2、

(a)

1、 $N+M-1 = 1499 \Rightarrow$ choose $N = 1680$

needed real mulitiplication $= 2\times 10420 + 3\times 1680 = 25880$

2、 direct $= 3\times N\times M = 1080000$

3、 Sectioned convolution $=$ select $L_0 = 600$ $\quad P_0 = L_0 + M - 1 = 899$

$MUL_{840} = 4580$ $\quad MUL_{1008} = 5356$ $\quad MUL_{560} = 3100$

$\downarrow$ $\qquad\qquad \downarrow$ $\qquad\qquad \downarrow$

$P=840$ $L=541$ $\quad P=1008$ $L=709$ $\quad P=560$ $L=261$

$S=3$ $\qquad S=2$ $\qquad S=5$

$3(2MUL + 3\times 541)$ $\quad 2(MUL\times 2 + 3\times 709)$ $\quad 5(MUL\times 2 + 3\times 560)$

$= 32349$ $\qquad = 25678$ $\qquad = 39400$

$\Uparrow$

best

(i) sectioned convolution with $L = 709$

(ii) $N = 1008$ pts.

(iii) 25678 times multiplication

(b) 1、 direct: $3\times N\times M = 108000$

2、 non-sectioned: $N+M-1 = 1229 \Rightarrow$ choose $N = 1260$

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

3. Sectioned: $L_0 = 174 \Rightarrow P = 203 \Rightarrow$ choose $P = 168, 192, 204, 240$

$P = 168 \Rightarrow L = 139 \Rightarrow S = 9 \Rightarrow 9(2MUL_{168} + 3\times 168) = 14976$#

$P = 192 \Rightarrow L = 163 \Rightarrow S = 8 \Rightarrow 8(2MUL_{192} + 3\times 192) = 16640$

$P = 204 \Rightarrow L = 175 \Rightarrow S = 7 \Rightarrow 7(2MUL_{204} + 3\times 204) = 20720$

$P = 240 \Rightarrow L = 211 \Rightarrow S = 6 \Rightarrow 6(2MUL_{240} + 3\times 240) = 15600$

(i) sectioned convolution with $L = 139$ (ii) 168 pts (iii) 14976 times

(c)

1. direct: $3 \times N \times M = 28800$

2. non-sectioned: $N+M-1 = 1207$ choose $N = 1260 \Rightarrow 19060$ same as (b)

3. Sectioned: $L_0 = 30$ $P = 37 \Rightarrow$ choose $P = 36, 40$

$P = 36 \Rightarrow L = 29 \Rightarrow S = 42 \Rightarrow 42(2\,MUL_{36} + 3 \times 36) = 9912$ #

$P = 40 \Rightarrow L = 33 \Rightarrow S = 37 \Rightarrow 37(2\,MUL_{40} + 3 \times 40) = 11840$

(i) sectioned convolution with $L = 29$ (ii) 36 pts (iii) 9912 times #

(d)

1. $3 \times N \times M = 3600$ #

2. non-sectioned: $N+M-1 = 1201$ choose $N = 1260 \Rightarrow 19060$ same as (b)

3. sectioned: $L_0 = 2 \Rightarrow P = 3$ choose $P = 4$ $(MUL_4 = 0)$

$P = 4 \Rightarrow L = 3 \Rightarrow S = 400 \Rightarrow 400(2 \cdot 0 + 3 \cdot 4) = 4800$

(i) Direct (ii) no FFT is needed (iii) 3600 times #

3.

