Homework 5 (Due: 6/19th)

(1) Write the Matlab or Python code to compute the FFT of two N-point real signals x and y using only one N-point FFT. (20 scores)

$$[Fx, Fy] = \text{fftreal}(x, y)$$

The code should be handed out by NTUCool.

(2) Suppose that length($x[n]$) = 1200. What is the best way to implement the convolution of $x[n]$ and $y[n]$ if

(a) length($y[n]$) = 300, (b) length($y[n]$) = 30,

(c) length($y[n]$) = 8, and (d) length($y[n]$) = 2?

Please show (i) the calculation method (direct, non-sectioned convolution, or sectioned convolution), (ii) the number of points of the FFT, (iii) and the number of real multiplications for the best implementation method. Also, consider the general case where $x[n]$ and $y[n]$ are complex sequences and the FFT of $y[n]$ can be computed in prior. (25 scores)

(3) (a) What are the number of entries equal to 1 and -1 for the 2^k-point Walsh transform? (b) What are the number of entries equal to 1, 0, and -1 for the 2^k-point Haar transform? (c) What is the most important application of the Walsh transform nowadays? (d) What is the most important advantage of the Haar transform nowadays? (20 scores)

(4) (a) What is the results of CDMA if there are three data [1 0 1], [1 1 0], [0 1 1] and these three data are modulated by the 1st, 4th, and 10th rows of the 16-point Walsh transform? (The beginning row is the 1st row). (10 scores)

(b) In (a), if the 7th and the 19th entries of the CDMA results are missed, can we recover the original data? Why? (5 scores)

(5) Ramanujan's Sum in NTT

Given $M = 11$, $\alpha = 8+6i$, and $N = 12$. Please determine the complex number theoretic transform (CNT) of $\mathbf{x}$ if

$$\mathbf{x} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Hint: fft(x) is as follows, which is Ramanujan's Sum

$$fft(\mathbf{x}) = \begin{bmatrix} 4 & 0 & 2 & 0 & -2 & 0 & -4 & 0 & -2 & 0 & 2 & 0 \end{bmatrix}$$ (8 scores)

(6) (a) Please determine

$$3^{2049} \bmod 103 \qquad \text{(Hint: 費馬小定理)}$$

(b) Suppose that $x \bmod 43 = 2$ *and* $x \bmod 67 = 13$

Please Determine

$$x \bmod 2881. \qquad \text{(Hint: Chinese Remainder Theorem)}$$

(c) $n! = n(n-1)(n-2) \ldots. 1$. Please determine 39! mod 43

(Hint: Wilson's Theorem) (12 scores)

(Extra): Answer the questions according to your student ID number.

(ended with (1, 6), (2, 7), (3, 8), (4, 9))

2.

(a)

$N = 1200,\ M = 300$

(i) $IFFT[FFT(x[n])FFT(h[n])]$, $P = N + M - 1 = 1499$

$2 \times M_{1499} + 3 \times 1499 = 2 \times 10420 + 3 \times 1499 = 25337$

(ii) Sectioned convolution, $L_0 = 600$

$P_0 = 600 + 300 - 1 = 799$, set $P = 784$, $L = 784 - 300 + 1 = 485$, $S = \frac{1200}{485} = 3$

$3(2MML_{784} + 3 \times 784) = 33528$

(iii) Direct $3 \times 1200 \times 300 = 1080000$

$\Rightarrow$ Best way: FFT then IFFT, total # of real mul.: 25337 #

(b)

$N = 1200,\ M = 30$

(i) FFT then IFFT

$P \geq 1200 + 30 - 1 = 1229$

$\Rightarrow P = 1260$

$2\,MML_{1260} + 3 \times 1260 = 19060$

(ii) Sectioned conv.

$L_0 = 174,\ P_0 = 174 + 30 - 1 = 203$, Let $P = 204$, $L = 204 - 30 + 1 = 185$, $S = \frac{1100}{185} = 7$

$7(2 \times MML_{204} + 3 \times 204) = 17948$

(iii) Direct $= 3 \times 1200 \times 30 = 108000$

$\Rightarrow$ Best way: Section Convolution, total # of rel mul. $= 17948$ #

(C)

$N = 1200, \; M = 8$

(i) FFT then IFFT

$P \geq 1200 + 8 - 1 = 1207$

$\Rightarrow P = 1260$

$2\,MUL_{1260} + 3 \times 1260 = 19060$

(ii) Sectioned conv.

$L_0 = 30, \; P_0 = 30 + 8 - 1 = 37$, Let $P = 36$, $L = 36 - 8 + 1 = 29$, $S = \frac{1100}{29} = 38$

$38(2 \times MUL_{36} + 3 \times 36) = 8968$

(iii) Direct $= 3 \times 1200 \times 8 = 28800$

$\Rightarrow$ Best way: Section Convolution, total # of rel mul. $= 8968$ #

(d)

$N = 1200,\ M = 2$

(i) FFT then IFFT

$P \geq 1200 + 2 - 1 = 1201$

$\Rightarrow P = 1260$

$2 MUL_{1260} + 3 \times 1260 = 19060$

(ii) Sectioned conv.

$L_0 = 2,\ P_0 = 2 + 2 - 1 = 4$, Let $P = 3$, $L = 3 - 2 + 1 = 4$, $S = \frac{1100}{4} = 275$

$275 (2 \times MUL_3 + 3 \times 3) = 2750$

(iii) Direct $= 3 \times 1200 \times 2 = 7200$

$\Rightarrow$ Best way: Section Convolution, total # of rel mul. $= 2750$ #

3.

