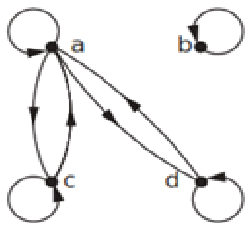
MID2 SOLUTION - DISCREATE STRUCTURE

Q1: [6*2=12]

a. Let $A = \{a, b, c, d\}$ and define relation on R whose directed graph is given in figure #1. Write the relation in tabular and adjacency matrix form.



$R = \{(a, a), (b, b), (c, c), (d, d), (a, c), (c, a), (a, d), (d, a)\}$

Tabular form

R	a	b	c	d
a	x		x	x
b		x		
c	x		x	
d	x			x

Matrix form

$$M= \begin{array}{cc} & \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{array}{c} a \\ b \\ c \\ d \end{array} & \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

b. Determine the relation R of given graph in figure #1 is an equivalence relation or partial order . Give proper reason.

SOLUTION

The directed graph is **reflexive**, because the directed graph contains loops at each vertex.

The directed graph is **symmetric**, because all edges in the directed graph come in pair (In other words: there are no single arrows between a pair of points).

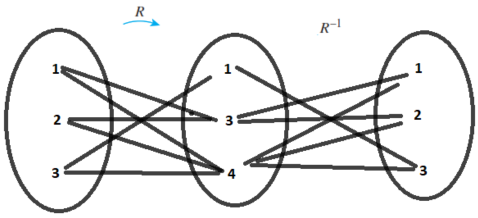
The directed graph is **not transitive**, because $(c, a) \in R$ and $(a, d) \in R$, while $(c, d) \notin R$ (as there is an edge from c to a and from a to d, but not from c to d).

CONCLUSION: The directed graph does NOT show an equivalence relation, because the relation is not transitive.

A relation R on a set S is called a *partial order,* if it is reflexive, antisymmetric, and transitive.

- Figure1 is neither antisymmetric, nor transitive
- Directed graph does not show a partial order relation because not satisfy all its properties.

c) $R = \{(1,3), (1,4), (2,3), (2,4), (3,1), (3,4)\}$



Solution:

$$R^{-1} = \{(3,1), (4,1), (3,2), (4,2), (1,3), (4,3)\}$$

$$R^{-1} o\ R = \{(1,1), ((2,2), (3,3)(1,3), (1,2), (2,1), (2,3), (3,1), (3,2)\}\}$$

d) If there are 451 history students given exam in ten rooms, what is the minimum possible number of students in any of the rooms?

Using pigeonhole principle

$$\left\lceil \frac{451}{10} \right\rceil = 45.1 = 46$$

e) You have a computer with eight empty slots for interface cards, two parallel ports for printers, and four serial ports for modems, scanners, or mice. Suppose you have three interface cards, one printer, one mouse, and one modem. In how many ways can you connect them to your computer?

Solution: Rule of multiplication

$(8 \times 7 \times 6) \times (2) \times (4 \times 3) = 8064.$

f) Find the 45th term in the expansion of $(\frac{a}{2} + \frac{b}{2})^{100}$.

Solution:

$$T_{45} = T_{44+1} = \binom{100}{44} \left(\frac{a}{2}\right)^{100-44} \left(\frac{b}{2}\right)^{44}$$

Q2: [4*2 + 4=12]

a. Determine the check digit for the UPCs that have 73232184434 initial 11 digits

Solution:

$$\boxed{3x_1 + x_2 + 3x_3 + x_4 + \cdots + 3x_{11} + x_{12} \equiv 0 \pmod{10} \text{ for } x_{12},}$$

$$3 \cdot 7 + 3 + 3 \cdot 2 + 3 + 3 \cdot 2 + 1 + 3 \cdot 8 + 4 + 3 \cdot 4 + 3 + 3 \cdot 4 + x_{12} \equiv 0 \pmod{10} \Rightarrow x_{12} = 5$$

b. Use Fermat's little theorem to find reminder of $15^{35}\ mod\ 19$.

Solution:

we can use Fermat's theorem. We observe that 15 and 19 are relative primes and $35 \geq 19$. If we take $p = 19, a = 15$, we get

$$15^{18} \equiv 1 \pmod{19}.$$

This removes a big exponent of 15, and the rest of the exponent can be simplified

$$\begin{aligned} 15^{35} = 15^{18} \cdot 15^{17} &\equiv 1 \cdot 15^{17} = (15^2)^8 \cdot 15 = 225^8 \cdot 15 \\ &\equiv 16^8 \cdot 15 = 2^{32} \cdot 15 = 2^{18} \cdot 2^{14} \cdot 15 \\ &\equiv 1 \cdot 2^{14} \cdot 15 = 64^2 \cdot 60 \\ &\equiv 7^2 \cdot 3 \\ &\equiv 11 \cdot 3 \\ &\equiv 14 \qquad \pmod{19} \end{aligned}$$

c. Encrypt the plaintext message "HOW ARE YOU" using the shift cipher with shift $k = 3$.

