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 2×2 matrix normally, except when you need to divide by something, find the modular inverse using the table.

Solution. The determinant is $33 - 26 \equiv 33 \equiv 7 \pmod{26}$. The inverse of 7 modulo 26 (by using the table) is 15. So using the formula for the inverse of a 2×2 matrix, one obtains

$$7^{-1} \begin{pmatrix} 3 & -13 \\ -2 & 11 \end{pmatrix} \equiv 15 \begin{pmatrix} 3 & 13 \\ 24 & 11 \end{pmatrix} \equiv \begin{pmatrix} 19 & 13 \\ 22 & 9 \end{pmatrix}.$$

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?

Solution. YGFI is $24, 6, 5, 8$. The inverse of the encryption matrix is the decryption matrix. We computed this in part Exercise 1. We can decrypt the ciphertext block by block by matrix multiplication. For example, for the first block $(24, 6)$, we do

$$\begin{pmatrix} 19 & 13 \\ 22 & 9 \end{pmatrix} \begin{pmatrix} 24 \\ 6 \end{pmatrix} = \begin{pmatrix} 14 \\ 10 \end{pmatrix}.$$

This is OK. The second block is done similarly. The plaintext was OKRA. Yes, that's a vegetable.

Exercise 3

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

Solution 1: Direct approach (longish). You have an unknown key which we can write as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

We know, from the encryption method, that the block SO goes to GE etc. That gives three matrix equations, namely

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 18 \\ 14 \end{pmatrix} \equiv \begin{pmatrix} 6 \\ 4 \end{pmatrix}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 11 \\ 21 \end{pmatrix} \equiv \begin{pmatrix} 25 \\ 23 \end{pmatrix}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 4 \\ 3 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 18 \end{pmatrix}.$$

Everything we will do is modulo 26, hence the $\equiv$ signs. These are linear equations in the unknowns a, b, c, d, namely

$$\begin{aligned} 18a + 14b &\equiv 6 \\ 18c + 14d &\equiv 4 \\ 11a + 21b &\equiv 25 \\ 11c + 21d &\equiv 23 \\ 4a + 3b &\equiv 3 \\ 4c + 3d &\equiv 18 \end{aligned}$$

Taking the 1st and 3rd and eliminating a, we obtain

$$11 \cdot 18a + 11 \cdot 14b - 18 \cdot 11a - 18 \cdot 21b \equiv 11 \cdot 6 - 18 \cdot 25 \pmod{26}$$

Using the multiplication table, this becomes

$$10b \equiv 6 \pmod{26}.$$

Since 10 is not invertible, we can't cancel anything here, but looking at the 10's column in the table we find *two* solutions, namely

$$b \equiv 11, 24.$$

We use the 5th equation now: assuming $b = 24$, the equation $4a + 3b \equiv 3$ becomes $4a \equiv 9$, which has no solutions. Therefore $b = 11$. Putting that into the equation $11a + 21b \equiv 25$ gives $a = 12$.

This determines a and b. We can now do something similar to find c and d (they are 3 and 2 respectively). So the correct final matrix is:

$$\begin{pmatrix} 12 & 11 \\ 3 & 2 \end{pmatrix}.$$

Solution 2: Using matrices (a bit slicker and interesting)

Shout-out to Jordan Jones for this solution!

Instead of thinking of the plaintext/ciphertext pair giving 3 matrix equations, one for each block, we combine two blocks to give a matrix equation of this form:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 18 & 11 \\ 14 & 21 \end{pmatrix} \equiv \begin{pmatrix} 6 & 25 \\ 4 & 23 \end{pmatrix}.$$

This is of the form $AB = C$ where A is what we want to solve for. So we could try to do $A = CB^{-1}$. But that needs B to be invertible. Let's check the determinant of B: it is $18 \cdot 21 - 11 \cdot 14 \equiv 16$. So it is not invertible. But if we try a different choice of blocks from the texts, we get this:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 11 & 4 \\ 21 & 3 \end{pmatrix} \equiv \begin{pmatrix} 25 & 3 \\ 23 & 18 \end{pmatrix}.$$

In this case, B has determinant 1! So its inverse is

$$\begin{pmatrix} 3 & 22 \\ 5 & 11 \end{pmatrix}$$

Therefore,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 25 & 3 \\ 23 & 18 \end{pmatrix} \begin{pmatrix} 3 & 22 \\ 5 & 11 \end{pmatrix} \equiv \begin{pmatrix} 12 & 11 \\ 3 & 2 \end{pmatrix}.$$

Exercise 4

Suppose the matrix

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

is used for a 2×2 Hill cipher.

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

Solution. First part: The determinant is $4 - 6 = -2$. This is not invertible, which means the matrix is not invertible, which means the matrix is a bad choice for encryption because there is no associated decryption matrix.

Second part: By linear algebra, if two plaintexts $\mathbf{v}_1$ and $\mathbf{v}_2$ encrypt to the same ciphertext, then their difference encrypts to $\mathbf{0}$. So this is really a question about the kernel of the matrix. That is, we would like to solve

$$x + 2y \equiv 0, \quad 3x + 4y \equiv 0.$$

Notice that y is always multiplied by 2, so taking $y = 13$ will be the same as taking $y = 0$ in this equation (take a look at the column for multiplication by 2 in the table). Hence the plaintexts $(0, 0)$ and $(0, 13)$ will encrypt to the same ciphertext, namely $(0, 0)$.