For all the part **A** problems, let $f_{a,b}$ denote the function from the set $\{0, 1, 2, \ldots, 25\}$ to the set $\{0, 1, 2, \ldots, 25\}$ that takes a number x to $ax + b \mod 26$, and let's use the same notation for the corresponding affine cipher from $\mathbb{A}$ to $\mathbb{A}$.

So, for instance, we can work with numbers, and say that

$$f_{3,5}(10) = 3 \times 10 + 5 \mod 26 = 9,$$

or we can work with letters, and say that $f_{3,5}(\mathtt{W}) = \mathtt{T}$ (check this).

You'll find a very useful table of multiplicative inverses modulo 26 on page 76 of Barr.

A1. Assuming that the number represented by a has a multiplicative inverse modulo 26, the affine function $f_{a,b}$ is always invertible, and its inverse is also an affine function.

Find the inverse of the affine function $f_{17,5}$. Write your answer in the form $f_{a,b}$, where a and b are numbers in the set $\{0, 1, 2, \ldots, 25\}$.

Solution: The affine function $f_{17,5}$ takes its input, multiplies by 17, and then adds 5. The inverse function must first subtract 5 and then multiply by the multiplicative inverse of 17, which is 23.

Let g be the inverse function. Then we have

$$\begin{aligned} g(x) &= 23(x - 5) \mod 26 \\ &= 23x - 115 \mod 26 \\ &= 23x + 15 \mod 26. \end{aligned}$$

So the inverse of $f_{17,5}$ is $f_{23,15}$.

A2. Several of the functions $f_{a,b}$ are actually their own inverses. Find at least three such functions.

Solution: If $f_{a,b}$ is its own inverse, then we must have

$$\begin{aligned} a(ax + b) + b &\equiv x \pmod{26} \\ a^2x + ab + b &\equiv x \pmod{26} \\ a^2x + b(a + 1) &\equiv x \pmod{26}. \end{aligned}$$

Since this has to hold for every value of x, it follows that we need $a^2 \equiv 1 \pmod{26}$ and $b(a+1) \equiv 0 \pmod{26}$.

The first condition, $a^2 \equiv 1 \pmod{26}$, is satisfied only by $a = 1$ and $a = 25$. We consider each of these cases separately.

If $a = 1$, then $b(a+1)$ is $2b$, and so we can take any value of b for which $2b \equiv 0 \pmod{26}$. Clearly this will be satisfied if $b = 0$, and we also note that if $b = 13$, then $2b \equiv 0 \pmod{26}$. So we have two functions,

$$f_{1,0} \quad \text{and} \quad f_{1,13},$$

that are their own inverses.

If, on the other hand, $a = 25$, then $a + 1 \equiv 0 \pmod{26}$, so the congruence $b(a+1) \pmod{26}$ is satisfied for all values of b. This means that every function of the form

$$f_{25,b}$$

is its own inverse. There are 26 such functions, so we have a total of 28 affine ciphers that are equal to their own inverses.

A3. Suppose we have a cryptogram that's known to be encrypted with some affine cipher $f_{a,b}$, but we don't know what a and b are. By frequency analysis, we have made guesses about the ciphertext equivalents of the plaintext letters t, h, and e. For each of the guesses listed, either:

find the indicated values of a and b, or
explain why the guess can't be correct.

(a) Plaintext t maps to ciphertext `N`
Plaintext h maps to ciphertext `H`
Plaintext e maps to ciphertext `Y`.

Solution: The congruences are

$$\begin{aligned} 19a + b &\equiv 13 \pmod{26} \\ 7a + b &\equiv 7 \pmod{26} \\ 4a + b &\equiv 24 \pmod{26} \end{aligned}$$

We subtract the third congruence from the second to get

$$\begin{aligned} 3a &\equiv -17 \pmod{26} \\ &\equiv 9 \pmod{26} \end{aligned}$$

We multiply both sides by 9 to get

$$\begin{aligned} a &\equiv 81 \pmod{26} \\ &\equiv 3 \pmod{26}. \end{aligned}$$

We then substitute 3 for a in the third congruence to get

$$12 + b \equiv 24 \pmod{26},$$

from which we get $b = 12$.

