

**The University of Melbourne**  
**Semester One 2006**  
**Department of Mathematics and Statistics**  
**620-142 Mathematics B**

**Exam duration:** Three hours

**Reading time:** 15 minutes

**This paper has 9 pages.**

**The total number of marks allocated is 100.**

**Common Content:** This examination paper contains questions in common with the papers for 620-122 and 620-211.

**Authorized Materials:** No materials are authorized. Calculators and mathematical tables are not permitted. Candidates are reminded that no written or printed material related to the subject may be brought into the examination. If you have any such material in your possession, you should immediately surrender it to an invigilator.

**Instructions to Invigilators:** One 14 page script book is to be given to each student initially. Students may retain this examination paper. No written or printed material related to the subject may be brought into the examination. No mathematical tables or calculators may be used.

**Instructions to Students:** This examination consists of 13 questions. All questions may be attempted. However some question parts (indicated with \*) are harder, and it is not anticipated that all students will attempt these. Students who do attempt these are advised to complete the routine question parts first.

The number of marks for each question is indicated on the examination paper. Use of calculators is not allowed.

**Paper to be held by Baillieu Library:** This paper may be reproduced and lodged with the Baillieu Library.



1. (a) Using *Euclid's Algorithm*, calculate  $\gcd(425, 357)$ .
- (b) Working in  $\mathbb{Z}_5$ , solve  $3x = 4^3$ , giving an  $x \in \{0, 1, 2, 3, 4\}$ .
- (c) Working in  $\mathbb{Z}_3$ , write down or calculate all the solutions in  $\mathbb{Z}_3$  to

$$\begin{array}{rcl} x & + & 2z = 1 \\ y & + & z = 2. \end{array}$$

[2 + 2 + 2 = 6 marks]

2. We are implementing the **RSA public key cryptosystem** with base  $m = 7 \times 13 = 91$ .

- (a) Calculate  $n = \phi(m)$ .
- (b) If the *encryption* key  $e$  is 5, find the *decryption* key  $d$ , so that

$$a \xrightarrow{\text{encrypt}} a^e \xrightarrow{\text{decrypt}} (a^e)^d = a \text{ in } \mathbb{Z}_{91}.$$

- (c) Decrypt the 'message' 53. That is, find  $a$  so that  $a^e = 53$ . It may help knowing that  $53^2 = 79 = -12$  and  $12^2 = 53$  in  $\mathbb{Z}_{91}$ .

[1 + 4 + 3 = 8 marks]

3. (a) In  $\mathbb{Z}_{17}$  find  $b$  so that  $6^2 = b$  and  $0 \leq b \leq 16$ .
- (b) How many *multiplicative units* are there in  $\mathbb{Z}_{17}$ ?
- (c) If  $u$  is a *multiplicative unit* in  $\mathbb{Z}_{17}$ , what does *Fermat's Little Theorem* tell you about the *order* of  $u$ ?
- (d) Given that  $2^4 = 16 = -1$  write down or calculate the *order* of 2 in  $\mathbb{Z}_{17}$ .
- (e) \* Using part (a) or otherwise, write down or calculate the *order* of 6 in  $\mathbb{Z}_{17}$ . Explain briefly.

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

4. Let

$$A = \begin{bmatrix} 2 & 5 & -4 & 38 & 0 \\ -4 & -10 & 8 & -76 & 0 \\ 2 & 1 & 4 & 14 & -1 \\ 3 & 7 & -5 & 54 & 8 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & 0 & 3 & 4 & 0 \\ 0 & 1 & -2 & 6 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

In this question you may assume that the matrix  $B$  is obtained from the matrix  $A$  by applying elementary row operations. Using this information, or otherwise, answer the following:

- (a) What is the rank of  $A$ ?
- (b) Write down a basis for the *column space* of  $A$ .
- (c) Write down a basis for the *row space* of  $A$ .
- (d) Are the rows of  $A$  linearly independent? Explain your answer.
- (e) Do the vectors  $(2, -4, 2, 3)$ ,  $(5, -10, 1, 7)$ ,  $(-4, 8, 4, -5)$ ,  $(38, -76, 14, 54)$ ,  $(0, 0, -1, 8)$  span  $\mathbb{R}^4$ ? Give a reason.
- (f) Write  $(-4, 8, 4, -5)$  as a linear combination of  $(2, -4, 2, 3)$  and  $(5, -10, 1, 7)$ .
- (g) Let  $T : \mathbb{R}^5 \rightarrow \mathbb{R}^4$  be the linear transformation with standard matrix  $A$ . Write down the rank of  $T$  ( $=\dim(\text{Im}(T))$ ) and the nullity of  $T$  ( $=\dim(\ker(T))$ ).  
[1 + 2 + 1 + 2 + 2 + 1 + 2 = 11 marks]

5. (a) Let  $V = \{(x, y) \in \mathbb{R}^2 : x \times y = 0\}$  be the *union* of the  $x$  and  $y$  axes of the Cartesian plane.

Show that  $V$  is NOT a *subspace* of  $\mathbb{R}^2$ .

