ET6501
Homework #3

Date: April 17, 2024.
Due Date: May 8, 2024. **Instructor: M. B. Lin**

Please note that **NO late homework** will be accepted.

1. Answer the following questions:
   (a) Compute the DFT of the vector (0, 1, 2, 3).
   (b) Show how Iterative-FFT computes the DFT of the input vector $(0, 2, 3, -1, 4, 5, 7, 9)$.
2. Consider the product of two polynomials as follows and answer the following questions:

$$A(x) = 4x - 5$$
$$B(x) = 10x + 9$$

   (a) Find $C(x) = A(x)B(x)$ with the conventional method.
   (b) Find the product with the DFT/IDFT method.
   (c) Verify your results.
3. Considering an RSA key set with $p = 11$, $q = 29$, $n = 319$, and $e = 3$, answer the following questions:
   (a) What value of d should be used in the secret key?
   (b) Compute the ciphertext $P(M)$, where $M = 100$ with the public key.
   (c) Compute the message M from the ciphertext with the secret key.
   (d) Verify their results.