

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 $\varphi(n)$?

$$\varphi(n) = \text{lcm}(p-1, q-1) = 84$$

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

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

$$\text{gcd}(4, \varphi(195)) = 4$$

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

We want to find the modulo multiplicative-inverse of e modulo $\varphi(n)$. ϕ is euler's totient function. Fermat's Little Theorem:

$$e^{\phi(\varphi(n))} \equiv 1 \pmod{\varphi(n)}$$

Multiply both sides by a^{-1} :

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

Since $e^{\phi(84)-2} \pmod{84} = 23$:

$$23 \equiv e^{-1} \pmod{\varphi(n)}$$

So $d = 23$.

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

The Public Key: ($n = 195$, $e = 11$). Encryption function:

$$c(m) = m^{11} \pmod{195}$$

$$11 \equiv 11^1 \pmod{195}$$

$$121 \equiv 11^2 \pmod{195}$$

$$161 \equiv 11^3 \pmod{195}$$

$$16 \equiv 11^4 \pmod{195}$$

$$176 \equiv 11^5 \pmod{195}$$

Question 3

[30 points] Compute the DFT for n=6 and $f(x) = 3x^5 + 4x^4 - 2x^3 - x^2 + 4$, for the 2nd 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.

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

$$X_0 = e^{-i2\pi0\cdot0/6} \cdot 4 + e^{-i2\pi0\cdot1/6} \cdot 0 + e^{-i2\pi0\cdot2/6} \cdot -1 + e^{-i2\pi0\cdot3/6} \cdot -2 + e^{-i2\pi0\cdot4/6} \cdot 4 + e^{-i2\pi0\cdot5/6} \cdot 3$$

$$X_1 = e^{-i2\pi1\cdot0/6} \cdot 4 + e^{-i2\pi1\cdot1/6} \cdot 0 + e^{-i2\pi1\cdot2/6} \cdot -1 + e^{-i2\pi1\cdot3/6} \cdot -2 + e^{-i2\pi1\cdot4/6} \cdot 4 + e^{-i2\pi1\cdot5/6} \cdot 3$$

$$X_2 = e^{-i2\pi2\cdot0/6} \cdot 4 + e^{-i2\pi2\cdot1/6} \cdot 0 + e^{-i2\pi2\cdot2/6} \cdot -1 + e^{-i2\pi2\cdot3/6} \cdot -2 + e^{-i2\pi2\cdot4/6} \cdot 4 + e^{-i2\pi2\cdot5/6} \cdot 3$$

$$X_3 = e^{-i2\pi3\cdot0/6} \cdot 4 + e^{-i2\pi3\cdot1/6} \cdot 0 + e^{-i2\pi3\cdot2/6} \cdot -1 + e^{-i2\pi3\cdot3/6} \cdot -2 + e^{-i2\pi3\cdot4/6} \cdot 4 + e^{-i2\pi3\cdot5/6} \cdot 3$$

$$X_4 = e^{-i2\pi4\cdot0/6} \cdot 4 + e^{-i2\pi4\cdot1/6} \cdot 0 + e^{-i2\pi4\cdot2/6} \cdot -1 + e^{-i2\pi4\cdot3/6} \cdot -2 + e^{-i2\pi4\cdot4/6} \cdot 4 + e^{-i2\pi4\cdot5/6} \cdot 3$$

$$X_5 = e^{-i2\pi5\cdot0/6} \cdot 4 + e^{-i2\pi5\cdot1/6} \cdot 0 + e^{-i2\pi5\cdot2/6} \cdot -1 + e^{-i2\pi5\cdot3/6} \cdot -2 + e^{-i2\pi5\cdot4/6} \cdot 4 + e^{-i2\pi5\cdot5/6} \cdot 3$$

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