

**The University of Melbourne**  
**Department of Mathematics and Statistics**  
**620-142 Mathematics B**  
**Semester One, 2007**

**This paper has 8 pages.**

**The total number of marks allocated is 120.**

**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 15 questions. All questions may be attempted.

The number of marks for each question is indicated on the examination paper. The total number of marks is 120. 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* show that

$$\gcd(1033, 100) = 1.$$

- (b) Using your working in (a) above (or otherwise) find the multiplicative inverse of 100 in  $\mathbb{Z}_{1033}$ .
- (c) In  $\mathbb{Z}_{1033}$  solve for  $x$ :  $100x = -3$ .
- (d) What can be said about the existence of a multiplicative inverse of 15 in  $\mathbb{Z}_{85}$ ? [8 marks]

2. Suppose the matrix  $A$  has eigenvector  $\mathbf{u}$  with eigenvalue  $\lambda$  that is

$$A\mathbf{u} = \lambda\mathbf{u}.$$

Using **mathematical induction** prove that  $A^n$  has eigenvector  $\mathbf{u}$  with eigenvalue  $\lambda^n$  that is

$$A^n\mathbf{u} = \lambda^n\mathbf{u}$$

for all integers  $n \geq 1$ .

[6 marks]

3. In this question, the RSA public key cryptosystem is being implemented with base  $m = 3 \times 29 = 87$ .

Knowing  $62 = -25$ ,  $16^2 = 82$ ,  $82^2 = 25$  and  $25^2 = 16$  in  $\mathbb{Z}_{87}$  may help arithmetically.

- (a) Calculate  $n = \phi(m)$ .
- (b) Using the encryption key  $e = 11$ , encrypt the message '16'.
- (c) With brief justification, decide which one of the following is an appropriate decrypting key (for  $e = 11$ ):  $d = 51$  or  $d = 8$ .
- (d) Using this decrypting key, decrypt the message '62'.

[9 marks]

4. In a 'real' implementation of the RSA public key cryptosystem  $M = pq$  where  $p$  and  $q$  are distinct primes of about 200 digits.

Explain why the decryption key  $d$  is effectively secure even if the base  $M$  and the encryption key  $e$  are made public.

[2 marks]

5. In  $\mathbb{Z}_{26}$  arithmetic, it is true that  $3^6 = 1$  and  $5^2 = 25 = -1$  (you need not show this).

(a) Find the order of the unit 3.

(b) The order of the unit 5 is 4 (you do not need to show this).

Using the order of 3 and 5 (or otherwise) show that  $15 = 3 \times 5$  is a primitive unit in  $\mathbb{Z}_{26}$ .

(c) Using an appropriate theorem (or otherwise), explain why in  $\mathbb{Z}_{26}$  arithmetic,  $a^{13} = a$  for any  $a$ .

[6 marks]

6. Let

$$A = \begin{bmatrix} 1 & -2 & 3 & 1 & 5 \\ -2 & 4 & -6 & -2 & -10 \\ 1 & 3 & -2 & 1 & 5 \\ 2 & -7 & 9 & 0 & 2 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

In this question you may assume the fact 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 (or calculate) the dimension of the row space of  $A$ .

(d) Are the rows of  $A$  linearly independent? Explain your answer.

(e) Write down a basis for the row space of  $A$ .

(f) Do the vectors  $(1, -2, 1, 2)$ ,  $(-2, 4, 3, -7)$ ,  $(3, -6, -2, 9)$ ,  $(1, -2, 1, 0)$ ,  $(5, -10, 5, 2)$  span  $\mathbb{R}^4$ ? Give a reason.

(g) Write  $(3, -6, -2, 9)$  as a linear combination of  $(1, -2, 1, 2)$  and  $(-2, 4, 3, -7)$ .

(h) Find a basis for the solution space of  $A$ .

(i) Write down a basis for the kernel of the linear transformation  $T : \mathbb{R}^5 \rightarrow \mathbb{R}^4$ , defined by  $T(\mathbf{x}) = A\mathbf{x}$ .

[12 marks]

7. (a) Let

$$P = \{(x, y, z) : x + y + z \leq 0\} \subset \mathbb{R}^3.$$

Show that  $P$  is NOT a subspace of  $\mathbb{R}^3$ .

(b) Let

$$T : \mathbb{R}^5 \rightarrow \mathbb{R}^4$$

be a linear transformation.

Suppose that  $T(\mathbf{u}) = \mathbf{u}'$ ,  $T(\mathbf{v}) = \mathbf{v}'$ .

(i) Write  $T(\mathbf{u} + \mathbf{v})$  and  $T(\alpha\mathbf{u})$  as linear combinations of  $\mathbf{u}'$  and  $\mathbf{v}'$ .

(ii) Give the definition of the kernel of  $T$  by completing the following (or otherwise)

$$\text{Ker}(T) = \{\mathbf{w} \in \mathbb{R}^5 : \dots\dots\dots\}.$$

(iii) Prove that  $\text{Ker}(T)$  is a subspace of  $\mathbb{R}^5$ .

[9 marks]

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

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

(a) Which of the words 1000000, 0001011, 0001111 are codewords? Justify your answer (the calculations below may help).

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

(b) The dimension of  $\mathcal{C}$  is 3. How many codewords does the code  $\mathcal{C}$  have?

(c) The minimum distance of the code is 4.

How many errors can the code  $\mathcal{C}$ :

(i) correct;

(ii) detect.

(d) Correct (if possible) any one of the words 1000000, 0001011, 0001111 that is not a codeword.

(e) Prove (using the rank/nullity theorem or otherwise) that the dimension of  $\mathcal{C}$  is 3.

