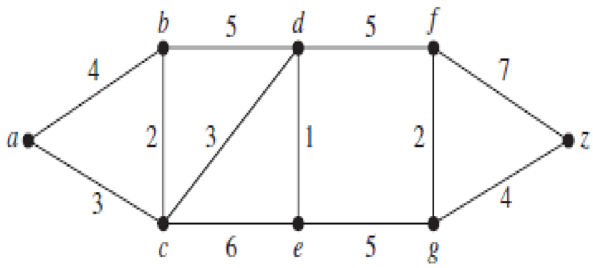
Both graph are isomorphic.
f(1) = D
f(2) = E
f(3) = A
f(4) = F
f(5) = C
f(6) = B

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

a)



b)



(a) Solution:

N	D(b)	D(c)	D(d)	D(e)	D(z)
a	2,a	3,a	∞	∞	∞
ab		3,a	7,b	4,b	∞
abc			7,b	4,b	∞
abce			5,e		8,e
abced					7,d
abcedz	2,a	3,a	5,e	4,b	7,d

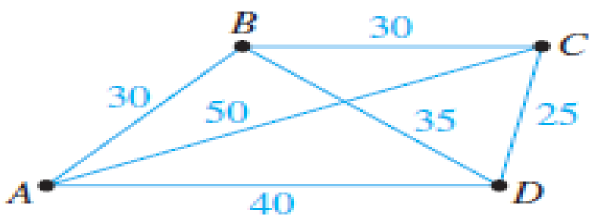
(b)Solution:

N	D(b)	D(c)	D(d)	D(e)	D(f)	D(g)	D(z)
a	4,a	3,a	∞	∞	∞	∞	∞
ac			6,c	9,c	∞	∞	∞
acb			6,c	9,c	∞	∞	∞
acbd				7,d	11,d	∞	∞
acbde					11,d	12,e	∞
acbdef						12,e	18,f
acbdefg							16,g
acbdefgz	4,a	3,a	6,c	7,d	11,d	12,e	16,g

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.)
Solution:
No! there is no graph possible, such that 15 vertices have degree 3.
Since (15 * 3) ≠ 2e.

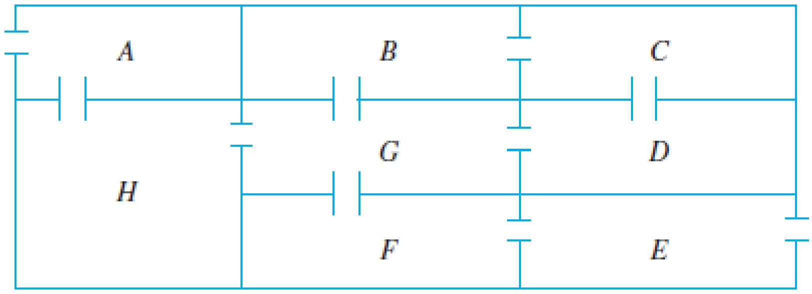
b) In a group of 4 people, is it possible for each person to have exactly 3 friends? Why?
Solution:
Yes! there is graph possible, such that 4 vertices have degree 3.
Since (4 * 3) = 2e.

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?



Solution:
Hamiltonian Circuit are: ABCDA = 125; ABDCA = 140; ACBDA = 155.
Hence ABCDA = 125 is the minimum distance travelled.

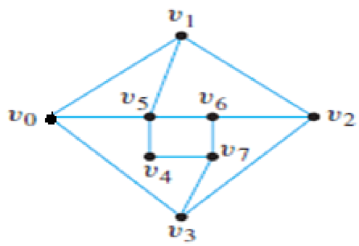
34. The following is a floor plan of a house. Is it possible to enter the house in room A, travel through every interior doorway of the house exactly once, and exit out of room E? If so, how can this be done?



