

1. *Solution.*

(a)

$$\begin{aligned}28 &= 2 \times 11 + 6 \\11 &= 1 \times 6 + 5 \\6 &= 1 \times 5 + 1 \\5 &= 5 \times 1\end{aligned}$$

(b)

$$\begin{aligned}1 &= 6 - 1 \times 5 \\&= 6 - 1 \times (11 - 6) \\&= 2 \times 6 - 1 \times 11 \\&= 2 \times (28 - 2 \times 11) - 1 \times 11 \\&= 2 \times 28 - 5 \times 11\end{aligned}$$

So in \mathbb{Z}_{28} $1 = 2 \times 28 - 5 \times 11 = 0 - 5 \times 11$ thus $11^{-1} = -5 = 23$ in \mathbb{Z}_{28} .

(c) $11x = 3 \Rightarrow 23 \times 11x = 23 \times 3 \Rightarrow x = 69 = 69 - 2 \times 28 = 13$ in \mathbb{Z}_{28} .

Let's check $11 \times 13 = 143 = 143 - 5 \times 28 = 143 - 140 = 3!$

(d) The multiplicative inverse of 7 in \mathbb{Z}_{77} does not exist as $\gcd(7, 77) = 7 \neq 1!$

2. *Solution.* Let \mathcal{P}_n be the proposition that $A^n \mathbf{u} = \lambda^n \mathbf{u}$ where n is a positive integer.

(base case $n = 1$) this case is true as $A\mathbf{u} = \lambda\mathbf{u} \Leftrightarrow A^1\mathbf{u} = \lambda^1\mathbf{u}$.

(the inductive step) We assume that \mathcal{P}_k is true:

$$\begin{aligned}A^k \mathbf{v} &= \lambda^k \mathbf{v} \text{ So,} \\A^{k+1} \mathbf{v} &= A(A^k \mathbf{v}) \\&= A(\lambda^k \mathbf{v}) \\&= (\lambda^k) [A\mathbf{v}] \\&= (\lambda^k) [\lambda \mathbf{v}] \\&= \lambda^{k+1} \mathbf{v}\end{aligned}$$

So we have $A^{k+1} \mathbf{v} = \lambda^{k+1} \mathbf{v}$ which is \mathcal{P}_{k+1} . Thus $\mathcal{P}_k \Rightarrow \mathcal{P}_{k+1}$ and so by the PRINCIPLE OF MATHEMATICAL INDUCTION \mathcal{P}_n is true for all integral $n \geq 1$, that is $A^n \mathbf{u} = \lambda^n \mathbf{u}$ for all integers $n \geq 1$.

3. *Solution.*

- (a) Calculate $n = \phi(m) = \phi(2 \times 29) = (2 - 1) \times (29 - 1) = 1 \times 28 = 28$.
- (b) If the encryption key e is 23 the decryption key d will be e^{-1} in \mathbb{Z}_{28} which is 11 from question 1.
- (c) We need $51^{11} = (-7)^{11} = -7^{11}$.

$$\begin{array}{r} 7 \quad \underline{11} \quad 7 \\ \quad \underline{5} \quad 7^2 = 49 \\ \quad \quad \underline{2} \quad 49^2 = 23 \\ \quad \quad \quad \underline{1} \quad 23^2 = 7 \end{array}$$

So $-7^{11} = -7 \times 49 \times 7 = -49^2 = -23 = 35$ that is 51 decrypts as 35.

4. *Solution.*

In an implementation of the RSA public key cryptosystem:

- (a) To encrypt we calculate a^e in \mathbb{Z}_m and to decrypt we calculate a^d in \mathbb{Z}_m .
- (b) The base m must be the product of distinct primes. $n = \phi(m)$ and e and d are inverses in \mathbb{Z}_n .
- (c) To find d we need to know e^{-1} in \mathbb{Z}_n hence we need to know $n = (p - 1) \times (q - 1)$ and to calculate this we need to know the prime factorization of $m = pq$. With current technologies and algorithms this is impracticable (may take more than a lifetime) if p and q are both about 200 digits .

