Math 139 Problem Set #3 Due 25 February 2003

Reading: Barr, §2.2.

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.

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 $f_{3,5}(\texttt{W}) = \texttt{T}$ (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 $\{0, 1, 2, \ldots, 25\}$.

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

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`.

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

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

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?

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.)