Week 13
Term 2
2022

Learning Brief

MA1

Consumer Arithmetic, Algebra & Matrices, Shape & Measurement

NAME_____

Goals

Unit goals

- Understand the concepts and techniques introduced in consumer arithmetic, algebra and matrices and shape and measurement.
- Apply reasoning skills and solve practical problems.

This week:

- Encoding and decoding using a shift factor
- Encoding and decoding using matrix addition
- Encoding and decoding using matrix multiplication

Theoretical Components

Resources:

For this week the theory work is in the *PDF file:* Week *1*3 Notes & Exercises

Mathspace Lesson on Matrix Multiplication:

https://bit.ly/3ntgT6C

Mathspace Lesson on Applications of Matrices:

https://bit.ly/2PsbUGC

Knowledge Checklist

- Encode, decode
- Shift factor
- Matrix shift
- Encoder matrix
- Decoder matrix
- Inverse matrix

Practical Components

Order

1. Complete the questions in the *Booklet*.
2. Complete the Investigation below.
3. Submit the questions for marking.
4. Complete the matrices quiz on Google Classroom.

Investigation

On HawkerMaths.com – attached to the brief.

On-line Quiz

Complete any outstanding Mathspace quizzes.

Encoding and Decoding Information

History has many accounts of the vital role that codes have played in protecting sensitive information used in wars and conspiracies. In the 1570's Mary, Queen of Scots, sent encoded messages from prison to Catholic supporters who planned to overthrow the Protestant Queen Elizabeth (Queen of England). Elizabeth was reluctant to execute her cousin Mary without direct evidence linking her to the plot. The charges were laid by the Principal Secretary, Sir Francis Walsingham. Unfortunately for Mary, Walsingham was also England's spymaster. He used an expert to break the code, and Mary was duly beheaded on February 8th, 1587.

Perhaps the most famous is the so called 'Enigma' code. During the Second World War the Germans used a machine to encode their messages. Alan Turing, a British mathematician developed the 'Bombe', a machine which eventually led to the ability to decode the German messages. This greatly helped the Allied war effort.

In the past codes usually involved swapping letters in a message for other letters. This is called **encoding** the message. It must be done using some specific pattern so that the **encoded** message can later be **decoded** by the person receiving the message.

Suppose we think of each letter as a number:

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

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

The weakness of this type of code is that in the English language, *E* is the most frequent occurring letter, followed by *T* and then *A*. A table of frequencies for letters can be used to replace numbers occurring in about the same frequency and hence break the code.

How Does it Work?

To encode a message, we could add or subtract a fixed number for each letter in our message.

This number is called a **shift factor**.

Using a shift factor of +5

"THE CAT" which is represented as	(20, 8, 5, 3, 1, 20)	We do not worry about the space between words.
would become	(25, 13, 10, 8, 6, 25)	
and so be **encoded** as	YMJHFY	

To **decode** such a message, we would use a shift factor of -5 so that

YMJHFY (25, 13, 10, 8, 6, 25)

would **decode** back to (20, 8, 5, 3, 1, 20) …"THE CAT"

Exercise Set 1

Q1. Encode the following message ATTACK AT DAWN using a shift of -5.

Note that the initial encoding gives numbers less than zero. To get around this add 26 to those numbers and then convert to a letter.

Q2. Decode the following message which was **encoded** using a shift factor of -3:

QEBPBZOBQZLABFPFQEOBB

It may help to rewrite the code with the letters 'spread' so that you can easily see the numbers beneath.

These types of codes are easy to break as any given letter is always **encoded** with the same code letter.

A big improvement is to use a **matrix shift.**

Instead of adding or subtracting the same number each time, we can apply a matrix such as (3 -1 0 5) which could also be written as $\begin{bmatrix} 3 & -1 \\ 0 & 5 \end{bmatrix}$ as the shift (or encoder).

Using this method, the message to be **encoded** is grouped into fours. In each group, the first letter has 3 added, the second has 1 subtracted, the third letter is unchanged, and the fourth letter has 5 added. This procedure is repeated for each group of four letters. If the last group has less than four letters, then you only use as many elements of the matrix as you need. You do not need to add spaces at the end.

