Project 4: RSA, DFT, FFT

Author: Gabriel Hofer

Course: CSC-372 Analysis of Algorithms

Instructor: Dr. Rebenitsch

Due: November 19, 2020

Computer Science and Engineering
South Dakota School of Mines and Technology

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 $\varphi(n)$?

φ is Euler's totient function.

$$\varphi(n) = 96$$

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

λ 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:

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

Multiply both sides by a^{-1}.

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

Simplify.

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

So $d = 1$.

[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.

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.