Math 139 Solution
Hour Exam I 4 March 2003

---

1. Let f and g, be functions mapping $\{\mathrm{A},\mathrm{B},\mathrm{C},\mathrm{D},\mathrm{E},\mathrm{F}\}$ to $\{\mathrm{A},\mathrm{B},\mathrm{C},\mathrm{D},\mathrm{E},\mathrm{F}\}$ as given in the following tables:

x	A	B	C	D	E	F	G
$f(x)$	C	B	E	A	F	G	E

x	A	B	C	D	E	F	G
$g(x)$	F	C	G	D	A	E	B

(a) Complete the following tables
Solution:

x	A	B	C	D	E	F	G
$f \circ g(x)$	G	E	E	A	C	F	B

x	A	B	C	D	E	F	G
$f \circ g(x)$	E	G	B	D	F	A	C

x	A	B	C	D	E	F	G
$f \circ g(x)$	E	G	B	D	F	A	C

(The notation g^{-1} stands for a function satisfying $g^{-1} \circ g(x) = x$ for all x.)

(b) Find two different letters that are sent to the same letter by $f \circ f$. (That is, find x and y with $f \circ f(x) = f \circ f(y)$.)
Solution: We find that

$$f \circ f(\mathtt{A}) = f \circ f(\mathtt{F}) = \mathtt{E}$$

and

$$f \circ f(\mathtt{C}) = f \circ f(\mathtt{G}) = \mathtt{F}.$$

2. Find all solutions (if they exist) to the following congruences:

(a) $3x + 7 \equiv 6 \pmod{11}$.

Solution: We subtract 7 from each side to get

$$\begin{aligned} 3x &\equiv -1 \pmod{11} \\ &\equiv 10 \pmod{11}. \end{aligned}$$

By trial and error, we find that $3 \times 4 \equiv 1 \pmod{11}$, so we multiply both sides of our congruence by 4 to get

$$\begin{aligned} x &\equiv 40 \pmod{11} \\ &\equiv 7 \pmod{11}. \end{aligned}$$

The solution is $x \equiv 7 \pmod{11}$.

(b) $3x + 7 \equiv 6 \pmod{9}$.

Solution: We subtract 7 from each side to get

$$\begin{aligned} 3x &\equiv -1 \pmod{9} \\ &\equiv 8 \pmod{9} \end{aligned}$$

Since 3 has no multiplicative inverse modulo 9, we need to look for solutions the low-tech way, by plugging in each of the nine available numbers to see if any of them gives the right answer. We make up the following table:

x	0	1	2	3	4	5	6	7	8
$3x \bmod 9$	0	3	6	0	3	6	0	3	6

The table shows that there are no solutions to $3x \equiv 8 \pmod{9}$.

(c) $3x + 7 \equiv 4 \pmod{9}$.

Solution: We subtract 7 from each side to get

$$\begin{aligned} 3x &\equiv -3 \pmod{9} \\ &\equiv 6 \pmod{9} \end{aligned}$$

From the table in the last part, we find that $x \equiv 2 \pmod{9}$, $x \equiv 5 \pmod{9}$, and $x \equiv 8 \pmod{9}$ are all solutions to this congruence.

3. Suppose we have an affine encryption function that sends plaintext `s` to ciphertext `C` and plaintext `t` to ciphertext `R`.

   Find the ciphertext equivalents of the plaintext letters `a`, `b`, and `c`.

   Solution: From the given data, we get the two congruences

$$\begin{aligned} 19a &+ b \equiv 17 \pmod{26} \\ 18a &+ b \equiv 2 \pmod{26}. \end{aligned}$$

   Subtracting the second congruence from the first, we get

$$a \equiv 15 \pmod{26}.$$

   We substitute this value for a back into the second congruence and solve for b. We get

$$\begin{aligned} 18 \times 15 + b &\equiv 2 \pmod{26} \\ b &\equiv -268 \pmod{26} \\ &\equiv 18 \pmod{26}. \end{aligned}$$

   The encryption function is $x \mapsto 15x + 18$.

   Applying this function to the letters `a` ($x = 0$), `b` ($x = 1$), and `c` ($x = 2$), we get the numerical answers 18, 33 MOD 26 = 7, and 48 MOD 26 = 22. That is, we have the mappings

$$\begin{aligned} \texttt{a} &\mapsto \texttt{S} \\ \texttt{b} &\mapsto \texttt{H} \\ \texttt{c} &\mapsto \texttt{W}. \end{aligned}$$

4. Suppose that $f_{a,b}$ is the decryption function corresponding to the affine encryption function $f_{17,8}$. Find a and b.

   Since the multiplicative inverse of 17 is 23 (modulo 26), we have We have

$$\begin{aligned} f_{a,b}(x) &= 23(x - 8) \text{ MOD } 26 \\ &= 23x - 184 \text{ MOD } 26 \\ &= 19x + 24 \text{ MOD } 26 \end{aligned}$$

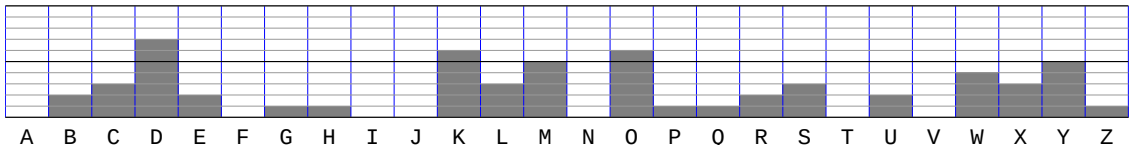
   so the answer is $a = 23$, $b = 24$.

5. Decrypt the following English sentence, which was encrypted using a shift cipher.

   KMYWZ EDOBL OKDWO KDMRO CCYXM OLEDS

   DGKCX YWKDM RPYBW OKDUS MULYH SXQ

   Solution: Here's the frequency histogram for the given text:



   The ciphertext letters B, C, and D might correspond to plaintext r, s, t, and the cluster at ciphertext K, L, M, N, O is probably plaintext a, b, c, d, e. We try this shift, and find that the ciphertext maps to the message

   > A computer beat me at chess once, but it was no match for me at kick-boxing.

6. The following text was encrypted using a keyword. The first word of the plaintext is "Playing" and the last is "unsafe." Decrypt the text and recover the keyword.

   OJDYF LBWFT CKDTN CESKD

   IESDN FOCEQ ULSDR E

   Solution: Using the given cribs, we start to construct an encryption alphabet.

   We get

Plaintext:	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
Ciphertext:	D				E	R	B		F			J		L		O			S		U				Y	

   It appears that the keyword has six letters: D___ER, and that one of the blanks will be filled by A. Plaintext h must map to C, so the keyword does *not* contain a C. It does contain either a G, H, or I, and either an M or an N.

   Knowing this, we can fill in most of the encryption alphabet:

```
Plaintext:  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
Ciphertext: D       E R B C F     J K L   O P Q S T U V W X Y Z
```

We next decrypt the letters we have, to get a message that reads

```
playi ngwit hmat__ hesma __esa__ ipher unsaf e
```

It is clear what the missing letters must be; the message is "Playing with matches makes a cipher unsafe." When we put the new cipher letters into the encryption alphabet, we get

```
Plaintext:  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
Ciphertext: D   N   E R B C F   I J K L M O P Q S T U V W X Y Z
```

The keyword has fits the pattern `D__N__ER`, with `A` in one blank (which must be the first) and either `G` or `H` in the other. The only English word that works is `DANGER`.