A1. Choose one of the cryptograms on the handout "Cryptograms #3."

(a) Make a frequency histogram of the first 200 letters. Some blank histograms are attached to this problem set.

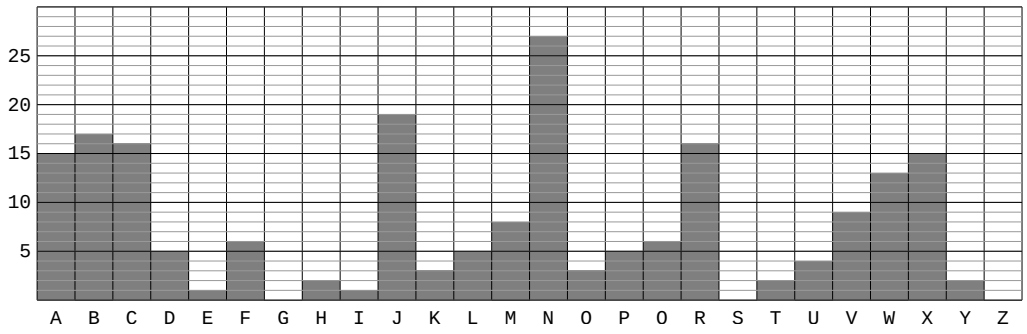
(b) Make a frequency *table* using the same data. Normalize it so that the sum of the frequencies is 1.

(c) Use either your frequency table or your frequency histogram to make a guess at the key letter for your cryptogram.

(d) Decipher at least the first 100 letters of your cryptogram.

Solution: I used the third cryptogram.

(a) Here is a frequency histogram:



(b) Here is a table showing the number of times each ciphertext letter occurs in the first 200 letters of the cryptogram.

A	15	H	2	N	27	U	4
B	17	I	1	O	3	V	9
C	16	J	19	P	5	W	13
D	5	K	3	Q	6	X	15
E	1	L	5	R	16	Y	2
F	6	M	8	S	0	Z	0
G	0			T	2		

Here is a frequency table, normalized so that the sum of the frequencies is 1.

A	0.075	H	0.010	N	0.135	U	0.020
B	0.085	I	0.005	O	0.015	V	0.045
C	0.080	J	0.095	P	0.025	W	0.065
D	0.025	K	0.015	Q	0.030	X	0.075
E	0.005	L	0.025	R	0.080	Y	0.010
F	0.030	M	0.040	S	0.000	Z	0.000
G	0.000			T	0.010		

(c) The frequency histogram suggests very strongly that ciphertext N corresponds to plaintext e. This means that plaintext a corresponds to ciphertext J. So that's the key.

(d) Using the cipher disk set with plaintext a going to ciphertext J, we get (after reformatting)

> I sometimes worried that trains were economic dinosaurs, but when the free marketeer in me suspected Amtrak was a government boondoggle, the foamer said it was only fair to subsidize trains, since there was already so much aid going to planes and highways. For a long time I enthusiastically rode trains but avoided economic analyses of rail travel. My policy toward Amtrak was "Don't ask, don't tell."

A2. Let $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^3 - 4x$ and let $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = 3x - 5$.

(a) Find $f \circ g(1)$ and $g \circ f(1)$.
Solution: We have

$$\begin{aligned} f \circ g(1) &= f(g(1)) \\ &= f(-2) \\ &= -8 - (-8) \\ &= 0 \end{aligned}$$

and

$$\begin{aligned} g \circ f(1) &= g(f(1)) \\ &= g(1 - 4) \\ &= g(-3) \\ &= -9 - 5 \\ &= -14. \end{aligned}$$

(b) Prove that the function g is one-to-one, and find a function h such that $h \circ g(x) = x$ for all x.

Solution: Suppose $g(x) = g(y)$. Then we have

$$3x - 5 = 3y - 5.$$

We add 5 to both sides to get

$$3x = 3y.$$

We next divide by 3 to get $x = y$, showing that g is indeed one-to-one.

To find the desired function h, we write $x = g(y)$ and solve for y. We have

$$\begin{aligned} x &= 3y - 5 \\ x + 5 &= 3y \\ y &= \frac{x+5}{3}. \end{aligned}$$

We can check that the function $h(x) = \dfrac{x+5}{3}$ satisfies $h \circ g(x) = x$ for all x, as follows. We have

$$\begin{aligned} h \circ g(x) &= h(g(x)) \\ &= h(3x - 5) \\ &= \frac{(3x-5)+5}{3} \\ &= \frac{3x}{3} \\ &= x. \end{aligned}$$

(c) Is f one-to-one? Why or why not?