(a)

2^k pts $\Rightarrow$ 2^k by 2^k matrix with half 1 & half -1

$\Rightarrow$ 2^{2k-1} 1s & 2^{2k-1} -1 s #

(b)

2^k pts $\Rightarrow$ $1 \times (2^k$ continuous ones$)$

$+ 1 \times (2^{k-1}$ continuous ones$)$

$2 \times (2^{k-2}$ continuous ones$)$

$\vdots$

$+ 2^{k-1} \cdot (1$ one$)$

$\Rightarrow 2^k + (k-1) \cdot 2^{k-1} = (k+1) 2^{k-1}$ ones #

$+ 1 \times (2^{k-1}$ continuous negative ones$)$

$2 \times (2^{k-2}$ continuous negative ones$)$

$\vdots$

$+ 2^{k-1} \cdot (1$ negative one$)$

$\Rightarrow (k-1) 2^{k-1}$ negative ones #

rest are zeros $\Rightarrow$ $2^{2k} - (k+1+k-1) 2^{k-1} = 2^{2k} - k \cdot 2^k$ zeros #

(c)

Walsh Transform is widely used in error detection and correction in CDMA.

(d) Haar transform is highly beneficial for image compression.

4、

(a)

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

$\xrightarrow[\text{of 16-pts Walsh}]{\text{modulated by } 1^{st} \text{ row}}$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

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

$\xrightarrow[\text{of 16-pts Walsh}]{\text{modulated by } 4^{th} \text{ row}}$

$$\begin{bmatrix} 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \end{bmatrix}$$

$[0\ 1\ 1] \Rightarrow [-1\ 1\ 1]$

$\xrightarrow[\text{of 16-pts Walsh}]{\text{modulated by } 10^{th} \text{ row}}$

$$\begin{bmatrix} -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \end{bmatrix}$$

combine

$$\begin{bmatrix} 1 & 1 & -1 & 3 & 1 & 1 & -1 & 3 & 3 & -1 & 1 & 1 & 3 & -1 & 1 & 1 \\ 1 & -3 & -1 & -1 & 1 & -3 & -1 & -1 & -1 & -1 & -3 & 1 & -1 & -1 & -3 & 1 \\ 1 & 1 & 3 & -1 & 1 & 1 & 3 & -1 & -1 & 3 & 1 & 1 & -1 & 3 & 1 & 1 \end{bmatrix}$$

(b)

$$
\begin{bmatrix}
1 & 1 & -1 & 3 & 1 & 1 & \overset{(-1)}{*} & 3 & 3 & -1 & 1 & 1 & 3 & -1 & 1 & 1 \\
1 & -3 & \overset{(-1)}{*} & -1 & 1 & -3 & -1 & -1 & -1 & -1 & -3 & 1 & -1 & -1 & -3 & 1 \\
1 & 1 & 3 & -1 & 1 & 1 & 3 & -1 & -1 & 3 & 1 & 1 & -1 & 3 & 1 & 1
\end{bmatrix}
$$

for [1 0 1]

inner product may be $\frac{17 \pm 3}{16} > 0 \Rightarrow 1$ for index 1-16

inner product may be $\frac{-15 \pm 3}{16} < 0 \Rightarrow -1$ for index 17-32

inner product may be $\frac{16}{16} > 0 \Rightarrow 1$ for index 33-48

$\Rightarrow$ we can solve [1 0 1] out of this noised signal

for [1 1 0]

inner product may be $\frac{15 \pm 3}{16} > 0 \Rightarrow 1$ for index 1-16

inner product may be $\frac{17 \pm 3}{16} > 0 \Rightarrow 1$ for index 17-32

inner product may be $\frac{-16}{16} < 0 \Rightarrow -1$ for index 33-48

$\Rightarrow$ we can solve [1 1 0] out of this noised signal

for [0 1 1]

inner product may be $\frac{-15 \pm 3}{16} < 0 \Rightarrow -1$ for index 1-16

inner product may be $\frac{17 \pm 3}{16} > 0 \Rightarrow 1$ for index 17-32

inner product may be $\frac{16}{16} > 0 \Rightarrow 1$ for index 33-48

$\Rightarrow$ we can solve [0 1 1] out of this noised signal

we can recover all three data since we use 16 dimensions to send 3 dimension data.

It is trivially that we can endure bit loss but also send the data correctly.

5.