Solution:
First translate the letter into numeric equivalents

07 14 22 00 17 04 24 14 20

Adding $k = 3$ to each number

10 17 25 03 20 07 02 17 23

Substitute the letter correspond to each number. The encrypted message becomes

K R Z D U H B R X

d. Use Euclidean algorithm to express $\gcd(13, 210)$ as a linear combination and state Bezout's identities.
Solution:

$$\begin{aligned} 210 &= 16 \cdot 13 + 2 & 2 &= 210 - 16 \cdot 13 \\ 13 &= 6 \cdot 2 + 1 & 1 &= 13 - 6 \cdot 2 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

$$\begin{aligned} 1 &= 13 - 6 \cdot 2 & 1 &= 13 - 6 \cdot 2 \\ &= 1 \cdot 13 - 6 \cdot 2 \\ &= 1 \cdot 13 - 6 \cdot (210 - 16 \cdot 13) & 2 &= 210 - 16 \cdot 13 \\ &= 97 \cdot 13 - 6 \cdot 210 \end{aligned}$$

Bezout's coefficient are 97 and -6

e. Use Chinese Remainder Theorem to find the unique value of x which satisfy the following congruent relations.

$$x \equiv 6(mod\ 11), x \equiv 13(mod\ 16), x \equiv 9(mod\ 21), x \equiv 19(mod\ 25)$$

Solution:

$x \equiv 6 \pmod{11}$

$x \equiv 13 \pmod{16}$

$x \equiv 9 \pmod{21}$

$x \equiv 19 \pmod{25}$

$a_1 = 6, a_2 = 13, a_3 = 9, a_4 = 19$ $\quad$ $n_1 = 11, n_2 = 16, n_3 = 21, n_4 = 25$

Check if each n_i is pairwise coprime

$GCD(11, 16) = 1$ $\quad$ $GCD(16, 21) = 1$

$GCD(11, 21) = 1$ $\quad$ $GCD(16, 25) = 1$ $\quad$ since all gcd is 1, so each n_i is pairwise coprime

$GCD(11, 25) = 1$ $\quad$ $GCD(21, 25) = 1$

There is a unique solution modulo N

$N = n_1 \cdot n_2 \cdot n_3 \cdot n_4 = 11 \cdot 16 \cdot 21 \cdot 25 = 92400$

$$z_1 = \frac{N}{n_1} = \frac{92400}{11} = 8400$$

$$z_2 = \frac{N}{n_2} = \frac{92400}{16} = 5775$$

$$z_3 = \frac{N}{n_3} = \frac{92400}{21} = 4400$$

$$z_4 = \frac{N}{n_4} = \frac{92400}{25} = 3696$$

Continue ....

Solution:

$x \equiv 6 \pmod{11}$ $\quad$ $x \equiv 13 \pmod{16}$ $\quad$ $x \equiv 9 \pmod{21}$ $\quad$ $x \equiv 19 \pmod{25}$.

Since 11, 16, 21, and 25 are pairwise relatively prime, the Chinese Remainder Theorem tells us that there is a unique solution modulo m,

m = 11*16*21*25 = 92400.

We compute

$M_1 = m / m_1 = 8400$ $\quad$ $M_2 = m / m_2 = 5775$ $\quad$ $M_3 = m / m_3 = 4400$ $\quad$ $M_4 = m / m_4 = 3696$

$y_1 \equiv M_1^{-1} \bmod m_1 \equiv 8$ $\quad$ $y_2 \equiv M_2^{-1} \bmod m_2 \equiv 15$ $\quad$ $y_3 \equiv M_3^{-1} \bmod m_3 \equiv 2$ $\quad$ $y_4 \equiv M_4^{-1} \bmod m_4 \equiv 6$

The solution, which is unique modulo 92400, is

$x \equiv ((a_1y_1M_1) + (a_2y_2M_2) + (a_3y_3M_3) + (a_4y_4M_4)) \bmod m$

$\equiv ((6*8*8400) + (13*15*5775) + (9*2*4400) + (19*6*3696)) \bmod 92400$

$\equiv 2029869 \pmod{92400} \equiv 89469.$

Happy Eid