Philadelphia University Faculty of Engineering Department of Computer Engineering		Second Semester Date:- 13/05/2018 Allowed time:- 60 minutes

Discrete Mathematics (630260) Second Exam (Solution)

Student Name: - ……..... ID: - ……

Question 1: If $a \equiv 7(mod\ 15)$ and $b \equiv 9(mod 15)$ then find the followings 10 points

$$c \equiv 3a^2 - 6b\ (mod\ 15)$$
$$c \equiv 3 \times a \times a - 6 \times b\ (mod\ 15)$$
$$c \equiv \big(3 \times 7 \times 7(mod\ 15) - 6 \times 9\ (mod 15)\big)(mod 15)$$
$$c \equiv \big(147\ (mod\ 15) - 54\ (mod\ 15)\big)\ (mod\ 15)$$
$$c \equiv 12 - 9\ (mod\ 15) \qquad c \equiv 3\ (mod\ 15)$$

Question 2: Solve the following congruence: 10 points

$$23x \equiv 21\ (mod\ 27)$$

Find the inverse of $23\ (mod\ 27)$

$27 = 1 \times 23 + 4$ $23 = 5 \times 4 + 3$ $4 = 1 \times 3 + 1$ $1 = 4 - 1 \times 3$ $1 = 4 - 1 \times (23 - 5 \times 4)$ $1 = -1 \times 23 + 6 \times 4$ $1 = -1 \times 23 + 6 \times (27 - 1 \times 23)$ $1 = 6 \times 27 - 7 \times 23$ The inverse id $-7(mod\ 27) \equiv 20\ (mod\ 27)$	Multiply both sides by 20 $20 \times 23x \equiv 20 \times 21\ (mod\ 27)$ $x \equiv 420\ (mod\ 27)$ $x \equiv 15\ (mod\ 27)$

Question 3: The following message was encrypted using affine cipher function $C = (7P + 3)\ mod\ 26$ where P is the original character and C cipher character decrypt to message. 25 points

GSNF

the decryption key is $P \equiv \bar{7}(C - 3)\ (mod\ 26)$ where $\bar{7}$ is the inverse of $7\ (mod\ 26)$

The inverse of $7\ (mod\ 26)$ is: $26 = 3 \times 7 + 5$ $7 = 1 \times 5 + 2$ $5 = 2 \times 2 + 1$ $1 = 5 - 2 \times 2$ $1 = 5 - 2 \times (7 - 1 \times 5)$ $1 = -2 \times 7 + 3 \times 5$ $1 = -2 \times 7 + 3 \times (26 - 3 \times 7)$ $1 = 3 \times 36 - 11 \times 7$ The inverse of $7\ (mod\ 26)$ is $-11\ (mod\ 26) \equiv 15\ (mod\ 26)$ So the decryption key is: $P \equiv 15(C - 3)\ mod\ 26$	$P_1 \equiv 15(6 - 3)\ (mod\ 26) \equiv 45\ (mod\ 26)$ $P_1 \equiv 19\ (mod\ 26) \quad G \equiv T$ $P_2 \equiv 15(18 - 3)\ (mod\ 26) \equiv 225\ (mod\ 26)$ $P_2 \equiv 17\ (mod\ 26) \quad S \equiv R$ $P_3 \equiv 15(13 - 3)\ (mod\ 26) \equiv 150\ (mod\ 26)$ $P_3 \equiv 20\ (mod\ 26) \quad N \equiv U$ $P_4 \equiv 15(5 - 3)\ (mod\ 26) \equiv 30\ (mod\ 26)$ $P_5 \equiv 4\ (mod\ 26) \quad F \equiv E$ The decryption text is: **TRUE**

Question 4: Use mathematical induction to prove the following summation

10 points

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^n}=\frac{2^n-1}{2^n}$$

1- Basic step verify the equation at n=1

$$\frac{1}{2^1}=\frac{2^1-1}{2^1} \qquad \frac{1}{2}=\frac{1}{2}$$

2- Inductive step:

Assume the equation is true at n=k

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^k}=\frac{2^k-1}{2^k}$$

Then at n=k+1 the equation should be

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^{k+1}}=\frac{2^{k+1}-1}{2^{k+1}}$$

By adding $\frac{1}{2^{k+1}}$ to both sides:

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^k}+\frac{1}{2^{k+1}}=\frac{2^k-1}{2^k}+\frac{1}{2^{k+1}}$$

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^k}+\frac{1}{2^{k+1}}=\frac{2\times(2^k-1)}{2\times 2^k}+\frac{1}{2^{k+1}}=\frac{2^{k+1}-2}{2^{k+1}}+\frac{1}{2^{k+1}}$$

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^k}+\frac{1}{2^{k+1}}=\frac{2^{k+1}-2+1}{2^{k+1}}=\frac{2^{k+1}-1}{2^{k+1}}$$

Question 5: 20 points

1- Give a recursive definition for $a_n=n(n+1)$

$a_1=1\times 2=2$ $a_2=2\times 3=6$ $a_3=3\times 4=12$ $a_4=4\times 5=20$	$a_1=2$ $a_n=a_{n-1}+2n$

2- Using the recursive definition of part 1 write a recursive algorithm to compute

$$\sum_{i=1}^{n} i(i+1)$$

```
Sum(n):int
If n=1 then
     Return 2
Else
     Return n*(n+1) + Sum(n-1)
```

Question 6: Determine whether the following relation on the set of all integers is reflexive, symmetric, antisymmetric, and/or transitive.

5 points

$$R=\{(a,b)\mid a\equiv b \bmod 7\}$$

The relation is reflexive because for $a\in Z \quad a\equiv a\ (mod\ 7)\ \ then\ \ (a,a)\in R$

The relation is symmetric because if

$$a\equiv b\ (mod\ 7)\ \ then\ \ b\equiv a\ (mod\ 7)\ then\ if\ (a,b)\in R\ then\ (b,a)\in R$$

The relation is not antisymmetric because $if\ (a,b)\in R\ then\ (b,a)\in R\ where\ a\neq b$

The relation is transitive because if

$$(a,b)\in R\ \ and\ (b,c)\in R\ then\ (a,c)\in R\ since\ a\equiv c\ mod\ 26$$

Question 7: Given that A={1,2,3} is a set and the following relations are on A. 20 points

$$R1 = \{(1,1),(1,3),(2,2),(3,1)\}$$
$$R2 = \{(1,2),(2,2),(3,2)\}$$

1- Represent these relation using Zero-One matrix then determine wither these relations reflexive, symmetric and/or antisymmetric.

$R1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$ Not reflexive Symmetric Not antisymmetric	$R2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ Not reflexive Not symmetric Antisymmetric

2- Use Zero-One matrices defined above to find $R1 \cup R2$ and $R2 \circ R1$

$$R1 \cup R2 = M_{R1} \vee M_{R2} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \vee \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

$$R2 \circ R1 = M_{R1} \odot M_{R2} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \odot \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$