(b) Let  $W$  be the span of the set

$$\mathcal{B} = \{(2, 2, 1, 0), (-2, 2, 0, 1)\}.$$

- (i) Using the *dot product* and using the *Gram Schmidt algorithm* on  $\mathcal{B}$  or otherwise, find an *orthonormal basis*  $\mathcal{U} = \{\mathbf{u}_1, \mathbf{u}_2\}$  for  $W$ .
- (ii) Find  $\mathbf{p} = \text{Proj}_W(\mathbf{v})$ , the *orthogonal projection* of  $\mathbf{v} = (3, 6, 0, 3)$  onto the *subspace*  $W$ .
- (iii) Hence or otherwise, find an *orthonormal basis* for  $W' = \langle\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{v}\}\rangle$  (the *span* of  $\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{v}\}$ ).

[2 + 2 + 2 + 2 = 8 marks]

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

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

- (a) Which of the words 101110101, 100100100, 011101110, 000000001 are codewords? Justify your answer (the calculations below may help).

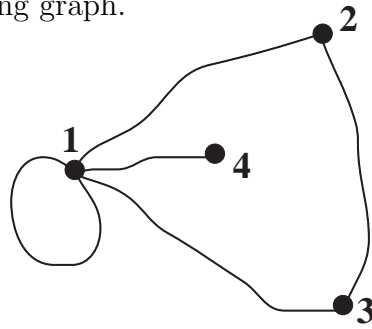
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix}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

- (b) Using the *rank/nullity theorem* prove that the dimension of the code  $\mathcal{C}$  is 2.  
(c) How many codewords does the code  $\mathcal{C}$  have?  
(d) Using part (a) or otherwise, write down a basis for the code.  
(e) Hence write down all codewords for the code  $\mathcal{C}$ .  
(f) What is the *minimum distance* of the code  $\mathcal{C}$ ?  
(g) Write down the number of errors the code  $\mathcal{C}$  can:  
(i) *correct*;  
(ii) *detect*.  
(h) Correct the following words (using *nearest neighbour decoding*) to codewords in  $\mathcal{C}$ .  
(i) 000000001.  
(ii) 111101111.

- (i) \* Can the code  $\mathcal{C}$  correct all words? Explain.

[2 + 1 + 1 + 1 + 1 + 1 + 1 + 2 + 2 + 1\* = 12 marks]

7. Consider the following graph.



- (a) Write down the incidence matrix  $M$  for the graph, adopting the convention that row/col 1, row/col 2, row/col 3, row/col 4 correspond to vertices 1, 2, 3, 4 respectively.

It can be checked that

$$M^2 = \begin{bmatrix} 4 & 2 & 2 & 1 \\ 2 & 2 & 1 & 1 \\ 2 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \quad M^3 = \begin{bmatrix} 9 & 6 & 6 & 4 \\ 6 & 3 & 4 & 2 \\ 6 & 4 & 3 & 2 \\ 4 & 2 & 2 & 1 \end{bmatrix}.$$

- (b) Hence, write down the number of 3 edge paths from 1 to 2.
- (c) Write down or calculate the number of 5 edge paths from 4 to 4.  
[2 + 1 + 1 = 4 marks]
8. (a) Find the line of best fit  $y = a + bx$  to the data  $(-3, -1), (0, -1), (1, 1), (2, 5)$ .
- (b) Sketch the line of best fit and include the data points on your graph.
- (c) Suppose you now try to fit a quadratic  $y = a + bx + cx^2$  to the data. Write down the matrix  $A$  you would use in the formula

$$A^T A \bar{\mathbf{u}} = A^T \mathbf{y}$$

to solve the least squares problem. **Do not try to solve the problem.**

[4 + 1 + 1 = 6 marks]

9. (a) Show that the following formulas DO NOT define *inner products* on  $\mathbb{R}^2$  :

(i)  $\langle(u_1, u_2), (v_1, v_2)\rangle = u_1v_1 + u_1v_2$ ;

(ii) \*  $\langle(u_1, u_2), (v_1, v_2)\rangle = 3u_1v_1 - u_1v_2 - u_2v_1$ .

(b) (i) For column vectors  $\mathbf{a}$  and  $\mathbf{b}$  in  $\mathbb{R}^2$ , define

$$\langle \mathbf{a}, \mathbf{b} \rangle = \mathbf{a}^T A \mathbf{b} \text{ where } A = \begin{bmatrix} 2 & 0 \\ 0 & \frac{2}{3} \end{bmatrix},$$

or equivalently,  $\langle(a_1, a_2), (b_1, b_2)\rangle = 2a_1b_1 + \frac{2}{3}a_2b_2$ .

Prove that  $\langle \cdot, \cdot \rangle$  DOES define an *inner product* on  $\mathbb{R}^2$ , by checking the inner product *axioms*.

(ii) Use this *inner product* to find

$\|(1, 2)\|$  and  $\langle(1, 2), (2, -3)\rangle$ . [1 + 1\* + 3 + 2 = 7 marks]

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

(i) Write down the standard matrix representations for  $S$  and  $R$ .

(ii) Use part (i) to find the standard matrix representation for  $R \circ S$  ( $S$  followed by  $R$ ).