(f) The received word 1100000 has syndrome  $1100^T$ . Explain why this word has at least 2 errors.

[10 marks]

9. (a) (i) Find the line of best fit  $y = a + bx$  to the five data points

$$\begin{array}{c|ccccc} \mathbf{x} & -4 & -2 & 1 & 2 & 3 \\ \hline \mathbf{y} & 5 & 5 & 2 & 0 & -2 \end{array}$$

- (ii) What is the least squares error in approximating the data given by the line of best fit?
- (b) 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.**

[8 marks]

10. (a) The formula

$$\langle \mathbf{x}_1, \mathbf{x}_2 \rangle = \langle (x_1, y_1), (x_2, y_2) \rangle = x_1 x_2 - x_2 y_1 - y_2 x_1 + 3y_1 y_2$$

does define an inner product on  $\mathbb{R}^2$ .

- (i) Write down all the properties  $\langle \cdot, \cdot \rangle$  must satisfy (to be an inner product on  $\mathbb{R}^2$ ).
- (ii) Use this inner product to find

$$\|(3, 2)\| \text{ and } \langle (3, 2), (-3, 1) \rangle.$$

- (b) Show (by exhibiting an inner product property that fails) that the following formula DOES NOT define an inner product on  $\mathbb{R}^2$  :

$$\langle (x_1, y_1), (x_2, y_2) \rangle = x_1 y_2 + x_2 y_1.$$

[8 marks]

11. In this question the inner product space is  $\mathbb{R}^4$  with the standard Euclidean inner product (that is the dot product).

- (a) Show the the set  $\{\mathbf{u}_1, \mathbf{u}_2\} = \left\{ \frac{1}{3}(-2, 2, 1, 0), \frac{1}{3}(2, 2, 0, 1) \right\}$  is an orthonormal set.

- (b) Using the Gram Schmidt algorithm or otherwise find an orthonormal basis

$$\mathcal{U} = \{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\} \text{ for } \left\langle \left\{ \frac{1}{3}(-2, 2, 1, 0), \frac{1}{3}(2, 2, 0, 1), (-2, 5, 4, 3) \right\} \right\rangle,$$

the span of  $\mathbf{u}_1 = \frac{1}{3}(-2, 2, 1, 0)$ ,  $\mathbf{u}_2 = \frac{1}{3}(2, 2, 0, 1)$  and  $\mathbf{v} = (-2, 5, 4, 3)$ .

- (c) Express  $(0, 3, 3, 3)$  as a linear combination of the basis ( $\mathcal{U}$ ) vectors  $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ .

[7 marks]

12. Let  $S : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  and  $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  be shears along the  $x$ -axis and  $y$ -axis respectively given by

$$S \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & -4 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \text{ and } T \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

- (a) Calculate the standard matrix representation for  $S \circ T$  ( $T$  followed by  $S$ ).
- (b) Find the image with respect to  $S \circ T$  of the vector  $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ .
- (c) Where does the line  $y = x$  get mapped to by  $S \circ T$ ?

Note that

$$\left\{ \begin{bmatrix} x \\ y \end{bmatrix} : y = x \right\} = \left\langle \left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\} \right\rangle$$

[5 marks]

13. Consider the transformation  $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  defined by  $T(\mathbf{x}) = A\mathbf{x}$  where  $A = \begin{bmatrix} 3 & 4 \\ -2 & -3 \end{bmatrix}$ , that is

$$T \left( \begin{bmatrix} x \\ y \end{bmatrix} \right) = \begin{bmatrix} 3 & 4 \\ -2 & -3 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

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

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

- (a) Write down  $[T]_{\mathcal{S} \rightarrow \mathcal{S}}$ , the *standard matrix* for  $T$ .
- (b) Write down the *transition matrix*  $P_{\mathcal{B} \rightarrow \mathcal{S}}$  from  $\mathcal{B}$  to  $\mathcal{S}$ .
- (c) Calculate the *transition matrix*  $P_{\mathcal{S} \rightarrow \mathcal{B}}$  from  $\mathcal{S}$  to  $\mathcal{B}$ .
- (d) Using  $P_{\mathcal{S} \rightarrow \mathcal{B}}$  or otherwise express  $\mathbf{w} = \begin{bmatrix} -7 \\ 11 \end{bmatrix}$  as a linear combination of the vectors in the basis  $\mathcal{B}$ .
- (e) Find  $[T]_{\mathcal{B} \rightarrow \mathcal{B}}$ .
- (f) Find  $[T(\mathbf{w})]_{\mathcal{B}}$ .

[11 marks]

14. Find the *eigenvalues* and *eigenvectors* of the matrix

$$A = \begin{bmatrix} 5 & 6 \\ -3 & -4 \end{bmatrix}.$$

[7 marks]

15. (a) Verify that the vectors

$$\mathbf{v}_1 = \begin{bmatrix} 2 \\ 2 \\ -1 \end{bmatrix}, \mathbf{v}_2 = \begin{bmatrix} 2 \\ -1 \\ 2 \end{bmatrix}, \mathbf{v}_3 = \begin{bmatrix} -1 \\ 2 \\ 2 \end{bmatrix}$$

are *eigenvectors* of the matrix

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

and find their associated *eigenvalues*.

- (b) Hence 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  $Q$  so that

$$D = Q^T A Q$$

(where  $D$  is the diagonal matrix above).

- (d) Comment briefly on the special features of  $A$  and the eigenvectors  $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$  that facilitate such a quick calculation of an *orthogonal* matrix  $Q$ .
- (e) Does  $\langle \mathbf{u}, \mathbf{w} \rangle = \mathbf{u}^T A \mathbf{w}$  define an inner product on  $\mathbb{R}^3$ ? Explain briefly why or why not.

[12 marks]