For example, using the above matrix, we would encode: "STEAL PLANS" using the algorithm

Step 1: Group the message into fours STEA| LPLA |NS |

Step 2: Write each group of four as a matrix of numbers

$$\begin{bmatrix} S & T \\ E & A \end{bmatrix} \quad \begin{bmatrix} L & P \\ L & A \end{bmatrix} \quad \begin{bmatrix} N & S \\ & \end{bmatrix}$$

$$\begin{bmatrix} 19 & 20 \\ 5 & 1 \end{bmatrix} \quad \begin{bmatrix} 12 & 16 \\ 12 & 1 \end{bmatrix} \quad \begin{bmatrix} 14 & 19 \\ & \end{bmatrix}$$

Step 3: Add the encoder matrix $\begin{bmatrix} 3 & -1 \\ 0 & 5 \end{bmatrix}$ to each matrix to obtain

$$\begin{bmatrix} 3 & -1 \\ 0 & 5 \end{bmatrix} + \begin{bmatrix} 19 & 20 \\ 5 & 1 \end{bmatrix} = \begin{bmatrix} 22 & 19 \\ 5 & 6 \end{bmatrix}$$

$$\begin{bmatrix} 3 & -1 \\ 0 & 5 \end{bmatrix} + \begin{bmatrix} 12 & 16 \\ 12 & 1 \end{bmatrix} = \begin{bmatrix} 15 & 15 \\ 12 & 6 \end{bmatrix}$$

$$\begin{bmatrix} 3 & -1 \\ 0 & 5 \end{bmatrix} + \begin{bmatrix} 14 & 19 \\ & \end{bmatrix} = \begin{bmatrix} 17 & 18 \\ & \end{bmatrix}$$

Thus, our encoded message is

$$\begin{bmatrix} 22 & 19 \\ 5 & 6 \end{bmatrix} \quad \begin{bmatrix} 15 & 15 \\ 12 & 6 \end{bmatrix} \quad \begin{bmatrix} 17 & 18 \\ & \end{bmatrix}$$

Step 4: Convert these numbers to letters to get the **encoded** message

VSEFOOLFQR

To decode this message, you would use the **decoder matrix**. The decoder matrix is found by multiplying the encoder matrix by -1.

$$-1 \times \begin{bmatrix} 3 & -1 \\ 0 & 5 \end{bmatrix} = \begin{bmatrix} -3 & 1 \\ 0 & -5 \end{bmatrix}$$

$\begin{bmatrix} -3 & 1 \\ 0 & -5 \end{bmatrix}$ is added to each of the encoded matrices to return to the original message.

Exercise Set 2

Q1. Encode the message “KILL THEM NOW” using the matrix shift $\begin{bmatrix} -3 & 5 \\ 7 & 4 \end{bmatrix}$

Q2. The matrix shift $\begin{bmatrix} 3 & -2 \\ 4 & 0 \end{bmatrix}$ was used to encode a message. The result is IYPLEYGK. Decode this message.

Q3. a) Encode the message SEND MONEY PLEASE using the encoding matrix $\begin{bmatrix} 2 & 7 \\ 13 & 5 \end{bmatrix}$

b) What is the decoding matrix?

Q4. Create a short message. Choose an encoding matrix and encode the message. State the decoding matrix and verify that it works or better still work in pairs and get your partner to decode your message.

Now For The Hard(er) Part

An even more effective means of encoding makes use of **matrix multiplication**. This uses the technique we learnt last week.

To encode the message FALL BACK the following steps are used.

Step 1 Write the message using 2 × 2 matrices.

$\begin{bmatrix} F & A \\ L & L \end{bmatrix} \begin{bmatrix} B & A \\ C & K \end{bmatrix}$ If any gaps are left fill it with a zero.

Step 2 Replace each letter with its corresponding number from the alphabet.

$\begin{bmatrix} 6 & 1 \\ 12 & 12 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 3 & 11 \end{bmatrix}$

Step 3 Now the matrix is encoded by multiplying it by encoding matrix known only to the sender and receiver.

For this example, the encoding matrix is $\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}$

$\begin{bmatrix} 6 & 1 \\ 12 & 12 \end{bmatrix}$ x $\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}$ = $\begin{bmatrix} 15 & 8 \\ 60 & 36 \end{bmatrix}$ = $\begin{bmatrix} 15 & 8 \\ 8 & 10 \end{bmatrix}$ After subtracting 26's from 60 and 36

$\begin{bmatrix} 2 & 1 \\ 3 & 11 \end{bmatrix}$ x $\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}$ = $\begin{bmatrix} 7 & 4 \\ 39 & 25 \end{bmatrix}$ = $\begin{bmatrix} 7 & 4 \\ 13 & 25 \end{bmatrix}$

FALL BACK in matrix form is $\begin{bmatrix} 6 & 1 \\ 12 & 12 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 3 & 11 \end{bmatrix}$ and encodes to $\begin{bmatrix} 15 & 8 \\ 8 & 10 \end{bmatrix} \begin{bmatrix} 7 & 4 \\ 13 & 25 \end{bmatrix}$