(iii) Draw the triangle  $T$  with corners at  $(0, 0)$ ,  $(1, 0)$ ,  $(1, 1)$  in the  $xy$ -plane and on the same set of axes draw the image of this triangle  $T'$  after applying  $R \circ S$ .

(b) Consider the *symmetric* matrix

$$A = \begin{bmatrix} -\frac{4}{5} & \frac{3}{5} \\ \frac{3}{5} & \frac{4}{5} \end{bmatrix}.$$

(i) Find the *eigenvalues* of  $A$ .

(ii) Find the corresponding *eigenvectors* of  $A$ .

(iii) \* Describe geometrically the *linear transformation*  $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  given by

$$T \left( \begin{bmatrix} x \\ y \end{bmatrix} \right) = A \begin{bmatrix} x \\ y \end{bmatrix}.$$

Hint: think about the action of  $T$  on a *canonical basis*.

[(2 + 1 + 1) + (2 + 2 + 1\*) = 9 marks]

11. (a) Show that

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

are *eigenvectors* of

$$A = \begin{bmatrix} -2 & -8 & -2 \\ -8 & 4 & 10 \\ -2 & 10 & 7 \end{bmatrix}$$

and find their associated *eigenvalues*.

(b) Using part (a) or otherwise write down an invertible matrix  $P$  and a diagonal matrix  $D$  so that

$$D = P^{-1}AP.$$

(c) Write down an *orthogonal matrix*  $Q$  such that

$$D = Q^T A Q.$$

(d) For column vectors  $\mathbf{u}$  and  $\mathbf{v}$  in  $\mathbb{R}^3$ , define  $\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u}^T A \mathbf{v}$ .

Is this an *inner product* on  $\mathbb{R}^3$ ? Explain briefly.

(e) We define a *quadratic form*  $F : \mathbb{R}^3 \rightarrow \mathbb{R}$  by

$$F(\mathbf{x}) = \mathbf{x}^T A \mathbf{x},$$

for column vectors  $\mathbf{x} \in \mathbb{R}^3$ .

Which ONE of the following *quadratic forms* is  $F$  equivalent to?

(i)  $x^2 + y^2 + z^2$ ;

(ii)  $x^2 + y^2 - z^2$ ;

(iii)  $x^2 - y^2 - z^2$ ;

(iv)  $x^2 + y^2$ ;

(v)  $x^2 - y^2$ .

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

12. Consider the transformation  $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  defined by  $T(\mathbf{x}) = A\mathbf{x}$  where  $A = \begin{bmatrix} 8 & -3 \\ 18 & -7 \end{bmatrix}$ , that is

$$T\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} 8 & -3 \\ 18 & -7 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

Let  $\mathcal{S}$  and  $\mathcal{B}$  be the following bases for  $\mathbb{R}^2$  :

$$\mathcal{S} = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}, \quad \mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 3 \end{bmatrix} \right\}.$$

- Write down  $[T]_{\mathcal{S} \rightarrow \mathcal{S}}$ , the *standard matrix* for  $T$ .
- Write down the *transition matrix*  $P_{\mathcal{B} \rightarrow \mathcal{S}}$  from  $\mathcal{B}$  to  $\mathcal{S}$ .
- Calculate the *transition matrix*  $P_{\mathcal{S} \rightarrow \mathcal{B}}$  from  $\mathcal{S}$  to  $\mathcal{B}$ .
- Find  $[T]_{\mathcal{B} \rightarrow \mathcal{B}}$ .
- If  $\mathbf{w} = 3 \begin{bmatrix} 1 \\ 2 \end{bmatrix} - 4 \begin{bmatrix} 1 \\ 3 \end{bmatrix}$  find  $[T(\mathbf{w})]_{\mathcal{B}}$ .

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

13. Let  $M^{2,2}$  be the real *vector space* of all real  $2 \times 2$  matrices.

For a fixed  $2 \times 2$  matrix  $A$ , define a function  $T : M^{2,2} \rightarrow M^{2,2}$  by

$$T(X) = AX - XA.$$

- \* Prove that  $T$  is a *linear transformation*.
- Now fix  $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ , and use the *standard basis* for  $M^{2,2}$ ,

$$\mathcal{S} = \{E_1, E_2, E_3, E_4\} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right\}.$$

- Verify that  $T(E_1) = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$ .
- Given, in addition, that

$$T(E_2) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, T(E_3) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, T(E_4) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

find the *coordinate vectors*, with respect to  $\mathcal{S}$ , of the images of the basis vectors in  $\mathcal{S}$ . That is, find  $[T(E_i)]_{\mathcal{S}}$  for  $i = 1, \dots, 4$ .

- Hence find the *standard basis*  $[T]_{\mathcal{S} \rightarrow \mathcal{S}}$  of  $T$ .
- \* Find *bases* for the *image* and *kernel* of  $T$  when  $A$  is defined as above.
- \* If we define  $T$  using any non-zero matrix  $A$ , prove that the linear transformation  $T$  never has a 4-dimensional *image*.

[2\*+1+1+1+2\*+1\* = 8 marks]