(a)

equal 1 : $\frac{2^k \times 2^k}{2} = 2^{2k-1}$

equal -1 : $\frac{2^k \times 2^k}{2} = 2^{2k-1}$

(b)

equal 1 or -1 : $2^k \log_2(2^k) = k \cdot 2^k$

equal 0 : $(2^k \times 2^k) - k \cdot 2^k = 2^{2k} - k \cdot 2^k$

(c)

spectrum analysis

(d)

edge dection, localized spectrum

4.

(a)

$[1\ 0\ 1],\ [1\ 1\ 0],\ [0\ 1\ 1] \Rightarrow [1\ {-1}\ 1],\ [1\ 1\ {-1}],\ [-1\ 1\ 1]$

1^{st} rows $= [1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1]$

4^{th} rows $= [1\ {-1}\ {-1}\ 1\ 1\ {-1}\ {-1}\ 1\ 1\ {-1}\ {-1}\ 1\ 1\ {-1}\ {-1}\ 1]$

10^{th} rows $= [1\ 1\ {-1}\ {-1}\ 1\ 1\ {-1}\ {-1}\ {-1}\ {-1}\ 1\ 1\ {-1}\ {-1}\ 1\ 1]$

Modulate $[1\ 0\ 1]$ for Channel 1 (1^{st} rows $\times$ $[1\ {-1}\ 1]$

$([1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1],\ [-1\ {-1}\ {-1}\ {-1}\ {-1}\ {-1}\ {-1}\ {-1}\ {-1}\ {-1}\ {-1}\ {-1}\ {-1}\ {-1}\ {-1}\ {-1}],$

$[1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1])$

Modulate [1 1 0] for Channel 1 (4th rows × [1 1 -1]

([1 -1 -1 1 1 -1 -1 1 1 -1 -1 1 1 -1 -1 1], [1 -1 -1 1 1 -1 -1 1 1 -1 -1 1 1 -1 -1 1 1],

[-1 1 1 -1 -1 1 1 -1 -1 1 1 -1 -1 1 1 -1])

Modulate [0 1 1] for Channel 1 (10th rows × [-1 1 1]

([-1 -1 1 1 -1 -1 1 1 1 1 -1 -1 1 1 -1 -1], [1 1 -1 -1 1 1 -1 -1 -1 -1 1 1 -1 -1 1 1],

[1 1 -1 -1 1 1 -1 -1 -1 -1 1 1 -1 -1 1 1])

result:

[3, -1, -3, 1, 3, -1, -3, 1, 1, -3, -1, 3, 1, -1, 1, 3]

(b)

可以

5.

$M = 11, \ \alpha = 8+6i, \ N = 12$

$x = [0\ 1\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 1]$

$FFT(x) = [4\ 0\ 2\ 0\ -2\ 0\ -4\ 0\ -2\ 0\ 2\ 0]$

$$CNTT = X(k) = \sum_{n=0}^{N-1} x(n) \cdot \alpha^{kn} \bmod M$$

$4 \bmod 11 = 4 \qquad 2 \bmod 11 \quad 2$

$0 \bmod 11 \quad 0 \qquad 0 \bmod 11 \quad 0$

$2 \bmod 11 \quad 2 \qquad \Rightarrow CNTT(x) = [4\ 0\ 2\ 0\ 9\ 0\ 7\ 0\ 2\ 0]$

$0 \bmod 11 \quad 0$

$-2 \bmod 11 \quad 9$

$0 \bmod 11 \quad 0$

$-4 \bmod 11 \quad 7$

$0 \bmod 11 \quad 0$

6.

(a)

$a^{p-1} \equiv 1 \mod p$

$a=3,\ p=103$

$2049 = 20 \times 102 + 9$

$\Rightarrow 3^{2049} = (3^{102})^{20} \cdot 3^9$

$\Rightarrow (3^{102})^{20} \equiv 1^{20} \equiv \mod 103$

$3^{2049} \equiv 3^9 \mod 103$

$19683 = 103 \times 191 + 90$

$\Rightarrow 3^9 = 90 \mod 103$

$\Rightarrow 3^{2049} = 90 \mod 103$ #

(b)

$x \mod 43 = 2$

$x \mod 67 = 13$

$43 \times 67 = 2881$

$\Rightarrow x \equiv 2 \mod 43$

$x \equiv 13 \mod 67$

Let $x = 43k+2$

$\Rightarrow 43k \equiv 11 \mod 67$

$\Rightarrow k = 55 \mod 67$

$x = 43k+2 = 2367$

$\Rightarrow x = 2367$ mode 2881 #

(c)

$(p-1)! \equiv -1 \mod p$

$42! = 42 \times 41 \times 40 \times 39!$

$\Rightarrow 42 \times 41 \times 40 \times 39! = -1 \mod 43$

$42 = -1 \mod 43$

$41 = -2 \mod 43$

$40 = -3 \mod 43$

$\Rightarrow 42 \times 41 \times 40 = -6 \mod 43 = 37 \mod 43$

$37 \times 39! = -1 \mod 43 \Rightarrow 39! = -37^{-1} \mod 43$

$\Rightarrow 39! = -7 \mod 43$

$\Rightarrow 39! = 36 \mod 43$ #