

# Hill Cipher Exercises (Daily Due Sept 4)

Katherine E. Stange, CU Boulder

## Exercise 1

Find the inverse of the following matrix whose entries are considered modulo 26:

$$\begin{pmatrix} 11 & 13 \\ 2 & 3 \end{pmatrix}$$

Note: you can do this exactly as you would find the inverse of a  $2 \times 2$  matrix normally, except when you need to divide by something, find the modular inverse using the table.

## Exercise 2

The matrix given in the last exercise was used as a key to a Hill cipher to encrypt a favourite vegetable of mine, and the resulting ciphertext was YGFI. What is the vegetable?

## Exercise 3

A  $2 \times 2$  Hill cipher encrypted the plaintext SOLVED to give the ciphertext GEZXDS. Find the encryption matrix.

## Exercise 4

Suppose the matrix

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

is used for a  $2 \times 2$  Hill cipher.

1. Compute the determinant. What is bad about this determinant?
2. Find two plaintexts that encrypt to the same ciphertext.