Math 272 Lab 2 Due Fri., March 10

Introduction. This lab is about Hill cyphers – it's based on Sec. 10.14 of the text. We'll use Mathematica instead of Matlab because it's easier to find inverses of matrices mod 26 in Mathematica.

Part 1. Encoding a message. Let's say we want to send a secret message (usually called "plaintext") to our pal Vladimir. The message is I LOVE VODKA. Here's a step-by-step guide to turning a plaintext message into "cybertext."

1. First, we encode each letter of the alphabet: A = 1, B = 2, ..., $Y = 25$, Z= 0. (We use 0 instead of 26 because we will want all of our numbers to be 0–25 throughout this process.) Then

   I LOVE VODKA becomes 9 12 15 22 5 22 15 4 11 1

2. Break up the numbers into pairs, ignoring the spaces between words, and think of these as vectors:
   $$\begin{bmatrix} 9 \\ 12 \end{bmatrix}, \begin{bmatrix} 15 \\ 22 \end{bmatrix}, \begin{bmatrix} 5 \\ 22 \end{bmatrix}, \begin{bmatrix} 15 \\ 4 \end{bmatrix}, \begin{bmatrix} 11 \\ 1 \end{bmatrix}$$

3. Make up a 2×2 matrix that has an inverse modulo 26. This means that all the entries need to be between 0 and 25, and the determinant is odd, and not a multiple of 13. We'll use
   $$A = \begin{bmatrix} 1 & 4 \\ 8 & 3 \end{bmatrix}.$$

4. Multiply the matrix A by each of the vectors in step 2. If any of the numbers is larger than 25, divide that number by 26 and just take the remainder. Here's how to do this in Mathematica:

   ```
   A = {{1, 4}, {8, 3}}
   x = {9, 14}
   cypher = Mod[A.x, 26]
   ```

   Do this for each of the five vectors **x**.

5. Now convert your five cypher answers back to letters. This gives you the encoded version of the message (usually called "cyphertext") . I got

   EDYDOBEBOM

Exercise 1. Use the matrix $B = \begin{bmatrix} 1 & 1 \\ 2 & 3 \end{bmatrix}$ to encode the message LINEAR ALGEBRA. (There are an odd number of letters, so add a "dummy" letter to the end, say Z.)

Part 2: Decoding a message. Suppose you receive the message EDYDOBEBOM, and you (somehow) know the matrix A that was used to encode. How can you decode the message?

If $\mathbf{p}$ is the plaintext vector, then the cyphertext $\mathbf{c} = A\mathbf{p}$. So, to decode, we need $A^{-1}\mathbf{c} = \mathbf{p}$.

So, for example, $A \begin{bmatrix} 9 \\ 12 \end{bmatrix} = \begin{bmatrix} 5 \\ 4 \end{bmatrix}$, so $\begin{bmatrix} 9 \\ 12 \end{bmatrix} = A^{-1} \begin{bmatrix} 5 \\ 4 \end{bmatrix}$.

Thus, to decode, we need to find A^{-1}. But, since all of these numbers have to be between 0 and 25, we need our inverse mod 26. Here are the steps you need:

1. As before, convert the encrypted message EDYDOBEBOM to numbers, then pair those up to get 5 vectors.
2. Find A^{-1} mod 26. Call this inverse matrix "decode." Here's the Mathematica code:

```
decode = Inverse[A, Modulus -> 26]
```

3. Now multiply the matrix "decode" by each of the 5 vectors.
4. Finally, convert those vectors back into the original message. You should get the original message!

Exercise 2. Decode the cyphertext you produced in Exercise 1. To do this, you'll need to find the inverse (mod 26) of the matrix $B = \begin{bmatrix} 1 & 1 \\ 2 & 3 \end{bmatrix}$, then multiply that inverse by the encrypted vectors.

Exercise 3. The fun part. Suppose I give you the cyphertext BLBWOPTGKNRMDA. I'm not telling you the matrix A that was used to encrypt this message, but I will tell you the first four letters of the plaintext were THIS. Decode the message!

To find the matrix A, here's an extended hint: The letters for THIS correspond to the two column vectors $\begin{bmatrix} 20 \\ 8 \end{bmatrix}$ and $\begin{bmatrix} 9 \\ 19 \end{bmatrix}$. The first four encrypted letters are BLBW, corresponding to the two vectors $\begin{bmatrix} 2 \\ 12 \end{bmatrix}$ and $\begin{bmatrix} 2 \\ 23 \end{bmatrix}$. That means $A \begin{bmatrix} 20 & 9 \\ 8 & 19 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 12 & 23 \end{bmatrix}$.

Extra Credit. Find a partner, and make up a message to send to them. Give them the cyphertext and a hint. (Make sure your matrix has an inverse, mod 26.) Decode the cyphertext your partner gave you!