$fft(x) = [\, 4 \;\; 0 \;\; 2 \;\; 0 \;\; -2 \;\; 0 \;\; -4 \;\; 0 \;\; -2 \;\; 0 \;\; 2 \;\; 0 \,]$

$\Rightarrow F_x = [\, 4 \;\; 0 \;\; 2 \;\; 0 \;\; 9 \;\; 0 \;\; 5 \;\; 0 \;\; 9 \;\; 0 \;\; 2 \;\; 0 \,]$ since $fft(x) \bmod 11 = F_x$

6.

$3^{2049} \bmod 103$

by Fermat's little theorem, $3^{102} \bmod 103 = 1$ since 103 is a prime number

$3^{2049} \bmod 103 = 3^{(102)\times 20} \cdot 3^{9} \bmod 103 = 3^{9} \bmod 103$

$= 10 \bmod 103$

(b)

$2881 = 43 \cdot 67$

$X \bmod 43 = 2$ $\quad X = 43a + 2$ $\quad$ a is an integer

$X \bmod 67 = 43a + 2 \bmod 67 = 13$

$43a \bmod 67 = 11 \Rightarrow a \bmod 67 = 43^{-1} \cdot 11 \bmod 67$

$= 53 \cdot 11 \bmod 67$

$= 47$

$\Rightarrow a \bmod 67 = 47 \Rightarrow a = 67b + 47$ $\quad$ b is an integer

$\Rightarrow X = 43 \cdot (67b + 47) + 2$

$= 2881b + 2023$

$\Rightarrow X \bmod 2881 = 2023$ #

(c)

By Wilson's Theorem, since 43 is a prime number, $42! = -1 \bmod 43$

$= 42 \bmod 43$

$\Rightarrow 41! \bmod 43 = 42 \times 42^{-1} \bmod 43 = 1 \bmod 43$

$39! \bmod 43 = (40 \cdot 41)^{-1} \bmod 43 = 6^{-1} \bmod 43$

$= 36 \bmod 43$ #

Special Question (3, 8)

$p = 48$, $L = 41$, $S = 13$

$\Rightarrow 13(2 \times \underbrace{MUL_{48}}_{92} + 3 \times 48) = 4264$ #

(1)

驗證 fftreal(x,y) 是否等價 fft(x), fft(y)

使用 x= 1:10 y= 11:20

得 [XX, YY] = fftreal(x,y) X = fft(x) Y = fft(y)

輸出如圖，得證等價 #

```
X =

 Columns 1 through 4

 55.0000 + 0.0000i  -5.0000 +15.3884i  -5.0000 + 6.8819i  -5.0000 + 3.6327i

 Columns 5 through 8

 -5.0000 + 1.6246i  -5.0000 + 0.0000i  -5.0000 - 1.6246i  -5.0000 - 3.6327i

 Columns 9 through 10

 -5.0000 - 6.8819i  -5.0000 -15.3884i

XX =

 Columns 1 through 4

 55.0000 + 0.0000i  -5.0000 +15.3884i  -5.0000 + 6.8819i  -5.0000 + 3.6327i

 Columns 5 through 8

 -5.0000 + 1.6246i  -5.0000 + 0.0000i  -5.0000 - 1.6246i  -5.0000 - 3.6327i

 Columns 9 through 10

 -5.0000 - 6.8819i  -5.0000 -15.3884i
```

```
  1.0e+02 *

 Columns 1 through 8

  1.5500 + 0.0000i  -0.0500 + 0.1539i  -0.0500 + 0.0688i  -0.0500 + 0.0363i  -0.0500 + 0.0162i  -0.0500 + 0.0000i  -0.0500 - 0.0162i  -0.0500 - 0.0363i

 Columns 9 through 10

 -0.0500 - 0.0688i  -0.0500 - 0.1539i

YY =

  1.0e+02 *

 Columns 1 through 8

  1.5500 + 0.0000i  -0.0500 + 0.1539i  -0.0500 + 0.0688i  -0.0500 + 0.0363i  -0.0500 + 0.0162i  -0.0500 + 0.0000i  -0.0500 - 0.0162i  -0.0500 - 0.0363i

 Columns 9 through 10

 -0.0500 - 0.0688i  -0.0500 - 0.1539i
```