CS372 Homework 5: FFFT

DUE: Tuesday, Nov 21, at 7AM

The purpose of this assignment is to give you practice with RSA, the DFT, and the FFT. Since it is a 1.5 week assignment, it is worth 75 points.

The assignment consists of 3 parts

1) Coding the area of a polygon
2) Application of geometry algorithms
3) Concepts

+2 Bonus points for submitted 1 days early! +4 Bonus points for submitted 2 days early!

Coding

[25 points] RSA Encryption

You will be coding a very basic form of the RSA encryption algorithm. You will accept 2 primes, e, and some text to encrypt via the command line. Your first task will be to find d. Your second tasks will be to make a fast modulus power functions since your values will quickly get too big to fit inside a integer. Your third task will be to encrypt the text as one integer per character. You're forth task will be to decrypt it. Your fifth task will be taking a encrypted value and decrypting it.

More details and specifications:

- [3 points] The program must be able to be run as follows:

  ```
  rsa.exe p q e my_text num1 num2 num3 …
  ```

- You may assume p, q and e are integers and my_text has no spaces.
- My_text is the text to encrypt
- Num1 to numN are OPTIONAL values that have been encrypted using p, q, and e. You must decrypt them with the d that you find.
- There are MANY pages of primes out there, and you may assume that that pq is less than the max value of a long int in c++.
- [4 points] You must CHECK if e is a valid choice for p and q. If not, output:

  ```
  E is invalid
  ```

  And then end the program there.
- Output d after finding the value
- [4 points] Encrypt each character separately, and store the result in an int
- [5 points] You may use which ever fast modulus power algorithm you wish.
- You must output the encrypted text in one line with a space separating the values, followed by the same text decrypted. See below for format.
- [4 points] You must output the decrypted num1 to numN (if applicable) on one line and no spaces.

- [5 points] The following is an example output. You MUST follow this format. (yes, please output the text to be encrypted in the encrypted line) :

  ```
  >rsa.exe 7 13 3 abc 53 33 51
  D:  77
  Encrypted (abc): 20 98 29
  Decoding gives: abc
  Decoding command line gives: def
  ```
- WARNING: if you try to encrypt and decrypt text whose ascii values are over pq, this will fail!
- Points will be given on the number of tests passed.

  OTHER RESTRICTIONS

  - *You may NOT use system("Pause"); cin >> var;, or any other means to stop the command window from closing. This breaks my script. Use "start without debugging" and have the linker subsystem set to "console." Let me know if you have trouble. This will be -5 if done.*
  - *If something is NOT working, put it in the file header for the cpp file with main(). If it is NOT there, there will be no partial credit.*
  - *Crashing immediately is -7%*
  - *Crashing sometimes is -5%*

You may NOT use OS or computer specific C++ libraries (e.g. no Linux/Mac/Win MACROs or new libraries you may have installed). This MUST compile on Visual Studio 2017.

This will be graded on correctness and coding style, as well. If anything is not working in the code when you submit, put what is going wrong, what you think is doing it, and whether you want me to take a closer look at it in the file header.

See submission guidelines at the end of the document

[32 points] Application

1. [16 points] Use the RSA algorithm, If p=13 and q=11, e=7 …
   a. [1 points] What is n?

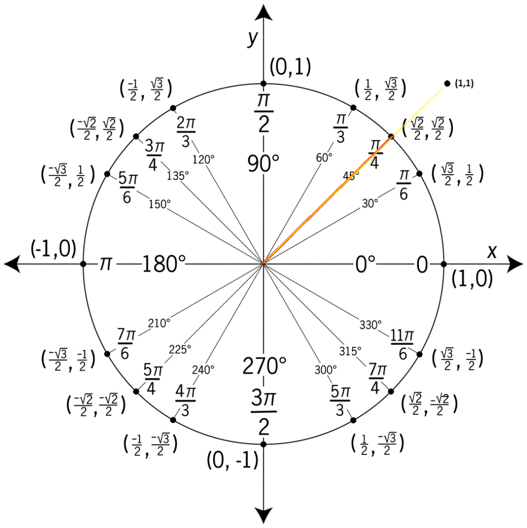
   b. [1 points] What is $\varphi(n)$?

   c. [1 points] Name an invalid e for this problem

   d. [3 points] What is d (you MUST show your work for credit)?

   e. [7 points] Use the above values to encode 5 (use the MOD-Exp function and show the values for each iteration)

   f. [3 points] Use these values to decode 71 (use may just punch this into your calculator)


y
x
(0,1)
$\frac{\pi}{2}$
90°
$(\frac{1}{2}, \frac{\sqrt{3}}{2})$
$\frac{\pi}{3}$
60°
(1,1)
$(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2})$
$\frac{\pi}{4}$
45°
$(\frac{\sqrt{3}}{2}, \frac{1}{2})$
$\frac{\pi}{6}$
30°
(1,0)
0°
0
$(\frac{-1}{2}, \frac{\sqrt{3}}{2})$
$\frac{2\pi}{3}$
120°
$(\frac{-\sqrt{2}}{2}, \frac{\sqrt{2}}{2})$
$\frac{3\pi}{4}$
135°
$(\frac{-\sqrt{3}}{2}, \frac{1}{2})$
$\frac{5\pi}{6}$
150°
(-1,0)
π
180°
210°
$\frac{7\pi}{6}$
$(\frac{-\sqrt{3}}{2}, \frac{-1}{2})$
225°
$\frac{5\pi}{4}$
$(\frac{-\sqrt{2}}{2}, \frac{-\sqrt{2}}{2})$
240°
$\frac{4\pi}{3}$
$(\frac{-1}{2}, \frac{-\sqrt{3}}{2})$
270°
$\frac{3\pi}{2}$
(0, -1)
300°
$\frac{5\pi}{3}$
$(\frac{1}{2}, \frac{-\sqrt{3}}{2})$
315°
$\frac{7\pi}{4}$
$(\frac{\sqrt{2}}{2}, \frac{-\sqrt{2}}{2})$
330°
$\frac{11\pi}{6}$
$(\frac{\sqrt{3}}{2}, \frac{-1}{2})$

2. [6 points] Compute the DFT for the 0th and 2nd roots (not FFT) of $f(x) = 2x^2 + 3x + 2$. You must should your work for credit. You must should your work for credit, and I highly suggest the table method used in class to track your work which makes it easier for me to give partial credit.

3. [15 points] Compute the FFT for of $f(x) = x^7 + 4x^6 + 2x^5 + 2x^2 + 3x + 2$. Note the missing powers! It must be clear it is the FFT and not the DFT (so a tree-like structure would be best). You **must** show your work for credit.

[13 points] Concepts

1. [5 points] How could the FFT be used to determine the common weather cycles for an area?

2. [8 points] RSA in its simplest form (small primes and 1 character at a time) is not used, name and explain at least two reasons.

Submission instructions (correct submission [5 points])

Full syllabus deductions for submissions are now in effect

You may upload as many times as you please, but only the last submission will be graded. A faulty submission that could have been checked (e.g. missing file), will have a 25% deduction if a corrected submission is submitted within 24 hours of the request, and will be a 0 otherwise. Not compiling is -15% as per syllabus policy.

1. Zip up your code files **(.cpp and .h files ONLY),** and the PDF into 1 zip folder. If the compressed folder opens with 7-zip, your good.
2. Submit this to D2L under the associated folder.

You may submit the PDF portion on paper by either giving it to me, sliding it under may door, or putting it in my mailbox.

If you have any trouble with D2L, please email me (with your submission if necessary).