Solution:
Yes! Path: A →H→G→B→C→D→G→F→E

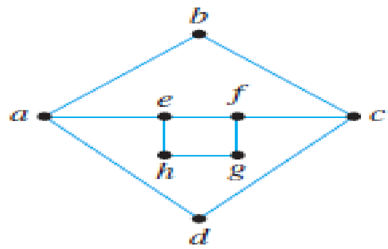
35. Find Hamiltonian circuits AND Path for those graphs that have them. Explain why the other graphs do not.

a)



Solution:
Hamiltonian Circuit: V_0 , V_1 , V_2 , V_6 , V_5 , V_4 , V_7 , V_3 , V_0
Hamiltonian Path: V_0 , V_1 , V_2 , V_6 , V_5 , V_4 , V_7 , V_3

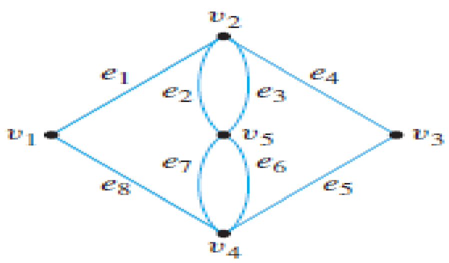
b)



Solution:
Hamiltonian Circuit: doesn't exist
Hamiltonian Path: b, c, f, g, h, e, a, d

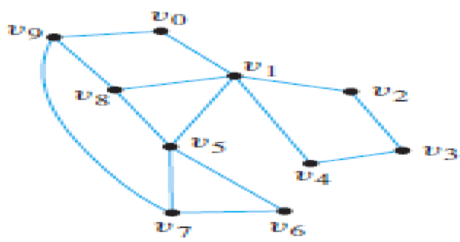
36. a) Determine which of the graphs have Euler circuits. If the graph does not have an Euler circuit, explain why not. If it does have an Euler circuit, describe one.

i)



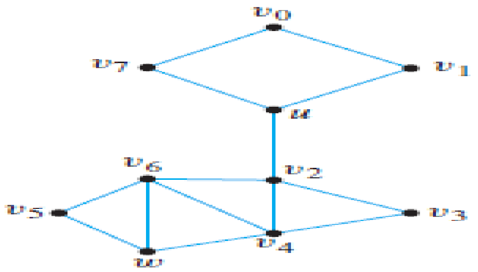
Solution:
Euler Circuit:
All vertices have even degree so circuit exists.
V_1 , V_2 , V_5 , V_4 , V_5 , V_2 , V_3 , V_4 , V_1
Euler path:
Not exist because exact two vertices do not have odd degree.

ii)

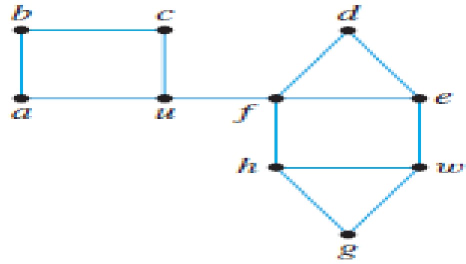


Solution:
Euler Circuit:
Not exists because all vertices don't have even degree.
Euler path:
Not exist because exact two vertices do not have odd degree.
b) Determine whether there is an Euler path from u to w. If there is, find such a path.

i)
Solution:
Euler Path:
Path exists because exact two vertices have odd degree.
U, V_1, V_0, V_7, U, V_2, V_3, V_4, V_2, V_6, V_5, W, V_6, V_4, W

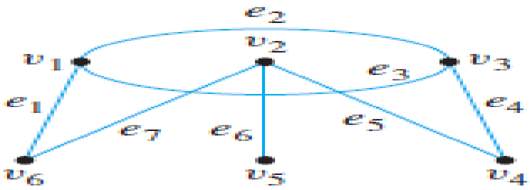


ii)
Solution:
Euler Path:
Path doesn't exist because four vertices have odd degree.



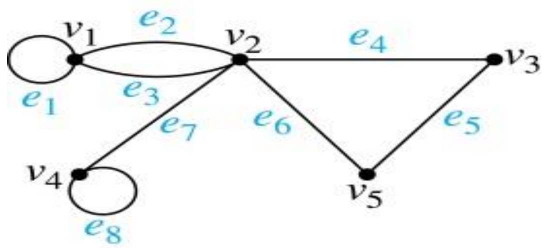
37. Use an incidence matrix to represent the graph shown below.
a)

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

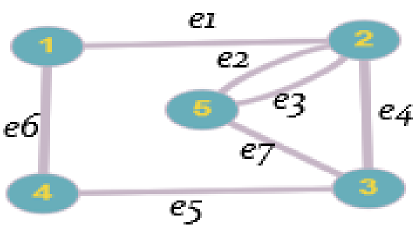


b)

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

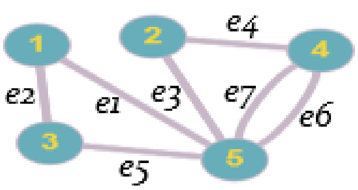


38. Draw a graph using below given incidence matrix.
a)



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

b)



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