Solution: The function f is not one-to-one, since $f(2) = 8 - 8 = 0$ and $f(-2) = -8 + 8 = 0$.

B1. Let $\mathbb{A}$ denote the set $\{A, B, C, \ldots, Z\}$. Consider the functions m_3 and p_2 mapping $\mathbb{A}$ to $\mathbb{A}$ as given below.

x	A	B	C	D	E	F	G	H	I	J	K	L	M
$m_3(x)$	A	D	G	J	M	P	S	V	Y	B	E	H	K
x	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$m_3(x)$	N	Q	T	W	Z	C	F	I	L	O	R	U	X

and

x	A	B	C	D	E	F	G	H	I	J	K	L	M
$p_2(x)$	A	B	E	J	Q	Z	K	X	M	D	W	R	O
x	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$p_2(x)$	N	O	R	W	D	M	X	K	Z	Q	J	E	B

Clearly m_3 is one-to-one and p_2 is not.

(a) Prove that $m_3 \circ m_3$ is one-to-one. That is, start by assuming that $m_3 \circ m_3(x) = m_3 \circ m_3(y)$ and show that $x = y$.

Solution: Suppose x and y represent two letters, and assume that $m_3 \circ m_3(x) = m_3 \circ m_3(y)$. Then

$$m_3(m_3(x)) \quad = \quad m_3(m_3(y)).$$

We know that m_3 is one-to-one, so this implies that

$$m_3(x) = m_3(y).$$

But now, again, we know that m_3 is one-to-one, so it follows that $x = y$, as required.

Alternate solution: We could just make up a table giving the values of $m_3 \circ m_3(x)$ for each letter x. We get

x	A	B	C	D	E	F	G	H	I	J	K	L	M
$m_3(m_3(x))$	A	J	S	B	K	T	C	L	U	D	M	V	E
x	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$m_3(m_3(x))$	N	W	F	O	X	G	P	Y	H	Q	Z	I	R

Since no letter is repeated in the second row of this table, we have shown directly that $m_3 \circ m_3$ is one-to-one.

(b) Is $m_3 \circ p_2$ one-to-one? Why or why not?
Is $p_2 \circ m_3$ one-to-one? Why or why not?

Solution: The composition $m_3 \circ p_2$ is not one-to-one, because $m_3(p_2(B)) = m_3(B) = D$ and $m_3(p_2(Y)) = m_3(B) = D$.

The composition $p_2 \circ m_3$ is not one-to-one, because $p_2(m_3(I)) = p_2(Y) = B$ and $p_2(m_3(J)) = p_2(B) = B$.

(c) Make a table for a function n such that $n \circ m_3(x) = x$ for all x.

Solution: Here is the function n:

x	A	B	C	D	E	F	G	H	I	J	K	L	M
$n(x)$	A	J	S	B	K	T	C	L	U	D	M	V	E

x	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$n(x)$	N	W	F	O	X	G	P	Y	H	Q	Z	I	R

B2. Set up an Excel spreadsheet as follows:

(a) Leaving the top row blank, enter the (upper-case) letters of the alphabet in cells A2 through A27 – that is, down the first column of the worksheet.

(b) In cell B2, enter the formula `=code(A2)-code("A")`. Highlight this cell, grab the small box at its lower-right corner, and drag it down the column to cell B27. Column B should now contain the numbers 0 through 25.

(c) In cell C2, enter the formula `=B2`. Highlight this cell, grab the small box at its lower-right corner, and drag it down the column to cell C27. Column C should now look just like column B.

(d) In cell D2, enter the formula `=char(C2+code("A"))`. Again, highlight the cell, grab the small box, and drag it down the column to cell D27. Column D should now look just like column A.

(e) Your worksheet is now set up to implement any arithmetic cipher (such as a shift cipher). Choose a number n between 1 and 25 for your shift key. Now go back to cell C2, and change the formula there to `=mod(B2+`n`,26)`. Highlight the formula and drag it down the column, as usual. Column D should now contain a shift of column A.

(f) Let's put some explanatory comments in the top row. Column A is the input column, so let's put an x in cell A1. Column B shows what happens when we apply the character-code function to column A, so let's put $cc(x)$ in cell B1. To

get column C, we apply a shift to column B, so cell C1 should say something like $s_n(cc(x))$. Finally, column D comes from column C by applying the inverse of the character-code function, so let's label that column with $cc^{-1}(s_n(cc(x)))$.

Print out your Excel spreadsheet with the shift cipher on it, and hand it in.