[6 marks]

5. *Solution.*

- (a) The rank of A is 3 (the number of row leaders in $\text{RREF}(A)$).
- (b) B has row leaders in columns 1, 2 and 4 thus a basis for the column space of A consists of the first, second and fourth columns of A that is $\{[1 \ 2 \ -1 \ 3]^T, [3 \ 5 \ -2 \ -2]^T, [0 \ -1 \ 1 \ 1]^T\}$. Please note the first 3 columns of A do not form a basis as they are not linearly independent.
- (c) The dimension of the row space of A is 3 (the rank of A).
- (d) There are 4 rows of A which cannot be linearly independent in a dimension 3 space.
- (e) The non-zero rows of B form a basis for the row space of A that is $\{[1 \ 0 \ 26 \ 0 \ -6], [0 \ 1 \ -9 \ 0 \ 10], [0 \ 0 \ 0 \ 1 \ 38]\}$ are a basis. Note that the first 3 rows of A are NOT linearly independent (row3=row1-row2) rows 1, 2, 4 of A would form a basis for the row space though.
- (f) The vectors $(1, 2, -1, 3), (3, 5, -2, -2), (-1, 7, -8, 96), (0, -1, 1, 1), (24, 0, 24, 0)$ are the columns of A and these only span a dimension 3 space (the column space of A) thus they DO NOT span \mathbb{R}^4 .
- (g) By interpreting B in particular the third column we see that (the third column of A) $(-1, 7, -8, 96) = 26(1, 2, -1, 3) - 9(3, 5, -2, -2)$ (a linear combination of the first 2 columns of A)
- (h) If $A\mathbf{v} = \mathbf{0}$ where $\mathbf{v}^T = [v_1 \ v_2 \ v_3 \ v_4 \ v_5]$ from $B=\text{rref}(A)$ we see that v_3 and v_5 are free variables and from row 3 of B $v_4 = -38v_5$ and from row 2 (of B) $v_2 = 9v_3 - 10v_5$ and from row 1 (of B) $v_1 = -26v_3 + 6v_5$ so

$$\begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{bmatrix} = \begin{bmatrix} -26v_3 + 6v_5 \\ 9v_3 - 10v_5 \\ v_3 \\ -38v_5 \\ v_5 \end{bmatrix} = \begin{bmatrix} -26v_3 \\ 9v_3 \\ v_3 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 6v_5 \\ -10v_5 \\ 0 \\ -38v_5 \\ v_5 \end{bmatrix} = v_3 \begin{bmatrix} -26 \\ 9 \\ 1 \\ 0 \\ 0 \end{bmatrix} + v_5 \begin{bmatrix} 6 \\ -10 \\ 0 \\ -38 \\ 1 \end{bmatrix}.$$

So a basis for the solution space of A is $\left\{ \begin{bmatrix} -26 \\ 9 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 6 \\ -10 \\ 0 \\ -38 \\ 1 \end{bmatrix} \right\}$.

- (i) $5 = 3 + 2$ the number of columns of A is equal to the rank of A + the nullity of A .

6. *Solution.*

Subspace Theorem

IF $W \subseteq \mathbb{R}^n$ satisfies

- (a) **1** W is non empty.
2 $\mathbf{u}, \mathbf{v} \in W \Rightarrow (\mathbf{u} + \mathbf{v}) \in W$
3 $\alpha \in \mathbb{R}, \mathbf{u} \in W \Rightarrow \alpha\mathbf{u} \in W$

THEN

W is a subspace of \mathbb{R}^n .

(b) Let

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

$(-1, -1, -1) \in P$ as $(-1)+(-1)+(-1) = -3 \leq 0$ but $(-1)(-1, -1, -1) = (1, 1, 1) \notin P$ as $1 + 1 + 1 \not\leq 0$ thus P is not closed under scalar multiplication and so is NOT a subspace of \mathbb{R}^3 .

(c)

$$\text{SolutionSpace}(A) = \{\mathbf{u} : A\mathbf{u} = \mathbf{0}\}.$$

(d) Let $\mathbf{0}$ be the zero vector in \mathbb{R}^n it is true that $A\mathbf{0} = \mathbf{0}$ (where the zero on the RHS is in \mathbb{R}^m) thus $\text{SolutionSpace}(A)$ is non empty.

Suppose \mathbf{u} and \mathbf{v} are both in $\text{SolutionSpace}(A)$ then $A\mathbf{u} = \mathbf{0}$ and $A\mathbf{v} = \mathbf{0}$ so $A(\mathbf{u} + \mathbf{v}) = A\mathbf{u} + A\mathbf{v} = \mathbf{0} + \mathbf{0} = \mathbf{0}$ thus $\mathbf{u} + \mathbf{v}$ is in $\text{SolutionSpace}(A)$. So $\text{SolutionSpace}(A)$ is closed under addition.

