

# Project 4: RSA, DFT, FFT

Author: Gabriel Hofer

Course: CSC-372 Analysis of Algorithms

Instructor: Dr. Rebenitsch

Due: November 19, 2020

## Question 1

[20 points] use the RSA algorithm. If  $p = 13$  and  $q = 15$ ,  $e = 11$

[2 points] What is  $n$ ?

$$n = p \cdot q$$

$$n = 195$$

[2 points] What is  $\varphi(n)$ ?

$\varphi$  is Euler's totient function.

$$\varphi(n) = 96$$

[2 points] Name an invalid  $e$  for this problem.

$\lambda$  is Carmichael's function.

$$\lambda(n) = 12$$

$e$  must be in the range  $1 < e < \lambda(n)$  and  $\gcd(e, \lambda(n)) = 1$ . So, an example of an invalid  $e$  would be 4 since

$$\gcd(4, \lambda(195)) = 4$$

[6 points] What is  $d$  (you MUST show your work for credit)?

We want to find the modulo multiplicative-inverse of  $e$  modulo  $\lambda(n)$ . Fermat's Little Theorem:

$$e^{\lambda(n)-1} \equiv 1 \pmod{\lambda(n)}$$

Multiply both sides by  $a^{-1}$ .

$$e^{\lambda(n)-2} \equiv e^{-1} \pmod{\lambda(n)}$$

Simplify.

$$1 \equiv e^{-1} \pmod{\lambda(n)}$$

So  $d = 1$ .

[8 points] Use the above values to encode 5 with  $e$  (use the MOD-Exp function and show the values for each iteration). You should only [show] the first 5 iterations rather than all  $e$  iterations.

### Question 3

[30 points] Compute the DFT for  $n=6$  and  $f(x) = 3x^5 + 4x^4 - 2x^3 - x^2 + 4$ , for the  $2^{nd}$  power ( $w_6^2$ ) Note the missing powers! It must be clear that this is the DFT (so a tree-like structure would be best). You must show your work for credit. Your answers must be in  $a + bi$  format.

$$f(x) = 3x^5 + 4x^4 - 2x^3 - x^2 + 4 \Rightarrow \mathbf{x} = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 4 \\ 0 \\ -1 \\ -2 \\ 4 \\ 3 \end{pmatrix}$$

$$X_0 = e^{-i2\pi 0 \cdot 0/6} \cdot 4 + e^{-i2\pi 0 \cdot 1/6} \cdot 0 + e^{-i2\pi 0 \cdot 2/6} \cdot -1 + e^{-i2\pi 0 \cdot 3/6} \cdot -2 + e^{-i2\pi 0 \cdot 4/6} \cdot 4 + e^{-i2\pi 0 \cdot 5/6} \cdot 3$$

$$X_1 = e^{-i2\pi 1 \cdot 0/6} \cdot 4 + e^{-i2\pi 1 \cdot 1/6} \cdot 0 + e^{-i2\pi 1 \cdot 2/6} \cdot -1 + e^{-i2\pi 1 \cdot 3/6} \cdot -2 + e^{-i2\pi 1 \cdot 4/6} \cdot 4 + e^{-i2\pi 1 \cdot 5/6} \cdot 3$$

$$X_2 = e^{-i2\pi 2 \cdot 0/6} \cdot 4 + e^{-i2\pi 2 \cdot 1/6} \cdot 0 + e^{-i2\pi 2 \cdot 2/6} \cdot -1 + e^{-i2\pi 2 \cdot 3/6} \cdot -2 + e^{-i2\pi 2 \cdot 4/6} \cdot 4 + e^{-i2\pi 2 \cdot 5/6} \cdot 3$$

$$X_3 = e^{-i2\pi 3 \cdot 0/6} \cdot 4 + e^{-i2\pi 3 \cdot 1/6} \cdot 0 + e^{-i2\pi 3 \cdot 2/6} \cdot -1 + e^{-i2\pi 3 \cdot 3/6} \cdot -2 + e^{-i2\pi 3 \cdot 4/6} \cdot 4 + e^{-i2\pi 3 \cdot 5/6} \cdot 3$$

$$X_4 = e^{-i2\pi 4 \cdot 0/6} \cdot 4 + e^{-i2\pi 4 \cdot 1/6} \cdot 0 + e^{-i2\pi 4 \cdot 2/6} \cdot -1 + e^{-i2\pi 4 \cdot 3/6} \cdot -2 + e^{-i2\pi 4 \cdot 4/6} \cdot 4 + e^{-i2\pi 4 \cdot 5/6} \cdot 3$$

$$X_5 = e^{-i2\pi 5 \cdot 0/6} \cdot 4 + e^{-i2\pi 5 \cdot 1/6} \cdot 0 + e^{-i2\pi 5 \cdot 2/6} \cdot -1 + e^{-i2\pi 5 \cdot 3/6} \cdot -2 + e^{-i2\pi 5 \cdot 4/6} \cdot 4 + e^{-i2\pi 5 \cdot 5/6} \cdot 3$$

$$X = \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \\ X_5 \end{pmatrix} = \begin{pmatrix} 8 + 0i \\ 6 + 6.928i \\ -1 - 1.732i \\ 6 + 0i \\ -1 + 1.732i \\ 6 - 6.928i \end{pmatrix}$$