MATH 1B03/1ZC3 Winter 2019

Lecture 25: An application to cryptography

Instructor: Dr Rushworth April 2nd

An application of linear algebra to cryptography

(from Chapter 10.14 of Anton-Rorres)

A direct application of linear algebra is in cryptography. We conclude this course by learning how to encrypt a message for secure communication using matrix multiplication.

Recall that one vector may be represented differently in two distinct bases, even though it contains the same intrinsic information. For example the vector

$$(7,\,1) = 7\,(1,\,0) + (0,\,1)$$

in the standard basis, but

$$(7,\,1) = -\frac{3}{2}\,(-3,\,1) + \frac{5}{4}\,(2,\,2)$$

so that

$$(7,\,1) = \left(-\frac{3}{2},\,\frac{5}{4}\right)_S$$

in the basis $S = \{(-3,\,1),\,(2,\,2)\}$.

In general, if you are given the vector $\mathbf{v} = (v_1,\,v_1)_S$ it is not possible to recover the co-ordinate expression of $\mathbf{v}$ in the standard basis unless you are also given the basis S.

This can be applied to secure communications in the following way.

1. Encrypt a message as a vector, then use a matrix to *change the basis*.
2. Transmit the message: any intercepting third parties do not know which basis you are using, and so the message is unreadable to them.

3. The intended recipient decrypts the message by changing back to the standard basis.

While this process is a straightforward application of matrix multiplication, we need one crucial new ingredient.

Modular arithmetic

Before we understand how to encrypt messages we must introduce modular arithmetic. There 26 letters in the English alphabet, so we want to work with matrices with only 26 possible values for their entries. To do this we need the following concepts.

Definition 25.1: Congruent integers

Let m be a positive integer. We say that two integers a and b are congruent modulo m if $a - b$ is a multiple of m.
If a is congruent to b we write

$$a = b \mod m$$

We also say that a is equal to b modulo m, or that a and b are equivalent.

Alternatively, a is congruent to b modulo m if a can be obtained from b by adding a multiple of m. That is, if

$$a = b + km$$

for some k.

One more way to think of congruence: a and b are congruent modulo m if they have the same remainder when divided by m.

Example 25.2

$$11 = 2 \mod 9$$

we can see this in two ways. First, notice that

$$11 - 2 = 9$$

Second, notice that

$$\frac{11}{9} = 1 \text{ remainder } 2$$

and

$$\frac{2}{9} = 0 \text{ remainder } 2.$$

Similarly

$$-3 = 11 \mod 7$$

as

$$-3 - 11 = -14 = 7 \times (-2)$$

Let's fix a value of m and only consider numbers up to congruence i.e. we consider a and b to be equal if $a = b \mod m$. What do we obtain?

If $m = 2$, then every number is congruent to either 0 or 1. To see this, pick an integer a. If a is even then $a = 2k$ for some k, and

$$a - 0 = 2k - 0 = 2k$$

so that $a = 0 \mod 2$ by definition. If a is odd, then $a = 2k + 1$ for some k, and

$$a - 1 = 2k + 1 - 1 = 2k$$

so that $a = 1 \mod 2$. Therefore, when viewed up to congruence modulo 2, there are only two numbers, 0 and 1!

The set of integers considered up to congruence modulo 2 is denoted $\mathbb{Z}_2$ and has two elements

$$\mathbb{Z}_2 = \{0, 1\}$$

If $m = 3$, every integer is congruent to either 0, 1, or 2. To help visualise this, think of three boxes, marked 0, 1, and 2. Given an integer a, the remainder of $\frac{|a|}{m}$ must be either 0, 1, or 2. Place a into the box corresponding to this remainder. Each of these boxes is an element of

$$\mathbb{Z}_3 = \{0, 1, 2\}$$

Question 25.3

Prove that every integer is congruent to either 0, 1, 2, or 3 modulo 4.
Hint: extend the argument given above for $m = 2$.

In general, every integer is congruent modulo m to exactly one number in the list

$$0,\ 1,\ 2,\ \ldots,\ m-2,\ m-1$$

We denote the integers considered up to congruence modulo m as

$$\mathbb{Z}_m = \{0,\ 1,\ 2,\ \ldots,\ m-2,\ m-1\}$$

The set $\mathbb{Z}_m$ is an example of a very interesting new type of number system, known as a *ring*. The study of rings and objects related to them represents the beginning of a central subject of modern mathematics. We don't have the time to do more than scratch the surface, sadly, and will limit ourselves to understanding what we need to for their application to cryptography.