Which then is written 15, 8, 8, 10, 7, 4, 13, 25

This as a code becomes OHHJGDMY

The Inverse Matrix

To decode a message we need to use the **inverse matrix**. This can be compared to multiplying a number by its

inverse eg $2 \times \frac{1}{2} = 1$. Multiplying a matrix by its inverse gives the equivalent of 1 in a matrix form. This matrix

is called the **identity matrix** and is written $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

If a matrix is of the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ then the inverse matrix is found by using the rule

Inverse matrix = $\frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

When applied to the matrix $\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}$ this becomes

$\frac{1}{2 \times 2 - 1 \times 3}$ $\begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix}$ which equals $\frac{1}{1}$ $\begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix}$ which simplifies to $\begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix}$

Note Values of *a, b, c, d* were chosen so that a*d* – *bc* = 1 which makes the inverse matrix simpler (no fractions)

The inverse matrix of message. $\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}$ $\begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix}$ and this is the matrix needed to decode the

FALL encoded to $\begin{bmatrix} 15 & 8 \\ 8 & 10 \end{bmatrix}$ and $\begin{bmatrix} 15 & 8 \\ 8 & 10 \end{bmatrix}$ x $\begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix}$ = $\begin{bmatrix} 6 & 1 \\ 12 & 12 \end{bmatrix}$ = $\begin{bmatrix} F & A \\ L & L \end{bmatrix}$

Luckily, there are on-line calculators which will do most of the work for you. One of these is

https://www.mathsisfun.com/algebra/matrix-calculator.html

Summary

1. Organise the message into 2 × 2 matrices
2. Replace the letters with numbers
3. Use an online calculator to multiply the message matrix by the encoder matrix.
4. Make sure the encoded matrix has all numbers less than 26
5. To **decode** use the online calculator to find the inverse matrix (of the encoder matrix)
6. Multiply the decoded matrix by the inverse matrix.
7. Replace the numbers with letters to get the original message.

Exercise Set 3

For these questions you may use the online calculator (matrix multiplication).

Q1. a) Make up an 8 letter message and encode it using the encoding matrix $\begin{bmatrix} 1 & 1 \\ 3 & 4 \end{bmatrix}$

b) What is the decoding matrix?

c) Verify that this decoding matrix takes you back to the original message.

Q2. a) Write a message and encode it using an encoding matrix of your choice.

b) Give your encoded message and the encoding matrix to another person. Include the name of this person so I can check your working.

Person you gave message to:

Person you received message from:

Decode the message you were given. Show working.

MA1 Week 13 Investigation

You are a secret agent, and your colleague has just broken into an enemy organisation's office and uncovered some secret plans. Unfortunately, they are now stuck inside the building, and need a password in order to escape. They have found an encrypted message: KYCUDQHJXKSKAQML and an encoding matrix $\begin{bmatrix} 8 & 5 \\ 3 & 2 \end{bmatrix}$, but do not know how to decrypt the message to receive the correct password.

a) What is the <u>decoding</u> matrix for the encoding matrix $\begin{bmatrix} 8 & 5 \\ 3 & 2 \end{bmatrix}$?

b) Put the encrypted message into 2x2 matrices and replace each letter with its corresponding number from the alphabet.

c) Multiply each of the matrices by the decoding matrix.

d) Translate each matrix into their corresponding letter values (remember to keep subtracting 26 until all your numbers are between 1-26!) .

e) What is the final decoded message?

MARKING RUBRIC

CRITERIA	EXPECTATIONS	POSS	MULT	GIVEN	TOTAL
Practical	Student completes practical work, including exercises and Mathspace task, of the brief to an acceptable standard set by the teacher.	**2**	**3**		**/6**
Portfolio Task	Student completes the investigation task of the week to an acceptable standard set by the teacher.	**2**	**2**		**/4**
Reasoning and Communications	Student responses are accurate and appropriate in presentation of mathematical ideas, with clear and logical working out shown.	**4**	**-**		**/4**
Concepts and Techniques	Student submitted work selects and applies appropriate mathematical techniques to solve practical problems and demonstrates proficiency in the use of mathematical facts, techniques and formulae.	**4**	**-**		**/4**
	Submission Guidelines				
Timeliness	Student submits the exercises, Mathspace task and investigation by the set deadline. See scoring guidelines for specific details.	**2**	**-**		**/2**
				FINAL	**/20**

Student Reflection:

How did you go with this week's work? What was interesting? What did you find easy? What do you need to work on?

Mathspace task title:

Mathspace score: