

1. Working in  $\mathbb{Z}_{60}$  :

- (a)  $\gcd(17, 60) = 1$  as 17 is prime and doesn't divide 60  
or a Euclid's Algorithm method
- (b) 17 **does** have a *multiplicative inverse* in  $\mathbb{Z}_{60}$ ,  
because  $\gcd(17, 60) = 1$ .
- (c)  $17 \times 7 = 119 = 2 \times 60 - 1 = -1$  in  $\mathbb{Z}_{60}$ .
- (d)  $17^{-1} = -7 = 53$  in  $\mathbb{Z}_{60}$ . (either ans is fine)
- (e) \*  $17^{17} = 17^{16} \times 17 = 1 \times 17 = 17$  in  $\mathbb{Z}_{60}$ .

[2 + 2 + 1 + 1 + 1\* = 7 marks]

2. We are implementing the **RSA public key cryptosystem** with base  $m = 77$ .

- (a)  $77 = 7 \times 11$ .
- (b) Calculate  $n = \phi(m) = (7 - 1) \times (11 - 1) = 60$ .
- (c) If the encryption key  $e$  is 17, the decryption key  $d = 53$ .
- (d) Calculate  $21^{31}$  in  $\mathbb{Z}_{77}$ .

$$\begin{array}{r} 21 \ 31 \\ 56 \ 15 \\ 21 \ 7 \\ 56 \ 3 \\ 21 \ 1 \end{array}$$

$$\text{So } 21^{31} = 21 \times 56 \times 21 \times 56 \times 21 = 56^2 \times 21^2 \times 21 = 21 \times 56 \times 21 = 21^2 \times 56 = 56 \times 56 = 21.$$

- (e) A *public key cryptosystem* is a method of encrypting messages where the means for encryption may be made public **without** giving away/compromising the means of decrypting.

[1 + 1 + 2 + 3 + 1 = 8 marks]

3. (a)  $0 = a = 15^2$  in  $\mathbb{Z}_{25}$ .

- (b) \*  $15^n = 15^2 \times 15^{n-2}$  where  $n - 2 > 0$  so  $15^n = 0 \times 15^{n-2} = 0$ .

- (c) \* The RSA public key cryptosystem is not implementable with base  $m = 25$  as for any  $e > 1$  both 15 and 0 encrypt to 0 thus decryption is not possible.

[2 + 1\* + 1\* = 4 marks]

4. (a) The rank of  $A$  is 3.
- (b)  $\{(0, 1, 2, 2)^T, (2, 3, 2, 1)^T, (3, 2, -2, 7)^T\}$  is a basis for the column space.
- (c) The dimension of the row space of  $A$  is 3.
- (d) The rows of  $A$  **are not linearly independent** as 4 vectors cannot be linearly independent in a dimension 3 space.
- (e) The vectors  $(0, 1, 2, 2), (0, -2, -2, -4), (2, 3, 2, 1), (-4, -1, 6, 8), (3, 2, -2, 7)$  **do not span**  $\mathbb{R}^4$  as they are the columns for  $A$  and hence only span a dimension 3 space.
- (f)  $(-4, -1, 6, 8) = 5 \cdot (0, 1, 2, 2) - 2 \cdot (2, 3, 2, 1)$ .
- (g) A basis for the solution space of  $A$  is  $\{(2, 1, 0, 0, 0)^T, (-5, 0, -2, 1, 0)^T\}$ .
- (h) Let  $T : \mathbb{R}^5 \rightarrow \mathbb{R}^4$  be the linear transformation with standard matrix  $A$ . Rank of  $T = \dim(\text{Im}(T)) = \dim(\text{ColSpace}(A)) = 3$  and the nullity of  $T (= \dim(\ker(T)) = \dim(\text{SolSpace}(A))) = 2$ .

[1 + 2 + 1 + 2 + 2 + 1 + 2 + 2 = 13 marks]

5. (a) (i)  $(-1, -2) \in W$  as  $-1 \times -2 \geq 0$  and  $(2, 1) \in W$  as  $2 \times 1 \geq 0$ .
- (ii) But  $(-1, -2) + (2, 1) = (1, -1) \notin W$  as  $1 \times -1 < 0$  so  $W$  is not closed under vector addition.
- (b) Suppose  $s_1, s_2 \in S$  (then  $As_1 = \mathbf{0}, As_2 = \mathbf{0}$ )  
 $A(s_1 + s_2) = As_1 + As_2 = \mathbf{0} + \mathbf{0} = \mathbf{0}$  so  $s_1 + s_2 \in S$ . (closed under +)  
 $A(\alpha s_1) = \alpha As_1 = \alpha \mathbf{0} = \mathbf{0}$  so  $\alpha s_1 \in S$  (closed under scalar mult.)  
 $\mathbf{0} \in S$  as  $A\mathbf{0} = \mathbf{0}$  thus  $S$  is non empty.  
 These 3 conditions mean  $S$  is a subspace of  $\mathbb{R}^3$ .
- (c) \* Consider  $\mathcal{F}$  the set of continuous functions with  $y$ -intercept 1, that is  
 $\mathcal{F} = \{f : \mathbb{R} \rightarrow \mathbb{R} : f(0) = 1 \text{ and } f \text{ continuous}\}$ .  
 This is **not** a subspace of the continuous functions  $\mathbb{R} \rightarrow \mathbb{R}$  as  $f(x) = 1$  for all  $x \in \mathbb{R}$  is a function in  $\mathcal{F}$  but  $2f$  with  $y$ -intercept 2 is not in  $\mathcal{F}$ .

6. Consider the binary code  $\mathcal{C}$  with check matrix

$$B = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

(a) Which of the words 1001101, 1000001, 0010111 are codewords?

As

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

1001101, 0010111 are codewords ( $B\mathbf{c} = \mathbf{0}$ ) and 1000001 isn't ( $B\mathbf{c} \neq \mathbf{0}$ ).

(b) The rank of  $B$  is 5.

(c) The code  $\mathcal{C}$  is the solution space of the check matrix  $B$  which by the rank-nullity theorem is  $7-5=2$ .

(d) The code  $\mathcal{C}$  has  $2^2 = 4$  codewords.

(e) The two codewords found above are linearly independent so  $\{1001101, 0010111\}$  is a basis for  $\mathcal{C}$ .

(f) The list of codewords in  $\mathcal{C}$  is 0000000, 1001101, 0010111 and 1011010 ( $=1001101+0010111$ ).

The code **can** correct 1 error.

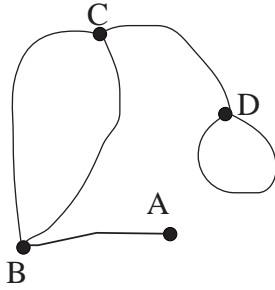
(g) 0000111  $\rightarrow$  0010111

(h) The closest codewords to 1000001 are 0000000 and 1001101 both distance 2 away – thus it is not possible to correct 2 errors.

(i) \* Yes as we cannot detect 4 errors e.g 0000000 with 4 errors may go to 1001101 in the code, thus explicitly  $\text{col1} + \text{col4} + \text{col5} + \text{col7} = \mathbf{0}$ .

[2 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1\* = 10 marks]

7. Consider the following graph.



(a) The incidence matrix  $M$  for the graph is

$$M = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 2 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

(b) The number of 4 edge paths from  $B$  to  $B$  is 29.

(c) The number of 5 edge paths from  $A$  to  $B$  is 29.

(d) \* The number of paths are equal because a 5 edge path from  $A$  to  $B$  must have the first edge from  $A$  to  $B$  and the remaining 4 edges form a 4 edge path from  $B$  to  $B$ .

[2 + 1 + 1 + 2\* = 6 marks]

8. (a) Find the line of best fit  $y = a + bx$  to the data  $(-1,6)$ ,  $(0,4)$ ,  $(1,0)$ ,  $(2,-1)$ ,  $(3,-4)$ .

$$A = \begin{bmatrix} 1 & -1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 2 \\ 1 & 3 \end{bmatrix}, \mathbf{y} = \begin{bmatrix} 6 \\ 4 \\ 0 \\ -1 \\ -4 \end{bmatrix}, A^T A = \begin{bmatrix} 5 & 5 \\ 5 & 15 \end{bmatrix}, (A^T A)^{-1} = \frac{1}{10} \begin{bmatrix} 3 & -1 \\ -1 & 1 \end{bmatrix}.$$

Also

$$A^t \mathbf{y} = \mathbf{y} = \begin{bmatrix} 5 \\ -20 \end{bmatrix} \text{ so } \begin{bmatrix} a \\ b \end{bmatrix} = (A^T A)^{-1} A^T \mathbf{y} = \frac{1}{2} \begin{bmatrix} 7 \\ -5 \end{bmatrix}.$$

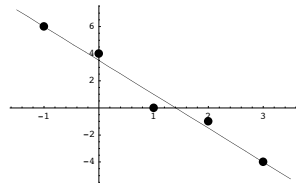
So the line of best fit is  $y = \frac{7}{2} - \frac{5}{2}x$ .

- (c) The error at  $x = 0$  has size  $|4 - \frac{7}{2}| = \frac{1}{2}$ .

- (d) For a quadratic of best fit we use

(b) 
$$A = \begin{bmatrix} 1 & -1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{bmatrix}. \quad [5 + 2 + 1 + 1 = 9 \text{ marks}]$$

Untitled-1



9. For all  $\mathbf{u} = (u_1, u_2, u_3)^T, \mathbf{v} = (v_1, v_2, v_3)^T$  in  $\mathbb{R}^3$  we define

$$\begin{aligned} \langle \mathbf{u}, \mathbf{v} \rangle &= (u_1, u_2, u_3) \begin{bmatrix} 2 & -2 & 1 \\ -2 & 2 & 1 \\ 1 & 1 & -1 \end{bmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} \\ &= \mathbf{u}^T A \mathbf{v} \\ \text{where } A &= \begin{bmatrix} 2 & -2 & 1 \\ -2 & 2 & 1 \\ 1 & 1 & -1 \end{bmatrix}. \end{aligned}$$

(a) Using  $\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u}^T A \mathbf{v}$

$$\begin{aligned} \langle \mathbf{u}, \mathbf{v} + \mathbf{w} \rangle &= \mathbf{u}^T A(\mathbf{v} + \mathbf{w}) \\ &= \mathbf{u}^T A \mathbf{v} + \mathbf{u}^T A \mathbf{w} \\ &= \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{u}, \mathbf{w} \rangle, \\ \text{and } \langle \mathbf{u}, \alpha \mathbf{v} \rangle &= \mathbf{u}^T A(\alpha \mathbf{v}) \\ &= \alpha \mathbf{u}^T A \mathbf{v} \\ &= \alpha \langle \mathbf{u}, \mathbf{v} \rangle. \end{aligned}$$

(b)  $A$  being *symmetric*  $A^T = A$  ensures  $\langle \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle$

(c)

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

Thus  $\mathbf{w} = \begin{bmatrix} 1 \\ 1 \\ -2 \end{bmatrix}$  is an *eigenvector* of  $A$  with *eigenvalue*  $-2$ .

(d)

$$\langle \mathbf{w}, \mathbf{w} \rangle = \mathbf{w}^T A \mathbf{w} = \mathbf{w}^T (-2\mathbf{w}) = -2\mathbf{w}^T \mathbf{w} = -2\|\mathbf{w}\|^2 = -12 < 0.$$

(e)  $\langle , \rangle$  is **not** an inner product as positivity fails. [3 + 1 + 2 + 1 + 1 = 8 marks]

10. (a)

$$\begin{array}{lll} \mathbf{v}_i & \mathbf{w}_i & \mathbf{u}_i \\ (1, 0, 0, 0) & \rightarrow (1, 0, 0, 0) & \rightarrow (1, 0, 0, 0) \\ (1, 1, 0, 0) & \rightarrow (0, 1, 0, 0) & \rightarrow (0, 1, 0, 0) \\ (1, 1, 1, 1) & \rightarrow (0, 0, 1, 1) & \rightarrow \frac{1}{\sqrt{2}}(0, 0, 1, 1) \end{array}$$

(Use the dot product on  $\mathbb{R}^4$  as the inner product.)

(b) You may assume the columns of

$$B = \begin{bmatrix} \frac{2}{7} & \frac{3}{7} & \frac{6}{7} \\ \frac{6}{7} & \frac{2}{7} & -\frac{3}{7} \\ \frac{3}{7} & -\frac{6}{7} & \frac{2}{7} \end{bmatrix}$$

form an orthonormal basis.

The output of the Matlab command:

`>> C = B'.B` is

$$C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

[5 + 1 = 6 marks]

11. Let  $R : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  be rotation by  $\frac{\pi}{2}$  anticlockwise about the origin and let  $S : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  be reflection in the  $x$ -axis .

(a)

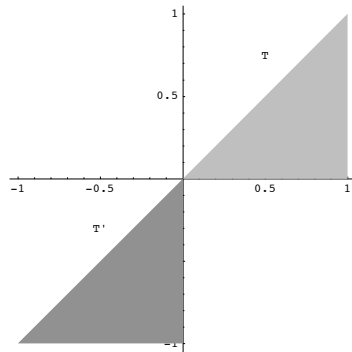
$$A_S = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad A_R = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

(b)

$$A_{S \circ R} = A_S A_R = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}.$$

Untitled-1

1



(c)

(d) A reflection about the line  $y = -x$ .

[2 + 1 + 2 + 1 = 6 marks]

12. Consider the transformation  $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  defined by

$$T\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} 1 & 2 \\ -1 & 4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

(a)  $T(\mathbf{w}) = A\mathbf{w}$  For any matrix  $A$  is a linear transformation.

Let  $\mathcal{S}$  be the standard basis for  $\mathbb{R}^2$  namely

$$\mathcal{S} = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}.$$

(b)  $[T]_{\mathcal{S} \rightarrow \mathcal{S}} = \begin{bmatrix} 1 & 2 \\ -1 & 4 \end{bmatrix}$  is the standard matrix for  $T$ .

The set

$$\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right\}$$

is another basis for  $\mathbb{R}^2$ .

(c)  $P_{\mathcal{B} \rightarrow \mathcal{S}} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$  is the transition matrix from  $\mathcal{B}$  to  $\mathcal{S}$ .

(d) The transition matrix from  $\mathcal{S}$  to  $\mathcal{B}$  is  $P_{\mathcal{S} \rightarrow \mathcal{B}} = P_{\mathcal{B} \rightarrow \mathcal{S}}^{-1} = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ .

(e)

$$P_{\mathcal{S} \rightarrow \mathcal{B}} [T]_{\mathcal{S} \rightarrow \mathcal{S}} P_{\mathcal{B} \rightarrow \mathcal{S}} = [T]_{\mathcal{B} \rightarrow \mathcal{B}}.$$

(f)

$$\begin{aligned} [T]_{\mathcal{B} \rightarrow \mathcal{B}} &= \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ -1 & 4 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \\ &= \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 3 & -1 \\ 3 & -5 \end{bmatrix} \\ &= \begin{bmatrix} 3 & -3 \\ 0 & 2 \end{bmatrix}. \end{aligned}$$