From now on we fix $m = 26$, and consider $\mathbb{Z}_{26}$. As we have justified above, every integer is congruent modulo 26 to one of the following

$$0,\ 1,\ 2,\ \ldots,\ 24,\ 25$$

Given an integer a, we say that r is the residue of a if

$$a = r \mod 26$$

and $0 \leq r \leq 25$. In other words, the residue of a is the number it is congruent to on the list

$$0,\ 1,\ 2,\ \ldots,\ 24,\ 25$$

Fact 25.4: Finding the residue

Let a be an integer. Let R be the remainder of $\dfrac{|a|}{26}$.

Then the residue r of a modulo 26 is given by

$$r = \begin{cases} R, & \text{if } a \geq 0 \\ 26 - R & \text{if } a < 0 \text{ and } R \neq 0 \\ 0 & \text{if } a < 0 \text{ and } R = 0 \end{cases}$$

Example 25.5

Question: Find the residue of the following integers modulo 26

$$-29,\ 14,\ -76,\ 45$$

Answer: for -29 consider

$$\frac{29}{26} = 1 \text{ remainder } 3$$

and as $26 - 3 = 23$

$$-29 = 23 \mod 26$$

Next $14 = 14 \mod 26$ as

$$\frac{14}{26} = 0 \text{ remainder } 14$$

Further, we have

$$\frac{76}{26} = 2 \text{ remainder } 24$$

so

$$-76 = 2 \mod 26$$

Finally

$$\frac{45}{26} = 1 \text{ remainder } 19$$

so

$$45 = 19 \mod 26$$

Reciprocals modulo 26

We are familiar with the concept of a reciprocal from the standard rational numbers. Given a we define the number a^{-1} to be the number such that

$$aa^{-1} = a^{-1}a = 1$$

Every rational number has a well-defined reciprocal. When we work with numbers in $\mathbb{Z}_{26}$ this is no longer the case, however. For example, when using arithmetic modulo 26 the number 13 does not possess a reciprocal i.e. 13^{-1} does not exist.

To see this, notice that

$$2 \times 13 = 26 = 0 \mod 26$$

If 13^{-1} did exist, then

$$\begin{aligned} 1 &= 13 \times 13^{-1} \\ 2 &= 2 \times 13 \times 13^{-1}, \text{ by multiplying from the left by } 2 \\ 2 &= 0 \times 13^{-1} \mod 26 \\ 2 &= 0 \mod 26 \end{aligned}$$

but $2 \neq 0$ so 13^{-1} does not exist.

(The failure of certain numbers to have reciprocals modulo 26 is an important property of rings, known as the presence of *zero divisors*.)

For our purposes we need to know which numbers possess reciprocals modulo 26.

Definition 25.6: Reciprocal modulo 26

Let a be an integer. We say that b is the reciprocal modulo 26 of a if

$$ab = 1 \mod 26$$

We write $b = a^{-1}$.

Fact 25.7

An integer does not possess a reciprocal modulo 26 if and only if it has 2 or 13 as a factor.
The integers which do possess reciprocals modulo 26 are as follows

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

The reciprocals modulo 26 of integers greater than 25 are found by first finding the residue, then using Fact 25.7.

Let's check one of the entries on the list:

$$\begin{aligned} 25 \times 25 &= 625 \\ \frac{625}{26} &= 24 \text{ remainder } 1 \text{ so that} \\ 625 &= 1 \mod 26 \end{aligned}$$

therefore $25^{-1} = 25$.

Question 25.8

Verify the remaining reciprocals given in Fact 25.7.

Invertibility of matrices modulo 26

We are going to encrypt messages using matrices with entries in $\mathbb{Z}_{26}$. Given a message we will use a fixed matrix M to encrypt it. The intended recipient will need to apply the inverse matrix M^{-1} to the decrypt the message. If M^{-1} does not exist, this will not be possible.

Definition 25.9: Matrix inverse modulo 26

Let M be an 2×2 matrix

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

for a, b, c, d integers. The matrix $M \mod 26$ is defined

$$M \mod 26 = \begin{bmatrix} a \mod 26 & b \mod 26 \\ c \mod 26 & d \mod 26 \end{bmatrix}$$

That is, it is the matrix with entries treated as elements of $\mathbb{Z}_{26}$.
The inverse modulo 26 of M is a matrix M^{-1} such that

$$MM^{-1} = M^{-1}M = I \mod 26$$

where I is the 2×2 identity matrix. If such an M^{-1} exists we say that M is invertible modulo 26.

We need to take extra care when checking if M is invertible modulo 26. To see why, let M be the 2×2 matrix

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

We know that the inverse, if it exists, is given by

$$M^{-1} = det(M)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Notice the presence of the term $det(M)^{-1}$, the reciprocal of $det(M)$. When we are working with the standard integers, the only number which does not possess a reciprocal is 0 i.e. $det(M)^{-1}$ exists if and only if $det(M) \neq 0$.

However, as we saw above, when we work with numbers in $\mathbb{Z}_{26}$ many numbers do not possess reciprocals.

