Math 2000 Project 2: Cryptography*

Subhadip Chowdhury

- **Purpose:** To learn a method of using modular arithmetic and matrix operations to encode and decode messages.
- **Prerequisite:** Matrix inverses and determinant.
- **Resources:** Feel free to use any mathematical software or website to make calculations faster.

Arithmetic Modulo n

Two integers r and s are called *congruent modulo* n if $r - s$ is an *integer* multiple of n. We denote this as

$$r \equiv s \pmod{n}$$

Another way to think of this is that both r and s have the same remainder when divided by n.

We use *modular arithmetic* almost everyday in our lives. If we want to find out what day it is **10** days after Monday, we add only **3** days since **10** is congruent to **3** modulo **7**. If we want to know what the clock reads **14** hours after **10** AM, we add only **2** to **10** since **14** is congruent to **2** modulo **12**. Here are some more abstract examples:

- $63 \equiv 11 \pmod{26}$, $39 \equiv 10 \pmod{29}$.
- $-3 \equiv 27 \pmod{30}$. This is because $(-3) - (27) = -30$, which is an integer multiple of **30**. Note that it is hard to use our second definition to interpret this claim, since we need to explicitly define what a remainder is in case of division of negative numbers. So in this case, the statement is better understood using the first definition.
- $-5 \equiv -7 \pmod{2}$. Why?

To *reduce a number modulo* n (where n is a *positive* integer) means to subtract or add multiples of n to get an integer between **0** and $n - 1$. For example, to reduce **63** modulo **26**, subtract **52** to see that $63 \equiv 11 \pmod{26}$. To reduce -3 modulo **30**, add **30** to see that $-3 \equiv 27 \pmod{30}$. Note that If the original number is positive, you can reduce it modulo n by dividing it by n and using the remainder.

*Adapted from Pearson Education website.

Exercise 1: (1+1 point)

Reduce **1001** modulo **6**. Reduce **1001** modulo **7**.

A number r is said to have an *inverse modulo* n if there is another number s such that $rs \equiv 1 \pmod{n}$. For example, $(3)(9) = 27$ which is congruent to **1** modulo **26** so **3** and **9** are inverses modulo **26**. However, **2** has no inverse modulo **26**, since $2.s - 1$ is always an odd integer and hence never divisible by **26**.

Note that the inverse of a number (in above sense) can be itself. And the inverse, if it exists, is not unique. For example, inverse of **7** modulo **8** is **7**, (also -1 and **15** etc.)

Exercise 2: (4 point)

Find an inverse modulo **4** of the numbers $0, 1, 2, 3$. If an inverse doesn't exist, explain your reasoning.

If B and C are integer matrices and reducing each entry in B modulo n yields C, we write

$$B \equiv C \pmod{n}$$

A square integer matrix $C_{k\times k}$ is said to have an inverse modulo n if there is another integer matrix $D_{k\times k}$ such that

$$CD \equiv I_k \pmod{n} \text{ and } DC \equiv I_k \pmod{n}$$

It is true that such D will exist if and only if $\det(C)$ is a number which has an inverse modulo n. We will use this result without proof.

To calculate the inverse of C modulo n, calculate the reduced echelon form of $[C \vdots I]$ by doing row operations as usual, except *use only integer multipliers* and *reduce each number modulo* n. It is important that when you scale a row you *do not divide*. Instead, multiply and then reduce modulo n. Here is an example.

Example. Suppose we want to find the inverse modulo **26** of the matrix $C = \begin{bmatrix} 1 & 0 \\ 2 & 9 \end{bmatrix}$. We set up the augmented matrix $[C\, I_2]$ and reduce it.

$$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 2 & 9 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 9 & -2 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 27 & -6 & 3 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 20 & 2 \end{bmatrix} \pmod{26}$$

Thus, the inverse of the matrix modulo **26** is $D = \begin{bmatrix} 1 & 0 \\ 20 & 3 \end{bmatrix}$.

Exercise 3: (2+2 points)

Check that $CD \equiv I_2 \pmod{26}$ and $DC \equiv I_2 \pmod{26}$ in the example above.

Secret Messages!