Finally, we check that these values of a and b work in the first congruence. We have

$$\begin{aligned} 19(3) + 12 &\equiv 69 \pmod{26} \\ &\equiv 17 \pmod{26}, \end{aligned}$$

which is not what we expected. The values $a = 3$, $b = 12$ do not check, so these three congruences are inconsistent, and the guess must be wrong.

(b) Plaintext t maps to ciphertext `H`
Plaintext h maps to ciphertext `F`
Plaintext e maps to ciphertext `Y`.

Solution: The congruences are

$$\begin{aligned} 19a + b &\equiv 7 \pmod{26} \\ 7a + b &\equiv 5 \pmod{26} \\ 4a + b &\equiv 24 \pmod{26} \end{aligned}$$

We subtract the third congruence from the second to get

$$\begin{aligned} 3a &\equiv -19 \pmod{26} \\ &\equiv 7 \pmod{26} \end{aligned}$$

We multiply both sides by 9 to get

$$\begin{aligned} a &\equiv 63 \pmod{26} \\ &\equiv 11 \pmod{26}. \end{aligned}$$

We then substitute 11 for a in the third congruence to get

$$\begin{aligned} 44 + b &\equiv 24 \pmod{26} \\ b &\equiv -20 \pmod{26} \\ &\equiv 6. \end{aligned}$$

Finally, we check that these values of a and b work in the first congruence. We have

$$\begin{aligned} 19(11)+6 &\equiv 215 \pmod{26} \\ &\equiv 7 \pmod{26}, \end{aligned}$$

This one checks. The values we want are $a = 11$, $b = 6$.

(c) Plaintext t maps to ciphertext `B`
Plaintext h maps to ciphertext `F`
Plaintext e maps to ciphertext `T`.

Solution: The congruences are

$$\begin{aligned} 19a + b &\equiv 1 \pmod{26} \\ 7a + b &\equiv 5 \pmod{26} \\ 4a + b &\equiv 19 \pmod{26} \end{aligned}$$

We subtract the third congruence from the second to get

$$\begin{aligned} 3a &\equiv -14 \pmod{26} \\ &\equiv 12 \pmod{26}. \end{aligned}$$

But 4 is not a possible value for a. This tells us that our guesses for the ciphertext equivalents of h and e cannot both be correct.

A4. Suppose we know that a particular affine cipher $f_{a,b}$ maps plaintext e to ciphertext `U` and plaintext i to ciphertext `W`.

Can we find a and b? Why or why not?

The information we have about a and b is that

$$\begin{aligned} 8a + b &\equiv 22 \pmod{26}, \text{ and} \\ 4a + b &\equiv 20 \pmod{26}. \end{aligned}$$

If we subtract the second of these congruences from the first, we get

$$4a \equiv 2 \pmod{26}.$$

The number 4 has no multiplicative inverse, but we *can* find two solutions to this congruence. Looking at a mod-26 multiplication table, we find that 4×7 and 4×20 are both equivalent to 2 modulo 26. So if a is anything, it must be either 7 or 20.

We know, however, that a itself must have a multiplicative inverse modulo 26, so we cannot have $a = 20$. Thus it must be that $a = 7$.

We substitute $a = 7$ into the second congruence to get

$$\begin{aligned} 4(7) + b &\equiv 20 \pmod{26} \\ b &\equiv -8 \pmod{26} \\ &\equiv 18 \pmod{26}. \end{aligned}$$

The solution is $a = 7$, $b = 18$.

B1. Pick one of the cryptograms on the handout *Cryptograms #4 – Affine Ciphers*.

(a) Using the first 200 letters of your cryptogram, determine the six most frequent ciphertext letters. List the number of times each one appears in the first 200 letters of your cryptogram.

(b) Make a contact table listing all the bigrams beginning with each of the six most common letters. (Again, use only the first 200 letters of your cryptogram.)