Fact 25.10

A matrix M is invertible modulo 26 if and only if $det(M)$ possess a reciprocal modulo 26.

Example 25.11

Question: Determine if the following matrices matrices are invertible modulo 26 and find their inverses if they exist

$$A = \begin{bmatrix} 0 & 14 \\ 23 & 12 \end{bmatrix} \quad B = \begin{bmatrix} -3 & 15 \\ 23 & 0 \end{bmatrix}$$

Answer: Calculate the determinant

$$\begin{aligned} det(A) &= 0 \times 12 - 14 \times 23 \\ &= -14 \times 23 \end{aligned}$$

As 14 does not possess a reciprocal modulo 26 then -14×23 does not either. We can verify this as follows:

$$det(A) = -14 \times 23 = -322$$

Now find the residue of -322:

$$\begin{aligned} \frac{322}{16} &= 12 \text{ remainder } 10 \\ 26 - 10 &= 16 \text{ so that} \\ det(A) = -322 &= 16 \mod 26 \end{aligned}$$

as 16 has 2 as a factor 16^{-1} does not exist, so that $det(A)^{-1}$ does not exist. Therefore the matrix A is not invertible modulo 26.
Next compute $det(B)$

$$det(B) = -3 \times 0 - 15 \times 23$$

As both 15 and 23 possess reciprocals modulo 26, the product -15×23 possesses a reciprocal also.
Recall that $15^{-1} = 7$ and $23^{-1} = 17$, therefore

$$det(B)^{-1} = (-15 \times 23)^{-1} = 23^{-1} \times 15^{-1} = -17 \times 7$$

To verify this, notice that

$$\begin{aligned} (-15 \times 23) \times (-17 \times 7) &= 15 \times (23 \times 7) \times 7 \\ &= 15 \times 1 \times 7 \mod 26 \\ &= 1 \mod 26 \end{aligned}$$

as required.
We have

$$det(B)^{-1} = -17 \times 7 = -119 = 11 \mod 26$$

so that B^{-1} exists and is found via the formula

$$\begin{aligned} B^{-1} &= 11 \begin{bmatrix} 0 & -15 \\ -23 & -3 \end{bmatrix} \\ &= \begin{bmatrix} 0 & -15 \times 11 \\ -23 \times 11 & -3 \times 11 \end{bmatrix} \\ &= \begin{bmatrix} 0 & -165 \\ -253 & -33 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 17 \\ 7 & 19 \end{bmatrix} \end{aligned}$$

Encrypting messages

We now have the tools to encrypt messages.

We will use the following table to convert letters into elements of $\mathbb{Z}_{26}$

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	14

O	P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25	0

Given a message in plaintext, we will form an encrypted message known as the Hill cipher.

Recipe 25.12: Producing a Hill cipher

Use this recipe to encrypt a message into a Hill cipher, given a 2×2 matrix A which is invertible modulo 26.

Step 1: Given a message such as

I LOVE MATRICES

group the letters into pairs. If the total number of letters is odd, add a dummy copy of the last letter at the end:

IL OV EM AT RI CE SS

Step 2: Use the table above to convert each pair of letters into a 2×1 column vector. For example

$$\text{IL} \mapsto \mathbf{p}_1 = \begin{bmatrix} 9 \\ 12 \end{bmatrix}$$

and

$$\text{AT} \mapsto \mathbf{p}_4 = \begin{bmatrix} 1 \\ 20 \end{bmatrix}$$

Step 3: Compute the products modulo 26

$$A\mathbf{p}_1, A\mathbf{p}_2, \ldots, A\mathbf{p}_n$$

For example

$$\begin{bmatrix} 75 \\ -11 \end{bmatrix} = \begin{bmatrix} 23 \\ 15 \end{bmatrix} \mod 26$$

Step 4: Convert the new vectors back to letter pairs. For example

$$\begin{bmatrix} 23 \\ 15 \end{bmatrix} \mapsto \text{WO}$$

and assemble the encrypted message.

Example 25.13

Question: Find the Hill cipher of the message

I LOVE MATRICES

using the matrix

$$A = \begin{bmatrix} 0 & 9 \\ 3 & 2 \end{bmatrix}$$

Answer: Group the letters into pairs (adding a dummy at the end if required)

IL OV EM AT RI CE SS

Form the vectors

$$\mathbf{p}_1 = \begin{bmatrix} 9 \\ 12 \end{bmatrix}, \mathbf{p}_2 = \begin{bmatrix} 15 \\ 22 \end{bmatrix}, \mathbf{p}_3 = \begin{bmatrix} 5 \\ 13 \end{bmatrix}, \mathbf{p}_4 = \begin{bmatrix} 1 \\ 20 \end{bmatrix}$$
$$\mathbf{p}_5 = \begin{bmatrix} 18 \\ 9 \end{bmatrix}, \mathbf{p}_6 = \begin{bmatrix} 3 \\ 5 \end{bmatrix}, \mathbf{p}_7 = \begin{bmatrix} 19 \\ 19 \end{bmatrix}$$