Suppose $\mathbf{u} \in \text{SolutionSpace}(A)$ and $\alpha \in \mathbb{R}$ then $A(\alpha\mathbf{u}) = \alpha(A\mathbf{u}) = \alpha\mathbf{0} = \mathbf{0}$ thus $\alpha(\mathbf{u}) \in \text{SolutionSpace}(A)$ so $\text{SolutionSpace}(A)$ is closed under scalar multiplication.

Thus by the subspace theorem (we have established **1**, **2**, **3**) the $\text{SolutionSpace}(A)$ is a subspace of \mathbb{R}^n .

7. *Solution.* Consider the binary linear code \mathcal{C} with codewords $\{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\} = \{00000000, 101101101, 010110111, 111011010\}$,

- (a) Using nearest neighbour decoding, correct the words:
 - (i) $001101101 \rightarrow 101101101$ (distance 1 away by changing the first bit);
 - (ii) 001011010 is distance 4 from \mathbf{c}_1 is distance 6 from \mathbf{c}_2 is distance 6 from \mathbf{c}_3 and is distance 2 from \mathbf{c}_4 thus $001011010 \rightarrow 111011010$ (corrects to \mathbf{c}_4).
- (b) As the code \mathcal{C} is linear the minimum distance of the code is the minimum weight amongst the non-zero words which by inspection is 6.
- (c) The code \mathcal{C} can:
 - (i) correct 2 errors;
 - (i) detect 5 errors.
- (d) The dimension of the code \mathcal{C} is 2 as there are 4 codewords and $|\mathbb{Z}_2|^2 = 4$.
- (e) The set $\{101101101, 010110111\}$ is linearly independent (consider the first two bits 10 and 01 are not linearly dependent) and as the code has dimension 2, 2 linearly independent vectors **in** \mathcal{C} form a basis for the code \mathcal{C} .
- (f) H has rank 8 (as it is in RREF form) so by the Rank-Nullity theorem the solution space to H has dimension 2. Now both the vectors in the basis for \mathcal{C} above are in the solution Space for H (as seen in the MatLab output) thus $\mathcal{C} \subseteq \text{SolutionSpace}(\mathcal{H})$ but as $\text{SolutionSpace}(H)$ and \mathcal{C} have the same dimension (2), $\mathcal{C} = \text{SolutionSpace}(\mathcal{H})$. This is equivalent to H being a check matrix for the code \mathcal{C} .

8. *Solution.*

(a)

$$A = \begin{bmatrix} 1 & -3 \\ 1 & -2 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}, \mathbf{y} = \begin{bmatrix} 9 \\ -7 \\ 3 \\ 1 \end{bmatrix}, A^T A = \begin{bmatrix} 4 & -4 \\ -4 & 14 \end{bmatrix}, A^T \mathbf{y} = \begin{bmatrix} 4 \\ -14 \end{bmatrix}$$

So solving $A^T A \bar{\mathbf{u}} = A^T \mathbf{y}$ for $\bar{\mathbf{u}}$ as follows

$$\left[\begin{array}{cc|c} 4 & -4 & 4 \\ -4 & 14 & -14 \end{array} \right] \sim \left[\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & -1 \end{array} \right]$$

so $a = 0$ and $b = -1$ Thus the line of best fit is $y = -x$.

(b)

$$A = \begin{bmatrix} 1 & -3 & 9 \\ 1 & -2 & 4 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix}.$$

(c) We would expect a least squares error of 0 as it is possible to find a cubic going through these 4 (or any 4 points) points.

9. *Solution.*

(a) (i) $\langle \cdot, \cdot \rangle$ must satisfy

- $\langle \mathbf{u}, \mathbf{w} \rangle = \langle \mathbf{w}, \mathbf{u} \rangle$ for all \mathbf{u} and \mathbf{w} .
- $\langle \mathbf{u}, \mathbf{w} + \mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{w} \rangle + \langle \mathbf{u}, \mathbf{v} \rangle$ for all \mathbf{u}, \mathbf{w} and \mathbf{v} .
- $\langle \mathbf{u}, \alpha \mathbf{w} \rangle = \alpha \langle \mathbf{u}, \mathbf{w} \rangle$ for all \mathbf{u}, \mathbf{w} and $\alpha \in \mathbb{R}$.
- $\langle \mathbf{u}, \mathbf{u} \rangle \geq 0$ for all \mathbf{u} .
- $\langle \mathbf{u}, \mathbf{u} \rangle = 0 \Rightarrow \mathbf{u} = \mathbf{0}$.

