

620-142 Mathematics B
Assignment 2
Due: 2pm, Friday, April 18

Please leave your assignment in your tutor's box located near the north entrance to the Richard Berry building. Make sure that you have written your name, your student number, your tutor's name, and your tutorial time on the front page.

You should give **complete explanations** for all your answers.

1. *RSA cryptosystem*. (You might want to use MATLAB to help with this problem. If so, indicate the MATLAB commands you used.)

Suppose it has been agreed that message symbols are encoded as follows:

$$A = 0, B = 1, \dots, Z = 25, a = 26, b = 27, \dots, z = 51$$

$$\text{space} = 52, \text{.} = 53, \text{,} = 54, \text{-} = 55, \text{' } = 56$$

Messages are made up of a sequence of numbers, each number being in the range 0 to 56.

Suppose Jan wants to be able to receive encrypted messages from her friends. She chooses two prime numbers p and q whose product is $m = 143$. The first part of her public key is therefore 143. Knowing that $e = 17$ satisfies $\gcd(e, \phi(m)) = 1$, she tells all her friends to encrypt messages to her using the numbers 143 and 17.

- (a) Suppose Mike wants to send Jan the 7 character message

Hi Jan.

Code each symbol of the message using the information in the first paragraph of this question, and then encrypt the code so that it is ready for sending to Jan.

- (b) Calculate $\phi(m)$. (Note that, in reality, m would be chosen so large that calculating $\phi(m)$ without knowing the prime factorization of m would be impractical given the current state of technology.)
- (c) Jan receives the encrypted message

$$112\ 23\ 25\ 13\ 137\ 105\ 44\ 67\ 92$$

from Linda.

- (i) Calculate d such that $ed \equiv 1 \pmod{\phi(m)}$.
- (ii) Decrypt the message, and recover the original text using the information in the first paragraph of this question.

2. Are the vectors

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

linearly dependent or linearly independent? If they are linearly dependent, write one vector as a linear combination of the others. Explain your answers.

3. (a) Prove that

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

is a subspace of \mathbb{R}^4 by verifying the three conditions in the definition of subspace.

- (b) Decide whether

$$T = \{(x, y) \in \mathbb{R}^2 : y^2 - x^2 = 0\}$$

is a subspace of \mathbb{R}^2 . Explain your answer.

4. (a) Are the vectors $(1, 1), (1, 3), (1, 4)$ linearly independent?

- (b) Do the vectors $(1, 0, 1, 0), (0, 1, 0, 1), (0, 0, 1, 1)$ span \mathbb{R}^4 ?

Give brief explanations. (Hint: try to avoid unnecessary calculations.)

Please turn over.

5. Consider the vectors $(2, -1, 4)$, $(1, 4, 2)$, $(3, -1, 3)$ in \mathbb{R}^3 .

(a) Do the vectors span \mathbb{R}^3 ?

(b) Do they form a basis for \mathbb{R}^3 ?

Explain your answers.

Challenge problem (Not for assessment)

(Chocolate bars will be given for the best solutions!)

Show that each Euclidean space \mathbb{R}^n is not the union of finitely many subspaces of dimension $n - 1$. (Hint: first consider the cases $n = 2, 3$.)