

620-142 Mathematics B
Solutions to Assignment 2

1. (a) The text is first converted to the numbers:

7 34 52 9 26 39 53

(You can use the table on page I.10.8 of the notes to help with this step.)

These are encrypted using $x \rightarrow x^e \pmod{m}$, i.e. $x \rightarrow x^{17} \pmod{143}$. Using the function `binarypow()` in MATLAB gives:

50 34 13 81 104 52 92

A quick way to do the calculation is the following:

```
>> x = [ 7 34 52 9 26 39 53 ]
>> y=[];
>> for i=1:7
>> y(i)= binarypow(x(i),17,143);
>> end
>> y
```

- (b) $m = 143 = 11 \times 13$ hence $\phi(m) = 10 \times 12 = 120$

- (c) (i) We use Euclid's algorithm to find $x, y \in \mathbb{Z}$ such that $17x + 120y = 1$.
We have $120 = 7 \times 17 + 1$, so $1 = -7 \times 17 + 1 \times 120$ and $-7 \times 17 \equiv 1 \pmod{120}$.
Hence we can take $d = -7$ or 113 (since $-7 \equiv 113 \pmod{120}$).

- (ii) We decrypt each number in the message

112 23 25 13 137 105 44 67 92

by $x \rightarrow x^d \pmod{m}$, i.e. $x \rightarrow x^{113} \pmod{143}$.

Using `binarypow()` as above gives:

8 56 38 52 37 40 44 45 53

Converting to text, gives the message:

I'm lost.

2. To test for linear dependence, we solve the equation $\alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \alpha_3 \mathbf{v}_3 = \mathbf{0}$ where $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$. Writing the vectors as columns of a matrix and reducing to row echelon form gives:

$$\begin{bmatrix} 1 & 2 & 9 \\ -1 & 5 & 5 \\ 3 & -1 & 13 \\ -1 & 6 & 7 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 2 & 9 \\ 0 & 7 & 14 \\ 0 & -7 & -14 \\ 0 & 8 & 16 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 2 & 9 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Since $\text{rank} < 3$, the system of linear equations has **non-zero solutions**, so the vectors are **linearly dependent**.

From the final reduced row echelon form, we see that $\alpha_3 = -1, \alpha_2 = 2, \alpha_1 = 5$ is one solution. Thus $2\mathbf{v}_1 + 5\mathbf{v}_2 - 1\mathbf{v}_3 = \mathbf{0}$ or $\mathbf{v}_3 = 5\mathbf{v}_1 + 2\mathbf{v}_2$, i.e.

$$(9, 5, 13, 7) = 5(1, -1, 3, -1) + 2(2, 5, -1, 6).$$

3. (a) We prove that

$$S = \{(x, y, z, w) \in \mathbb{R}^4 : x + y - 2z - w = 0\}$$

is a subspace of \mathbb{R}^4 by checking the three subspace properties.

(0) S is not empty: For example, it contains $(0, 0, 0, 0)$.

(1) S is closed under addition: Let $\mathbf{v}_1 = (x_1, y_1, z_1, w_1)$ and $\mathbf{v}_2 = (x_2, y_2, z_2, w_2)$ be arbitrary vectors in S . Then we have $x_1 + y_1 - 2z_1 - w_1 = 0$ since $\mathbf{v}_1 \in S$ and $x_2 + y_2 - 2z_2 - w_2 = 0$ since $\mathbf{v}_2 \in S$. Now

$$\mathbf{v}_1 + \mathbf{v}_2 = (x_1 + x_2, y_1 + y_2, z_1 + z_2, w_1 + w_2) = (x, y, z, w)$$

has coordinates satisfying

$$\begin{aligned} x + y - 2z - w &= (x_1 + x_2) + (y_1 + y_2) - 2(z_1 + z_2) - (w_1 + w_2) \\ &= (x_1 + y_1 - 2z_1 - w_1) + (x_2 + y_2 - 2z_2 - w_2) \\ &= 0 + 0 = 0. \end{aligned}$$

Thus $\mathbf{v}_1 + \mathbf{v}_2 \in S$.

(2) S is closed under scalar multiplication: Let $\mathbf{v}_1 = (x_1, y_1, z_1, w_1) \in S$ and $\alpha \in \mathbb{R}$. Then

$$\alpha \mathbf{v}_1 = (\alpha x_1, \alpha y_1, \alpha z_1, \alpha w_1) = (x, y, z, w)$$

has coordinates satisfying

$$x + y - 2z - w = \alpha x_1 + \alpha y_1 - 2(\alpha z_1) - (\alpha w_1) = \alpha(x_1 + y_1 - 2z_1 - w_1) = \alpha \cdot 0 = 0.$$

Thus $\alpha \mathbf{v}_1 \in S$.

Since (0), (1), (2) are satisfied, we conclude that S is a subspace of \mathbb{R}^4 .

- (b) $T = \{(x, y) \in \mathbb{R}^2 : y^2 - x^2 = 0\}$ is **not** a subspace of \mathbb{R}^2 since it is not closed under addition. For example, $\mathbf{v} = (1, 1) \in T$ and $\mathbf{w} = (1, -1) \in T$ but $\mathbf{v} + \mathbf{w} = (2, 0) \notin T$.

4. We can use the “Powerful Facts” on page II.7.4 of the notes.

- (a) Any linearly independent set in the 2-dimensional space \mathbb{R}^2 contains at most 2 vectors. So the given 3 vectors are **not** linearly independent.
- (b) Any spanning set for the 4-dimensional space \mathbb{R}^4 contains at least 4 vectors, hence the given 3 vectors do **not** span \mathbb{R}^4 .

(**Alternatively:** both parts can be done by writing the vectors as columns of a matrix and using row reduction as in Q2 and Q5.)

5. (a) We must check whether $\alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \alpha_3 \mathbf{v}_3 = \mathbf{v}$ has a solution for all $\mathbf{v} = (a, b, c) \in \mathbb{R}^3$. We write the vectors $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ as columns of a matrix and reduce to row echelon form:

$$\begin{bmatrix} 2 & 1 & 3 \\ -1 & 4 & -1 \\ 4 & 2 & 3 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & -4 & 1 \\ 2 & 1 & 3 \\ 4 & 2 & 3 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & -4 & 1 \\ 0 & 9 & 1 \\ 0 & 18 & -1 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & -4 & 1 \\ 0 & 9 & 1 \\ 0 & 0 & -3 \end{bmatrix}$$

Since the rank of this matrix is 3, we conclude that the vectors **span** \mathbb{R}^3 .

Alternatively: Start with an augmented matrix

$$\begin{bmatrix} 2 & 1 & 3 & | & a \\ -1 & 4 & -1 & | & b \\ 4 & 2 & 3 & | & c \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & -4 & 1 & | & b \\ 0 & 9 & 1 & | & a + 2b \\ 0 & 0 & -3 & | & c - 2a \end{bmatrix}.$$

and conclude that the corresponding linear system has a solution for all $a, b, c \in \mathbb{R}$.

- (b) Since we have a spanning set containing 3 vectors and $\dim \mathbb{R}^3 = 3$, the vectors **do** give a basis for \mathbb{R}^3 by the “Powerful Facts” on page II.7.4 of the notes.

(**Alternatively:** the row reduction above shows that the vectors are linearly independent, so form a basis.)