Hill Cipher

We're doing cryptography - which is the sending of secret messages. First we encrypt (or hide) the message. Then send it. Someone with the "key" can then unlock the message (decrypt it) to read it.

Prime numbers play a very important role in encryption schemes. Hill ciphers, which we'll consider today, are an example of one encryption scheme. One of the most famous ones, called RSA, encrypts messages using the product of two very large prime numbers and some mathematical results from number theory. The reason why our information is safe from intruders is because it is enormously challenging to factor large numbers; i.e., ones which are the product of two primes on the order of 150 digits long (this is about the length of the ones used in practice). Computers are getting faster and faster.... which means that we need larger and larger prime numbers to hide our messages... Or we need more mathematical theory (involving elliptic curves and a new definition of "multiplication")... Want to learn more? Take the cryptography course this Spring.

But for today, Hill Ciphers. It's a more basic kind of encryption scheme based on linear algebra.

To design a Hill Cipher, we first assign a number to each letter of the alphabet. We will want an alphabet of prime length (p = 29), so let's add three punctuation marks. We want all of the numbers that we use throughout to be between 0 and 28, so we must use "modulus p" (called "mod p"). This operator takes a number and repeatedly adds or subtracts p until we arrive at a number between 0 and p-1. In other words, it is the remainder when we divide our number by the modulus (i.e., the p when we write "mod p"). It is "clock arithmetic."

We can also do mod for other (non-prime) numbers. The theory is just *really nice* when we work mod p. Want to know why? Take Groups, Rings and Fields or Cryptography.

For instance, if we were working in "mod 5", then "12 mod 5" would be 2. And "16 mod 5" would be 1. And "-3 mod 5" would be 2.

In this lab, rather than use real number scalars, we will instead use the digits {0, 1, 2, ..., 28}. This set is also a *field,* which means that we can do addition, subtraction, multiplication and division in it. **So... our vector space is over {0, 1, 2, ..., 28} rather than R.** We can also do linear algebra over complex numbers, too, just our scalars will be complex numbers and so on....

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

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

Our original message will be translated to a string of numbers, which will be broken into groups of 3 letters and formed into a matrix P (each group of 3 corresponding to a column of the matrix).

The matrix P is then multiplied by an invertible encryption matrix M (it's invertible so that we can get the matrix P back!), and then the resulting numbers are translated into letters to create a coded message (which looks like gibberish).

Question 0.5. What is 13 mod 4? What is 8 mod 29? What is 50 mod 29? What is -1 mod 5? Find the product of 8 and 5 in mod 29; first find the product, then write the answer mod 29. Verify that the inverse of 5 is 6 by showing that 5*6 is equal to 1 mod 29.

```
In[1]:= Mod[13, 4]
Out[1]= 1

In[2]:= Mod[8, 29]
Out[2]= 8

In[3]:= Mod[50, 29]
Out[3]= 21

In[4]:= Mod[-1, 5]
Out[4]= 4

In[5]:= Mod[(8 * 5), 29]
Out[5]= 11

In[6]:= Mod[(5 * 6), 29]
Out[6]= 1

In[7]:= Mod[1, 29]
Out[7]= 1
```

Now let's hide a message. Perhaps we'll take the encryption matrix to be the matrix M below:

```
In[ ]:= {{2, 7, 6}, {4, 5, 13}, {2, 6, 1}} // MatrixForm

In[8]:= M = {{2, 7, 6}, {4, 5, 13}, {2, 6, 1}}; (* make sure to run this line! *)
```

Step 1: Let's encode the message "hide this message". Remove spaces from the message and break it up into groups of 3 letters (add extra letters to the end if necessary).

Step 2: Replace letters with their assigned numbers 0-28 and write each group as a *column* of a matrix P which we call the "plaintext matrix."
The message is being held in the columns of the matrix:

HID ETH ISM ESS AGE ------> 8,9,4 5,20, 8 9,19,13 5,19,19 1,7,5

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

Use the function Mod[n, p] to calculate n mod p. To try it out use Mathematica to find 48 mod 29.

In[10]:=
```
Mod [48, 29]
```
Out[10]=
```
19
```

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

In[11]:=
```
A = Mod[M.P, 29]
(* notice that we can multiply matrices by putting a . between them *)
```
Out[11]=
```
{{16, 24, 26, 25, 23}, {13, 21, 10, 14, 17}, {16, 22, 0, 27, 20}}
```

Step 4. Replace the numbers with letters to obtain the coded message.

PMPXUVZJ?YN,WQT

Step 5: The recipient of this message would return the matrix to matrix form and solve M.P = A.
When we find the inverse of the matrix, M, [**Inverse[]**]we'd get some fractions (from the 1/determinant part)... but we want everything to be integers (counting numbers) between 0 and 28. We can get rid of fractions by multiplying by a number which is equal to "1 mod p". (This is a disguised version of 1, one of the only math tricks in the book.)