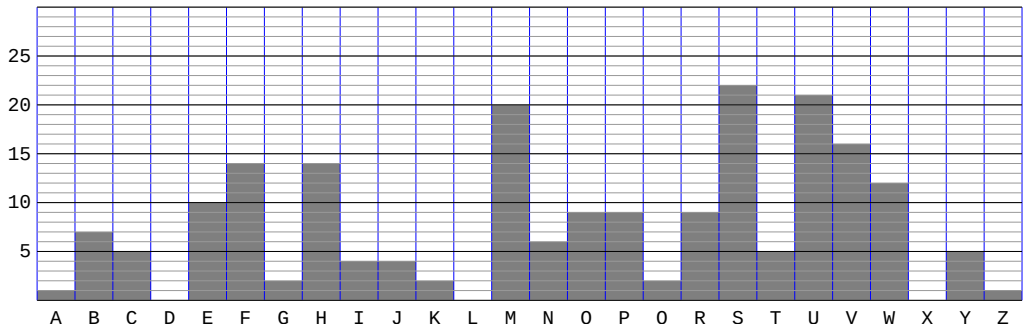
(c) Based on your frequency count, your contact table, and other information you might glean from your cryptogram, guess the ciphertext equivalents of two or three plaintext letters (probably e, t, and h).

(d) Based on your guess, determine the affine encryption key (the numbers a and b in $f_{a,b}$).

(e) Use the encryption key to find the decryption key, and decrypt at least the first 100 letters of your cryptogram. (The quick way to do this is to make up a table giving the decryption alphabet.)

Solution: I used the fourth cryptogram.

(a) Here is the frequency histogram for the first 200 letters.



The six most common letters (and their frequencies) are S (22), U (21), M (20), V (16), F (14), and H (14).

(b) Here is the contact table:

S	U	M	V	F	H
VV	HH	FFFFF	WWW	RRRR	UUU
JJJ	G	RR	UU	VV	MMM
K	FFF	HHHHH	R	C	B
G	VV	CCC	PPPP	B	E
EE	T	Y	SS	NN	OO
HHH	N	O	Y	I	SS
FFF	UU	T	BB	SS	W
YY	M	E	Q	M	I
Q	SSS	M			
NN	R				
T	OO				
O	K				
	P				

(c) I tried several possibilities for t, h, and e. Here's one that seems to work:

$$\begin{aligned} e &\mapsto \mathrm{U} \\ t &\mapsto \mathrm{V} \\ h &\mapsto \mathrm{P} \end{aligned}$$

(d) The congruences are

$$\begin{aligned} 19a + b &\equiv 21 \pmod{26} \\ 7a + b &\equiv 15 \pmod{26} \\ 4a + b &\equiv 20 \pmod{26}. \end{aligned}$$

Subtracting the third congruence from the first, we get

$$15a \equiv 1 \pmod{26},$$

so that a is the multiplicative inverse of 15, which is 7. Substituting $a = 7$ into the third equation, we get

$$28 + b \equiv 20 \pmod{26},$$

which implies that $b = 18$. To check the second congruence, we compute

$$\begin{aligned} 7(7) + 18 &\equiv 67 \pmod{26} \\ &\equiv 15 \pmod{26}, \end{aligned}$$

so that these three congruences are at least consistent.

(e) The decryption function must subtract 18 and then multiply by the inverse of 7, which is 15. Let g be the decryption key. We have

$$\begin{aligned} g(x) &= 15(x - 18) \bmod 26 \\ &= 15x - 270 \bmod 26 \\ &= 15x + 16 \bmod 26. \end{aligned}$$

(f) Here's the decryption alphabet for this decryption function:

x	A	B	C	D	E	F	G	H	I	J	K	L	M
$f_{15,16}(x)$	q	f	u	j	y	n	c	r	g	v	k	z	o
x	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$f_{15,16}(x)$	d	s	h	w	l	a	p	e	t	i	x	m	b

(g) Here's the decryption of the first 200 letters of the cryptogram:

> It is only quite recently that I have taken up golf. In fact, I have played for only three or four years, and seldom more than ten games in a week, or at most four in a day. I have had a proper golf vest for only two years. I bought a spoon only this year and I am ...