Hill Cipher

Please upload your completed Mathematica file to Moodle by 1pm on Friday:
https://lms.ats.amherst.edu/mod/assign/view.php?id=304430

Prime numbers play important roles in various encryption schemes. Hill ciphers are quite simple, while other methods are much more sophisticated, like RSA public key encryption that involves two very large prime numbers and is used for internet security.

To design a Hill cipher, we first assign a number to each letter of the alphabet, then add three punctuation marks so that we have a prime number (29) of coded letters.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

P	Q	R	S	T	U	V	W	X	Y	Z	,	.	!
16	17	18	19	20	21	22	23	24	25	26	27	28	0

The original message will be translated to a string of numbers, which will be partitioned into groups of 3 letters and formed into a matrix **P** (each group of 3 comprising a column). The matrix **P** is then multiplied by an invertible encryption matrix **M** (we want to be able to get the message back!) and the resulting numbers translated back into letters to create a coded message of apparent gibberish.

The extra bit of complication is that we want all numbers to be between 0 and 28, so we must use the "mod *p*" (modulus) operator, which takes a number and repeatedly adds or subtracts *p* until we have a number between 0 and *p*-1. In our case, we will use *p*=29.

For example, 25 mod 29 = 25, 30 mod 29=1, 183 mod 29 = 9 and -1 mod 29 = 28.

Exercise 1. Mod[*n,p*] calculates *n* mod *p*. Use Mathematica to find 201 mod 29.

Now we are ready to try out a Hill code. Suppose we want to encode "hide this message" using the encryption matrix $\mathbf{M} = \begin{bmatrix} 2 & 7 & 6 \\ 4 & 5 & 13 \\ 2 & 6 & 1 \end{bmatrix}$.

```
M = {{2,7,6},{4,5,13},{2,6,1}};
```

To check that **M** is invertible, we can use the *determinant* of **M**, denoted det(**M**). This is a number associated with every matrix, and we will study it in more detail later in the semester. For now, all we need is that a matrix is invertible if and only if its determinant is not 0 (or in this case, non-0 mod 29).

```
Det[M];
```

Exercise 2. Use Mathematica to find the determinant of **M** mod 29.

Now to encode the message:

Step 1: Remove spaces from the message to be encoded and break it up into groups of 3 letters (add extra letters to end if necessary): HID ETH ISM ESS AGE

Step 2: Replace letters with their assigned numbers 0-28 and write each group as a column of a matrix **P**, which we will call the "plaintext matrix."

```
P = Transpose[{{8, 9, 4}, {5, 20, 8}, {9, 19, 13}, {5, 19,
19}, {1, 7, 5}}]; (* to turn rows into columns *)
```

Step 3: Calculate **MP** mod 29. We will call the resulting matrix the "code matrix" **A**.

```
A = Mod[M.P,29]
```

Step 4: Replace the numbers (reading down columns) with letters to obtain the coded message: **PMPXUVZJ!YN,WQT**

Step 5: The recipient of this coded message would return it to the matrix form and then solve **M**.**P**=**A** (the solution is **P**= $\mathbf{M}^{-1}\mathbf{A}$). Here, we must be careful in finding the inverse of the matrix M, since we are working "mod 29" (this is called matrix algebra over the finite field $\mathbf{Z}_{29}$). We use a handy theorem from Number Theory that tells us the inverse of **M** when working over a finite field $\mathbf{Z}_p$: we use $(\det(\mathbf{M}))^{p-1}$ times the usual inverse of **M**.

```
Minverse=Mod[Det[M]^28 Inverse[M], 29]
```

Exercise 3. Create a message that is *at least* 24 letters long. For example, "HOORAY, MORNING CLASSES WERE CANCELLED!!" If the length of your message isn't a multiple of three, pad with extra punctuation marks. Translate into a plaintext matrix **P**.

Exercise 4. Make up a new 3x3 encryption matrix **M**. **M** should be invertible (that is, its determinant should not equal 0 modulo 29), and contain only integers between 0 and 28.

Exercise 5. Compute the code matrix **A** and translate to the coded message.

Exercise 6. Use the code matrix **A** and the encryption matrix **M** to get back the original plaintext matrix **P** (as in step 5).

Exercise 7. Suppose Naval Intelligence intercepts the following coded message and believes it was encrypted using a Hill code. They think the first three words of the message are "I THINK OUR". Find the encryption matrix and decode the rest of the message.

Coded message: **QUAS.AGFOUFCEDCLKSGPE**