Theorem (from number theory): Suppose that p is a prime number, and x is an integer. Then

x^(p-1) mod p = 1.

Question 1.5. Test this out for yourself. Take any number to the 28th power and then mod 29.
All of the fractions are coming from a 1/det(M)... So, if we want to clear out the fractions there, we can compute the matrix inverse the normal way, and then multiply it by det(M)^(p-1) = det(M)^28 [which is just the number 1] and reduce mod 29.

In[12]:=
```
fiftyOneToTheTwentyEightPower = 51^28
```
Out[12]=
```
648 582 058 464 708 589 095 023 081 933 669 425 215 879 196 401
```

In[13]:=
```
Mod[fiftyOneToTheTwentyEightPower, 29]
```

Out[13]=
```
1
```

.....

Question 2: Find the inverse of M.

In[26]:=
```
InverseM = Inverse[M] * Det[M]^28;
InverseM // MatrixForm
InverseM = Mod[InverseM, 29]
InverseM // MatrixForm
```

Out[27]//MatrixForm=

$$\begin{pmatrix} -7\,684\,121\,061\,510\,757\,505\,542\,645\,743\,632\,364\,323\,021\,169\,039\,931\,080\,704 & 3\,052\,596\,038\,134\,410\,515\,900\,5(\\ 2\,315\,762\,511\,688\,173\,494\,821\,071\,319\,998\,794\,727\,485\,831\,765\,458\,681\,856 & -1\,052\,619\,323\,494\,624\,315\,827\,7 \\ 1\,473\,667\,052\,892\,474\,042\,158\,863\,567\,271\,960\,281\,127\,347\,487\,110\,070\,272 & 210\,523\,864\,698\,924\,863\,165\,55 \end{pmatrix}$$

Out[28]=
```
{{26, 0, 18}, {16, 27, 17}, {26, 12, 8}}
```

Out[29]//MatrixForm=

$$\begin{pmatrix} 26 & 0 & 18 \\ 16 & 27 & 17 \\ 26 & 12 & 8 \end{pmatrix}$$

Then, verify that it is the inverse (in mod 29) by multiplying it by M and then reducing mod 29. Notice, your inverse *musn't contain fractions, since we're working in {0, 1, 2, ..., 28} throughout.*

In[31]:=
```
Mod[InverseM.M, 29] // MatrixForm
```

Out[31]//MatrixForm=

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

.....

Question 3: Create a message that is at least 18 letters long. If the length of your message isn't a multiple of three, pad with extra punctuation marks. Translate into a plaintext message P.

Message = antiestablishmentarianisms?

ANT IES TAB LIS HME NTA RIA NIS MS? ---- 1,14,20 . 9,5,19 . 20,1,2 . 12,9,19 . 8,13,5 . 14,20,1 . 18,9,1 . 14,9,19 . 13,19,0

Transpose to turn rows into columns.

P = Transpose[{{1,14,20}, {9,5,19}, {20,1,2}, {12,9,19}, {8,13,5}, {14,20,1 }, {18,9,1}, {14,9,19}, {13,19,0}}];

In[49]:=
```
P = Transpose[{{1, 14, 20}, {9, 5, 19}, {20, 1, 2}, {12, 9, 19},
    {8, 13, 5}, {14, 20, 1}, {18, 9, 1}, {14, 9, 19}, {13, 19, 0}}];
P // MatrixForm
```

Out[50]//MatrixForm=

$$\begin{pmatrix} 1 & 9 & 20 & 12 & 8 & 14 & 18 & 14 & 13 \\ 14 & 5 & 1 & 9 & 13 & 20 & 9 & 9 & 19 \\ 20 & 19 & 2 & 19 & 5 & 1 & 1 & 19 & 0 \end{pmatrix}$$

.....

Question 4: Make up a new 3x3 encryption matrix M. M should be invertible (that is, its determinant

should not equal 0 or any multiple of 29 - since we are working mod 29) and contain only integers between 0 and 28. [You'll see how to calculate determinants in homework.]

In[46]:=
```
M = {{3, 1, 2}, {4, 1, 5}, {6, 7, 8}};
M // MatrixForm
Det[M]
```

Out[47]//MatrixForm=

$$\begin{pmatrix} 3 & 1 & 2 \\ 4 & 1 & 5 \\ 6 & 7 & 8 \end{pmatrix}$$

Out[48]=
```
-39
```

Now, get out a piece of paper. Get organized. What calculation do you do in order to encrypt the message? How can you then recover the original message?

encryption: A = M.P

decryption: P = M-1(A)

.....

Question 5: Compute the code matrix A and translate to the coded message into letters. Write down this gibberish message.