(ii) Use this inner product to find

$$\|(1, -2)\| = (\langle (1, -2), (1, -2) \rangle)^{1/2} = (5 \times 1^2 + 4 \times 1 \times -2 + 4 \times -2 \times 1 + 5 \times (-2)^2)^{1/2} = \sqrt{5 - 16 + 20} = 3.$$

$$\langle (1, -2), (-2, 1) \rangle = (5 \times 1 \times (-2) + 4 \times (-2) \times (-2) + 4 \times 1 \times 1 + 5 \times -2 \times 1) = -10 + 16 + 4 - 10 = 0.$$

(b) Let us suppose that the following formula

$$\langle (u_1, u_2), (v_1, v_2) \rangle = u_1 v_1 - 3u_1 v_2 - 3u_2 v_1 + u_2 v_2$$

defines an inner product on \mathbb{R}^2 .

(i) $\|(1, 1)\|^2 = \langle (1, 1), (1, 1) \rangle = 1^2 - 3 \times 1^2 - 3 \times 1^2 + 1^2 = -4.$

(ii) The formula does not form an inner product as $\langle (1, 1), (1, 1) \rangle = -4 < 0$ violating positive definiteness which means the length of $(1, 1) = \|(1, 1)\| = \sqrt{-4}$ is not a real number.

10. *Solution.* Let W is the span of the set $\mathcal{B} = \{(-2, 2, 1, 0), (-1, -2, 2, 0)\}$.

$$(a) \mathbf{u}_1 = \frac{1}{\|\mathbf{b}_1\|} \mathbf{b}_1 = \frac{1}{3}(-2, 2, 1, 0)$$

$$\begin{aligned} \mathbf{w}_2 &= \mathbf{b}_2 - ((\mathbf{b}_2 \cdot \mathbf{u}_1) \mathbf{u}_1) \\ &= (-1, -2, 2, 0) - \left((-1, -2, 2, 0) \cdot \frac{1}{3}(-2, 2, 1, 0) \right) \frac{1}{3}(-2, 2, 1, 0) \\ &= (-1, -2, 2, 0) - \left(0 \frac{1}{3}(-2, 2, 1, 0) \right) \\ &= (-1, -2, 2, 0) \\ \mathbf{u}_2 &= \frac{1}{\|\mathbf{w}_2\|} \mathbf{w}_2 \\ &= \frac{1}{3}(-1, -2, 2, 0) \end{aligned}$$

Thus

$$\mathcal{U} = \left\{ \frac{1}{3}(-2, 2, 1, 0), \frac{1}{3}(-1, -2, 2, 0) \right\}$$

is an orthonormal basis (w.r.t. the usual Euclidean inner product) for W .

(b)

$$\begin{aligned} \mathbf{p} &= \text{Proj}_W(\mathbf{v}) \\ &= (\mathbf{v} \cdot \mathbf{u}_1) \mathbf{u}_1 + (\mathbf{v} \cdot \mathbf{u}_2) \mathbf{u}_2 \\ &= \left((-3, 0, 3, 2) \cdot \frac{1}{3}(-2, 2, 1, 0) \right) \frac{1}{3}(-2, 2, 1, 0) + \\ &\quad \left((-3, 0, 3, 2) \cdot \frac{1}{3}(-1, -2, 2, 0) \right) \frac{1}{3}(-1, -2, 2, 0) \\ &= \frac{1}{9}9(-2, 2, 1, 0) + \frac{1}{9}9(-1, -2, 2, 0) \\ &= (-2, 2, 1, 0) + (-1, -2, 2, 0) \\ &= (-3, 0, 3, 0) \end{aligned}$$

