Math 139 Problem Set #1 Due 11 February 2003

Reading: Barr, Chapter 1.

Exercises: Write your solutions clearly, remembering that they will be graded for presentation as well as correctness. Please prepare *separate* solution sets for the A problems and the B problems. You will hand them in in different places.

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.

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 $g \circ f(1)$.

(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.

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

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 $x = y$.

(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?

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

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.