In[61]:=
```
A = Mod[M.P, 29]
```

Out[61]=
```
{{28, 12, 7, 25, 18, 6, 7, 2, 0}, {2, 20, 4, 7, 12, 23, 28, 15, 13}, {3, 9, 27, 26, 5, 0, 5, 9, 8}}
```

Gibberish = .BC LTI GD, YGZ RLE FW? G.E BOE ?MH

.....

Question 6: Use the code matrix A and the encryption matrix M to get back to the original plaintext message P.

P = M-1(A)

In[59]:=
```
InverseM = Mod[Inverse[M] * Det[M]^28, 29]
```

Out[59]=
```
{{23, 11, 20}, {6, 22, 21}, {21, 16, 3}}
```

In[65]:=
```
DecryptedMessageP = InverseM.A
Mod[DecryptedMessageP, 29] // MatrixForm
```

Out[65]=
```
{{726, 676, 745, 1172, 646, 391, 569, 391, 303},
 {275, 701, 697, 850, 477, 542, 763, 531, 454}, {629, 599, 292, 715, 585, 494, 610, 309, 232}}
```

Out[66]//MatrixForm=

$$\begin{pmatrix} 1 & 9 & 20 & 12 & 8 & 14 & 18 & 14 & 13 \\ 14 & 5 & 1 & 9 & 13 & 20 & 9 & 9 & 19 \\ 20 & 19 & 2 & 19 & 5 & 1 & 1 & 19 & 0 \end{pmatrix}$$

When translated with the table, we get back "ANTIESTABLISHMENTARIANISMS?"

.....

Question 7: Suppose an intelligence agency intercepts the following coded message:

QUAS.AGFOUFCEDCLKSGPE

and believes that it was encrypted using a 3x3 Hill code with p = 29. They think that the first three words of the message are "I THINK OUR". Find the encryption matrix and decode the rest of the message. *Unsolicited advice:* Make sure that you label your M, P and A matrices. Get out a piece of paper and figure out what you know and what you're trying to figure out. How are you going to be able to solve for the encryption matrix?

Find the encryption matrix M, using A and P for the first three words

A = MP; means M = A.InverseOfP

1. Convert "I THINK OUR" to a three-rowed matrix shortP using the translation table
2. Convert the beginning of our coded message "QUAS.AGFO" into a three-rowed matrix shortA using the translation table
3. Find the inverse of shortP, remove the fractions using the determinant and then find the mod of 29 and that value
4. Find the matrix product of A (shortA) and the inverse of P (shortP). This is M.

Use M to decrypt the rest of the message

1. Translate the gibberish to a three-rowed matrix A, using the given table and transposing.
2. Multiply A by the inverse of M (as deduced above)
3. Mod it by 29
4. Translate the three rowed matrix P with the table into the original plain-text message

Highlights

"I THINK OUR" = {9,20,8},{9,14,11},{15,21,18}

"QUAS.AGFO" = {17,21,1},{19,28,1},{7,6,15}

Our encryption = {{2,6,3},{4,9,1},{5,2,4}}

In[150]:=

```
(*Find the encryption matrix M*)
shortP = Transpose[{{9, 20, 8}, {9, 14, 11}, {15, 21, 18}}];
InverseShortP = Mod[Inverse[shortP] * Det[shortP]^28, 29]
shortA = Transpose[{{17, 21, 1}, {19, 28, 1}, {7, 6, 15}}];
thisM = Mod[shortA.InverseShortP, 29]

(*Now, decrypt the rest of the message*)fullA = Transpose[
   {{17, 21, 1}, {19, 28, 1}, {7, 6, 15}, {21, 6, 3}, {5, 4, 3}, {12, 11, 19}, {7, 16, 5}}];
thisInverseM = Mod[Inverse[thisM] * Det[thisM]^28, 29]
fullP = Mod[thisInverseM.fullA, 29]
fullP // MatrixForm
```

Out[151]=

```
{{11, 14, 18}, {3, 22, 25}, {11, 19, 9}}
```

Out[153]=

```
{{2, 6, 3}, {4, 9, 1}, {5, 2, 4}}
```

Out[155]=

```
{{9, 14, 26}, {15, 28, 18}, {3, 12, 24}}
```

Out[156]=

```
{{9, 9, 15, 3, 5, 2, 11}, {20, 14, 21, 15, 9, 18, 5}, {8, 11, 18, 4, 19, 15, 14}}
```

Out[157]//MatrixForm=

$$\begin{pmatrix} 9 & 9 & 15 & 3 & 5 & 2 & 11 \\ 20 & 14 & 21 & 15 & 9 & 18 & 5 \\ 8 & 11 & 18 & 4 & 19 & 15 & 14 \end{pmatrix}$$

Converting P back to plain text with this table:

ITH INK OUR COD EIS BROKEN

“I THINK OUR CODE IS BROKEN”

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