MEDGAR EVERS COLLEGE
The City University of New York

Discrete Structures

CS 241 - 001

Department of Physical and Computer Sciences

Medgar Evers College

Workshop Lab 8: Congruency, Functions & Matrices

Name: _____

Name: _____

Name: _____

Name: _____

Directions: Write or type solutions on a separate paper(s) and attach this paper to the front of your work.

1. Given the functions

$$f = \{(0,1),(1,5),(2,4),(3,7),(4,0),(5,3),(6,9),(7,1),(8,8),(9,2)\}$$
$$g = \{(0,3),(1,4),(2,5),(3,6),(4,7),(5,8),(6,9),(7,0),(8,1),(9,2)\}$$

   find

   (a) $f \circ g$

   (b) $g \circ f$

2. Given the functions

$$f = \{(0,1),(1,5),(2,4),(3,7),(4,0),(5,3),(6,9),(7,1),(8,8),(9,2)\}$$
$$g = \{(0,3),(1,4),(2,5),(3,6),(4,7),(5,8),(6,9),(7,0),(8,1),(9,2)\}$$

   find

   (a) f^{-1}

   (b) g^{-1}

3. Given the function

$$f = \begin{pmatrix} A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ Q & R & S & T & U & V & W & X & Y & Z & A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P \end{pmatrix}$$

find the equivalent congruence function $g(p)$ knowing that f is generated by a shift cipher.

4. Given the function

$$f = \begin{pmatrix} A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ U & D & M & V & E & N & W & F & O & X & G & P & Y & H & Q & Z & I & R & A & J & S & B & K & T & C & L \end{pmatrix}$$

find the equivalent congruence function $g(p)$ knowing that f is generated by an affine cipher.

5. Given the matrices

$$\mathsf{A} = \begin{bmatrix} 2 & 1 & 6 \\ 5 & 8 & 4 \\ 0 & 11 & 3 \end{bmatrix} \qquad \mathsf{B} = \begin{bmatrix} 4 & 10 & 5 \\ 8 & 13 & 2 \\ 7 & 6 & 9 \end{bmatrix}$$

with elements in $\mathbb{Z}_{17}$, find $5\mathsf{A} + 3\mathsf{B}$.

Extra Credit Given the Vigenere encrytion function

$$f(p,n) = \begin{cases} f_1(p) & \text{if } n \equiv 0 \bmod 5 \\ f_2(p) & \text{if } n \equiv 1 \bmod 5 \\ f_3(p) & \text{if } n \equiv 2 \bmod 5 \\ f_4(p) & \text{if } n \equiv 3 \bmod 5 \\ f_5(p) & \text{if } n \equiv 4 \bmod 5 \end{cases}$$

where n is the position of the plaintext and

$$f_1 = \begin{pmatrix} A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z & A & B & C & D & E & F & G & H & I & J & K \end{pmatrix}$$

$$f_2 = \begin{pmatrix} A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z & A & B & C \end{pmatrix}$$

$$f_3 = \begin{pmatrix} A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ U & V & W & X & Y & Z & A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T \end{pmatrix}$$

$$f_4 = \begin{pmatrix} A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ N & O & P & Q & R & S & T & U & V & W & X & Y & Z & A & B & C & D & E & F & G & H & I & J & K & L & M \end{pmatrix}$$

$$f_5 = \begin{pmatrix} A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z & A & B & C & D & E & F & G \end{pmatrix}$$

, decipher

NRHTYLWOYHELIA