(c) By the properties of the orthogonal projection $\mathbf{w}_3 = \mathbf{v} - \mathbf{p} = (0, 0, 0, 2)$ is perpendicular to the basis \mathcal{U} and as $\left\{ \frac{1}{3}(-2, 2, 1, 0), \frac{1}{3}(-1, -2, 2, 0), (0, 0, 0, 2) \right\}$ is an orthogonal set it is a basis for $\langle \{\mathbf{u}_1, \mathbf{u}_2, \mathbf{v}\} \rangle = \langle \{\mathbf{u}_1, \mathbf{u}_2, \mathbf{p}\} \rangle$ and so normalizing the last vector (to obtain an orthonormal set) as $\mathbf{u}_3 = \frac{1}{\|\mathbf{w}_3\|} \mathbf{w}_3 = (0, 0, 0, 1)$ we have

$$\mathcal{U}' = \left\{ \frac{1}{3}(-2, 2, 1, 0), \frac{1}{3}(-1, -2, 2, 0), (0, 0, 0, 1) \right\} \text{ as an orthonormal basis for } W' = \langle \{\mathbf{u}_1, \mathbf{u}_2, \mathbf{v}\} \rangle.$$

The Gram Schmidt algorithm applied blindly would arrive at exactly this orthonormal basis – the above calculates the \mathbf{w}_3 of Gram Schmidt from first principles rather than rote application of the algorithm.

11. *Solution.*

$$(a) \mathbf{w} = T(\mathbf{x}) = \begin{bmatrix} -1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ -1 \end{bmatrix} = \begin{bmatrix} -2 \\ 1 \end{bmatrix}.$$

$$(b) \mathbf{v} = S(\mathbf{w}) = \begin{bmatrix} 1 & 6 \\ 0 & -2 \end{bmatrix} \begin{bmatrix} -2 \\ 1 \end{bmatrix} = \begin{bmatrix} 4 \\ -2 \end{bmatrix}.$$

(c) The standard matrix for $S \circ T$

$$A_{S \circ T} = A_S A_T = \begin{bmatrix} 1 & 6 \\ 0 & -2 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 5 & 6 \\ -2 & -2 \end{bmatrix}$$

(d) The image $S \circ T(\mathbf{x})$ is

$$A_{S \circ T} \mathbf{x} = \begin{bmatrix} 5 & 6 \\ -2 & -2 \end{bmatrix} \begin{bmatrix} 2 \\ -1 \end{bmatrix} = \begin{bmatrix} 4 \\ -2 \end{bmatrix}.$$

Alternatively $S(T(\mathbf{x})) = S(\mathbf{w}) = \mathbf{v}$ as given in (a) and (b).

(e) We notice that $S(T(\mathbf{x})) = 2\mathbf{x}$ and so \mathbf{x} is an eigenvector with eigenvalue 2 for $A_{S \circ T}$.

12. *Solution.*

(a) Note from the previous question we have that 2 is an eigenvalue with eigenvector $[2 \ -1]^T$ so as the sum of the eigenvalues is the TRACE of the matrix we have the other eigenvalue being 1. This gives $A - 1I = \begin{bmatrix} 4 & 6 \\ -2 & -3 \end{bmatrix} \sim \begin{bmatrix} 2 & 3 \\ 0 & 0 \end{bmatrix}$ which has non-zero vector $[3 \ -2]^T$ in its solution space so $[3 \ -2]^T$ is an eigenvector with eigenvalue 1.

Or calculating from scratch

$$\det(A - \lambda I) = \det \left(\begin{bmatrix} 5 - \lambda & 6 \\ -2 & -2 - \lambda \end{bmatrix} \right) = (5 - \lambda)(-2 - \lambda) + 12 = 2 - 3\lambda + \lambda^2 = (1 - \lambda)(2 - \lambda).$$

So the eigenvalues are 1 and 2 we can calculate the eigenvector $[3 \ -2]^T$ for eigenvalue 1 exactly as above.

If $\lambda = 2$

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

which has $[2 \ -1]^T$ in its solution space, thus $[2 \ -1]^T$ is an eigenvector with eigenvalue 2.

(b) As the line is the span of the eigenvector $[2 \ -1]^T$ the line will get mapped on top of itself setwise and pointwise will be stretched by a factor of 2 that is $T(\alpha[2 \ -1]^T) = 2\alpha[2 \ -1]^T$.