One simple way to encode a message is to use a *substitution cipher*. This works by substituting each letter of the alphabet by a unique symbol and rewriting the message. A disadvantage of this simple encoding system is that it preserves the frequencies of individual letters. For example, the letter **'e'** is the most common letter in English and, therefore, the letter most commonly appearing in the encoded message will probably be the substitute for **e**. That makes the code breakable by using simple statistical methods. A somewhat more sophisticated method is to divide the uncoded text into groups of letters and replace each group with another group of letters. In this project we will use *groups of two letters*. The first step in the method described here is to assign each letter in the alphabet and the three punctuation marks in the table above a corresponding number between **0** and **28**, as shown in the table. This will help us transfer the problem of letter transformations to a problem involving number transformations. In what follows we will use the underscore symbol (_) to denote blank space to avoid confusion.

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

T	*U*	*V*	*W*	*X*	*Y*	*Z*	_(blank space)	'(apostrophe)	.(full stop)
20	21	22	23	24	25	26	27	28	0

Substitution Table

You would like to send the message

HURRY_UP

to your agent on the field on an encrypted channel. To encode this message, we first divide the message into groups of two letters. If your message has an odd number of letters, we would have added a ''dummy'' letter to fill out the last pair.

HU RR Y_ UP

Exercise 4: (3 points)

Using the substitution Table, find the column vector for each pair of letters. The first is given, and you fill in the rest.

$$\text{HU} \to \begin{bmatrix} 8 \\ 21 \end{bmatrix} \qquad \text{RR} \to ? \qquad \text{YU} \to ? \qquad \text{PP} \to ?$$

Denote the above four vectors as $\vec{\mathbf{a}}, \vec{\mathbf{b}}, \vec{\mathbf{c}}$, and $\vec{\mathbf{d}}$. Transform each vector by multiplying it by the matrix $A = \begin{bmatrix} 1 & 1 \\ 0 & 3 \end{bmatrix}$, and use arithmetic modulo **29** to reduce each number you see to a new number between **0** and **28**. Call the new vectors $\vec{\mathbf{a}}_1, \vec{\mathbf{b}}_1, \vec{\mathbf{c}}_1$, and $\vec{\mathbf{d}}_1$. For example,

$$A\vec{\mathbf{a}} = \begin{bmatrix} 29 \\ 63 \end{bmatrix} \text{ and } \vec{\mathbf{a}}_1 = \begin{bmatrix} 0 \\ 5 \end{bmatrix}$$

which reads '• **E**'.

Exercise 5: (3 points)

Find $\vec{\mathbf{b}}_1, \vec{\mathbf{c}}_1$, and $\vec{\mathbf{d}}_1$.

Exercise 6: (3 points)

Finish the encrypted message:

$$\cdot E \_\_\_\_\_$$

Decoding Gibberish!

You received the following message back from your agent.

XORLKJNZBLGEOX

Suppose that you know this message was encoded using the matrix $A = \begin{bmatrix} 1 & 1 \\ 0 & 3 \end{bmatrix}$ from last section. To decode it you must create a vector for each block of two letters and multiply these by a matrix B, which is the inverse of A modulo **29**. Note that this will not be the usual inverse of A, read the first two page on how to find this matrix.

Exercise 7: (5 points)

Find the inverse of A modulo **29**.

Exercise 8: (1+7+7+1 points)

(a) Divide the coded message sent by your friend into blocks of two letters.

__ __ __ __ __ __ __

(b) Write the vector for each block:

$\vec{a}_1 = ?$ $\vec{b}_1 = ?$ $\vec{c}_1 = ?$ $\vec{d}_1 = ?$ $\vec{e}_1 = ?$ $\vec{f}_1 = ?$ $\vec{g}_1 = ?$

(c) Let B be the inverse of A modulo **29**. Multiply each of the above vector by B. Let $\vec{a} = B\vec{a}_1$, $\vec{b} = B\vec{b}_1$ etc. Find

$\vec{a} = ?$ $\vec{b} = ?$ $\vec{c} = ?$ $\vec{d} = ?$ $\vec{e} = ?$ $\vec{f} = ?$ $\vec{g} = ?$

(d) Use the Substitution Table to retrieve the letter pairs corresponding to the vectors for the decoded message. What's the decoded message?

_____

Remarks. The method used here is still not too safe because statistical analysis using tables of letter-pair frequencies can be used to break it. However, this method can be used in combination with other encoding systems to produce a more secure system. For more about this, see Elementary Linear Algebra with Applications, H. Anton and C. Rorres, Wiley, 1987.