A coding exercise

MATH390

June 2011

1 Your brief

You will be in groups of size 3, 4, 5 or 6. There will be 6 groups in each class. You will need access to a laptop running *Microsoft Excel, OpenOffice.org Calc* or a similar spreadsheet package. The exercise is divided into two parts:

- In part one, you will be given a matrix to use as an **encoding key** and a short passage of text. Apply a coding method to the text and pass the encoded text to the group on your left.
- In part two, you will receive a coded message from the group on your right, together with their encoding key. By inverting this matrix, find the **decoding key** and use this to decode the message.

2 Your method

A **message** is a string of 140 characters or less, made up of 27 possible characters – the letters A to Z plus space. To encode a message:

- Convert the message into a sequence of column vectors;
- Use the matrix you have been given as an encoding key;
- Apply this matrix to each of the column vectors to obtain a sequence of coded column vectors;
- Convert these vectors back into characters to obtain the coded message.

To decode a message, having been given the encoding key:

- Find the decoding key by inverting the encoding key;
- Apply the decoding key to the coded message, using the coding method above, to obtain the decoded message.

3 Converting characters into column vectors

Consider the following table, based on a standard mobile phone keypad layout where S and Z have been moved to the top left key (…denotes a space):

		2nd digit		
		0	1	2
1st digit	0	…SZ	ABC	DEF
	1	GHI	JKL	MNO
	2	PQR	TUV	WXY

Use this table to encode each character as a three-digit number in base 3 – each digit is 0, 1 or 2. The first two digits are read from the table; the third is given by whether the character appears first, second or third on its key (0 for first, 1 for second and 2 for third). E becomes 021, for example. Treat each three-digit number as a column vector with three components, each of which is an element of $\mathbb{Z}_3$, the set of integers modulo 3. So:

$$Character \mapsto \begin{pmatrix} Row \\ Column \\ Keystrokes \end{pmatrix}$$

and thus, for example:

$$HORSE \mapsto \begin{pmatrix} 1 & 1 & 2 & 0 & 0 \\ 0 & 2 & 0 & 0 & 2 \\ 1 & 2 & 2 & 1 & 1 \end{pmatrix}.$$

There is a bijection between the set of all three-dimensional vectors with entries in $\mathbb{Z}_3$ and the set of letters in the English alphabet, plus space – both have 27 elements.

4 Your encoding key

Your encoding key will be a 3 x 3 invertible matrix K whose entries are 0, 1 or 2. Treat K as a matrix with entries in $\mathbb{Z}_3$, the set of integers modulo 3. As it is invertible, the determinant will not be a multiple of 3. For example, you might receive:

$$K = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

whose determinant is 1.

5 Encoding your message

Apply K to each column vector in turn, calculating your answers modulo 3, to get a sequence of encoded column vectors. Next apply the same conversion table you used earlier to convert these vectors back into characters. For the choice of K above:

$$K \begin{pmatrix} 1 & 1 & 2 & 0 & 0 \\ 0 & 2 & 0 & 0 & 2 \\ 1 & 2 & 2 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 1 & 1 & 0 \\ 1 & 1 & 2 & 1 & 0 \\ 1 & 2 & 2 & 1 & 1 \end{pmatrix} \mapsto UVOKS.$$

Notice that a space encodes as a space, whatever the choice of K. For some choices of K, other characters will be left unaltered by the action of K. For other choices of K, all characters other than space will be altered. An effective encoding key will not leave any vector unaltered. You should now have an encoded message of the same length as your original. Pass this to the group on your left, together with your matrix K. You will now receive a coded message, plus matrix, from the group on your right.

6 Decoding another group's message

The decoding process is identical to the encoding process except that you will need to use the correct decoding key D. This is the 3 x 3 invertible matrix whose entries are 0, 1 or 2, given by the formula:

$$D = K^{-1} \pmod 3.$$

The decoding key D is the inverse of the encoding key K in the matrix ring $M_3(\mathbb{Z}_3)$. Having found D you may apply it to the coded message and, hopefully, recover the original message. Alternatively, there is a method of decoding the message without calculating D. You may wish to think about what this method would be.

7 Examining the decoded message

Finally, examine the message you have just decoded. Can you identify which work of literature it comes from?