13. *Solution.*

(a)

$$[T]_{\mathcal{S} \rightarrow \mathcal{S}} = \begin{bmatrix} 5 & 6 \\ -2 & -2 \end{bmatrix}$$

(b)

$$P_{\mathcal{B} \rightarrow \mathcal{S}} = \begin{bmatrix} 3 & 2 \\ -2 & -1 \end{bmatrix}$$

(c)

$$P_{\mathcal{S} \rightarrow \mathcal{B}} = (P_{\mathcal{B} \rightarrow \mathcal{S}})^{-1} = \begin{bmatrix} 3 & 2 \\ -2 & -1 \end{bmatrix}^{-1} = \begin{bmatrix} -1 & -2 \\ 2 & 3 \end{bmatrix}$$

(d)

$$[\mathbf{w}]_{\mathcal{B}} = P_{\mathcal{S} \rightarrow \mathcal{B}}[\mathbf{w}]_{\mathcal{S}} = \begin{bmatrix} -1 & -2 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} -2 \\ -1 \end{bmatrix} = \begin{bmatrix} -8 \\ 5 \end{bmatrix}$$

So $[-2 \quad -1]^T = -8\mathbf{b}_1 + 5\mathbf{b}_2$

(e)

$$\begin{aligned} [T]_{\mathcal{B} \rightarrow \mathcal{B}} &= P_{\mathcal{S} \rightarrow \mathcal{B}}[T]_{\mathcal{S} \rightarrow \mathcal{S}}P_{\mathcal{B} \rightarrow \mathcal{S}} \\ &= \begin{bmatrix} -1 & -2 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 5 & 6 \\ -2 & -2 \end{bmatrix} \begin{bmatrix} 3 & 2 \\ -2 & -1 \end{bmatrix} \\ &= \begin{bmatrix} -1 & -2 \\ 4 & 6 \end{bmatrix} \begin{bmatrix} 3 & 2 \\ -2 & -1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \end{aligned}$$

That $[T]_{\mathcal{B} \rightarrow \mathcal{B}}$ is diagonal should come as no surprise as the vectors in \mathcal{B} are eigenvectors of A with eigenvalues 1 and 2 respectively (as seen in the previous question).

(f)

$$[T(\mathbf{w})]_{\mathcal{B}} = [T]_{\mathcal{B} \rightarrow \mathcal{B}}[\mathbf{w}]_{\mathcal{B}} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} -8 \\ 5 \end{bmatrix} = \begin{bmatrix} -8 \\ 10 \end{bmatrix}$$

14. *Solution.*

(a)

$$\begin{aligned} \begin{bmatrix} 7 & 24 & 0 \\ 24 & -7 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 4 \\ 3 \\ 0 \end{bmatrix} &= \begin{bmatrix} 28 + 72 \\ 96 - 21 \\ 0 \end{bmatrix} = \begin{bmatrix} 100 \\ 75 \\ 0 \end{bmatrix} = 25 \begin{bmatrix} 4 \\ 3 \\ 0 \end{bmatrix} \\ \begin{bmatrix} 7 & 24 & 0 \\ 24 & -7 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ -4 \\ 0 \end{bmatrix} &= \begin{bmatrix} 21 - 96 \\ 72 + 28 \\ 0 \end{bmatrix} = \begin{bmatrix} -75 \\ 100 \\ 0 \end{bmatrix} = -25 \begin{bmatrix} 3 \\ -4 \\ 0 \end{bmatrix} \\ \begin{bmatrix} 7 & 24 & 0 \\ 24 & -7 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} &= \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = 1 \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \end{aligned}$$

thus

$$\begin{bmatrix} 4 \\ 3 \\ 0 \end{bmatrix}, \begin{bmatrix} 3 \\ -4 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

are eigenvectors of the matrix A with eigenvalues 25, -25 and 1 respectively.
and find their associated eigenvalues.

(b) The matrix P which has the eigenvectors of A as columns and D being the diagonal matrix with the corresponding eigenvalues as diagonal entries (in the appropriate order) explicitly

$$P = \begin{bmatrix} 4 & 3 & 0 \\ 3 & -4 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad D = \begin{bmatrix} 25 & 0 & 0 \\ 0 & -25 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

(c) We normalize the already orthogonal columns of P to find

$$Q = \begin{bmatrix} \frac{4}{5} & \frac{3}{5} & 0 \\ \frac{3}{5} & -\frac{4}{5} & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

15. *Solution.* Let A be an $n \times n$ real matrix.

- (a) The $n \times n$ matrix A is diagonalizable IF AND ONLY IF A has n linearly independent eigenvectors.
- (b) A is orthogonally diagonalizable IF A is symmetric that is $A^T = A$.
- (c) If A is orthogonally diagonalizable then $Q^T A Q = D \Leftrightarrow A = Q D Q^T$ (as Q is orthogonal if and only if $Q^{-1} = Q^T$) thus $A^T = (Q D Q^T)^T = (Q^T)^T D^T Q^T = Q D Q^T = A$ the matrix A is symmetric.