(g)

$$[T(\mathbf{v})]_{\mathcal{B}} = [T]_{\mathcal{B} \rightarrow \mathcal{B}} [\mathbf{v}]_{\mathcal{B}} = \begin{bmatrix} 3 & -3 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 4 \end{bmatrix} = \begin{bmatrix} -9 \\ 8 \end{bmatrix}.$$

[1 + 1 + 1 + 2 + 1 + 2 + 1 = 9 marks]

13. (a)

$$\begin{aligned} \left| \begin{bmatrix} 1-\lambda & 2 & 0 \\ 2 & 1-\lambda & 0 \\ 0 & 0 & 5-\lambda \end{bmatrix} \right| &= (5-\lambda) \left| \begin{bmatrix} 1-\lambda & 2 \\ 2 & 1-\lambda \end{bmatrix} \right| \\ &= (5-\lambda) ((1-\lambda)^2 - 4) \\ &= (5-\lambda)(\lambda^2 - 2\lambda - 3) \\ &= (5-\lambda)(\lambda-3)(\lambda+1) \end{aligned}$$

so the *eigenvalues* are 5, 3, -1.

(b) \*

$$\mathbf{u}_1 \cdot \mathbf{u}_2 + \mathbf{u}_2 \cdot \mathbf{u}_3 + \mathbf{u}_3 \cdot \mathbf{u}_1 = 0$$

as  $A$  is a real symmetric matrix meaning that the eigenvectors for different eigenvalues are orthogonal  $\mathbf{u}_i \cdot \mathbf{u}_j = 0$  for  $i \neq j$ .

[4 + 1\* = 5 marks]

14. (a) Show that

$$\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

are *eigenvectors* of

$$\begin{bmatrix} 1 & -1 & 1 \\ -4 & 4 & 2 \\ -2 & 2 & 4 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 6 \\ 6 \end{bmatrix} = 6 \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -1 & 1 \\ -4 & 4 & 2 \\ -2 & 2 & 4 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix} = \begin{bmatrix} 3 \\ 0 \\ 6 \end{bmatrix} = 3 \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -1 & 1 \\ -4 & 4 & 2 \\ -2 & 2 & 4 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = 0 \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

thus they are all *eigenvectors* with *eigenvalues* 6, 3, 0 respectively.

(b) (i)  $P = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}$  and (diagonal)  $D = \begin{bmatrix} 6 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{bmatrix}$  are such that so that  $D = P^{-1}AP$ .

(ii)

$$A^n = PD^nP^{-1}$$

[5 + 2 + 1 = 8 marks]

15. The eigenvalues of  $M = \begin{bmatrix} 2 & 1 & -1 \\ 1 & 3 & 2 \\ -1 & 2 & 3 \end{bmatrix}$  are 0, 3 and 5.

(a) Find an eigenvector for the eigenvalue 0.

$$\begin{bmatrix} 2 & 1 & -1 \\ 1 & 3 & 2 \\ -1 & 2 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

so an *eigenvector* is  $\begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}$ .

The vectors  $\begin{bmatrix} 2 \\ 1 \\ -1 \end{bmatrix}$  and  $\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$  are eigenvectors for 3 and 5.

Notice that the matrix  $M$  is symmetric so that there is a matrix  $P$  so that  $D = P^{-1}MP$  where  $D$  is diagonal.

(b) (i) Where

$$D = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 5 \end{bmatrix} \text{ and } P = \begin{bmatrix} 1 & 2 & 0 \\ -1 & 1 & 1 \\ 1 & -1 & 1 \end{bmatrix}.$$

(ii)

$$Q = \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{2}{\sqrt{6}} & 0 \\ -\frac{1}{\sqrt{3}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{2}} \end{bmatrix}$$

is an *orthogonal* matrix so that  $D = Q^T M Q$ .

[2 + 1 + 1 = 4 marks]