Compute the products modulo 26

$$A\mathbf{p}_1 = \begin{bmatrix} 108 \\ 51 \end{bmatrix} = \begin{bmatrix} 4 \\ 25 \end{bmatrix} \mod 26$$
$$A\mathbf{p}_2 = \begin{bmatrix} 198 \\ 89 \end{bmatrix} = \begin{bmatrix} 16 \\ 11 \end{bmatrix} \mod 26$$
$$A\mathbf{p}_3 = \begin{bmatrix} 117 \\ 41 \end{bmatrix} = \begin{bmatrix} 13 \\ 15 \end{bmatrix} \mod 26$$
$$A\mathbf{p}_4 = \begin{bmatrix} 180 \\ 43 \end{bmatrix} = \begin{bmatrix} 24 \\ 17 \end{bmatrix} \mod 26$$
$$A\mathbf{p}_5 = \begin{bmatrix} 81 \\ 72 \end{bmatrix} = \begin{bmatrix} 3 \\ 20 \end{bmatrix} \mod 26$$
$$A\mathbf{p}_6 = \begin{bmatrix} 45 \\ 19 \end{bmatrix} = \begin{bmatrix} 19 \\ 19 \end{bmatrix} \mod 26$$
$$A\mathbf{p}_7 = \begin{bmatrix} 171 \\ 95 \end{bmatrix} = \begin{bmatrix} 15 \\ 17 \end{bmatrix} \mod 26$$

Find new letter groups

$$\begin{bmatrix}4\\25\end{bmatrix} \mapsto \text{DY}$$
$$\begin{bmatrix}16\\11\end{bmatrix} \mapsto \text{PK}$$
$$\begin{bmatrix}13\\15\end{bmatrix} \mapsto \text{MO}$$
$$\begin{bmatrix}24\\17\end{bmatrix} \mapsto \text{XQ}$$
$$\begin{bmatrix}3\\20\end{bmatrix} \mapsto \text{CT}$$
$$\begin{bmatrix}19\\19\end{bmatrix} \mapsto \text{SS}$$
$$\begin{bmatrix}15\\17\end{bmatrix} \mapsto \text{OQ}$$

Then the Hill cipher is

DYPKMOXQCTSSOQ

We can also decrypt messages, if we know the matrix used to encrypt them.

Recipe 25.14: Decrypting a Hill cipher

Given a message which has been encrypted using a matrix A, find the inverse of A modulo 26.
Then repeat the process given in Recipe 25.12 on the encrypted message, this time using A^{-1} modulo 26 (instead of A).

Example 25.15

Question: Decrypt the Hill cipher

YBVQTYEUUBGGBM

which has been encrypted using the matrix

$$A = \begin{bmatrix} -4 & 3 \\ 1 & 2 \end{bmatrix}$$

Answer: First find A^{-1} modulo 26:

$$\begin{aligned} det(A) &= (-4) \times 2 - 3 \\ &= -11 \\ &= 15 \mod 26 \end{aligned}$$

We have $15^{-1} = 7$, so

$$\begin{aligned} A^{-1} &= 7 \begin{bmatrix} 2 & -3 \\ -1 & -4 \end{bmatrix} \\ &= \begin{bmatrix} 14 & -21 \\ -7 & -28 \end{bmatrix} \\ &= \begin{bmatrix} 14 & 5 \\ 19 & 24 \end{bmatrix} \mod 26 \end{aligned}$$

Splitting the Hill cipher into pairs of letters

YB VQ TY EU UB GG BM

and applying Recipe 25.12 with A^{-1} we obtain

VE CT OR SA RE CO OL

which yields the decrypted message

VECTORS ARE COOL

Extending the method

There are a number of ways this method can be extended to make it more useful and more secure.

We used arithmetic modulo 26 as there are 26 letters in the alphabet. If we wanted to transmit messages which also contain the characters 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 we would have to use arithmetic modulo 36 i.e. work with matrices with entries in

$\mathbb{Z}_{36}$.

We also grouped the letters of a message into pairs, and used 2×2 matrices to encrypt the message. There are $26^4 = 456,976$ possible 2×2 matrices with entries in $\mathbb{Z}_{26}$.

What if we group the letters of the messages into triples, and use 3×3 matrices instead? There are $26^9 = 5,429,503,678,976$ possible 3×3 matrices with entries in $\mathbb{Z}_{26}$, so this drastically increases security.

Suggested Problems

Practice the material covered in this lecture by attempting the following questions from Chapter 10.14 of Anton-Rorres, starting on page 662

- Questions $1, 2, 3, 7, 8$