姓名:胡劭 系級:資工碩一 學號:M11215075

1. Answer the following questions:

   (a) Compute the DFT of the vector (0, 1, 2, 3).

   (b) Show how Iterative-FFT computes the DFT of the input vector $(0, 2, 3, -1, 4, 5, 7, 9)$.

a. $X[m] = \sum_{n=0}^{N-1} x[n] e^{j\frac{2\pi m n}{N}} \longrightarrow \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & j & -1 & -j \\ 1 & -1 & 1 & -1 \\ 1 & -j & -1 & j \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 6 \\ -2j-2 \\ -2 \\ 2j-2 \end{bmatrix}$

$x[n] = \begin{bmatrix} 0 \\ 1 \\ 2 \\ 3 \end{bmatrix} \rightarrow N = 4$

$X[0] = x[0] + x[1] + x[2] + x[3]$
$= 0 + 1 + 2 + 3 = 6$

$X[1] = 0 + x[1] e^{j\frac{2}{4}\pi} + x[2] e^{j\frac{4}{4}\pi} + x[3] e^{j\frac{6}{4}\pi} \quad (e^{j\theta} = \cos\theta + j\sin\theta)$
$= 0 + e^{j\frac{\pi}{2}} + 2e^{j\pi} + 3e^{j\frac{3}{2}\pi}$
$= \cos(\frac{\pi}{2}) + j\sin(\frac{\pi}{2}) + 2(\cos(\pi) + j\sin(\pi)) + 3(\cos(\frac{3}{2}\pi) + j\sin(\frac{3}{2}\pi))$
$= j + 2(-1) - 3j = -2j - 2$

$X[2] = 0 + 1e^{j\pi} + 2e^{j2\pi} + 3e^{j3\pi}$
$= \cos(\pi) + j\sin(\pi) + 2(\cos(2\pi) + j\sin(2\pi)) + 3(\cos(3\pi) + j(3\pi))$
$= -1 + 2 + -3 = -2$

$X[3] = 0 + 1e^{j\frac{3}{2}\pi} + 2e^{j3\pi} + 3e^{j\frac{9}{2}\pi}$
$= \cos(\frac{3}{2}\pi) + j\sin(\frac{3}{2}\pi) + (-2) + 3(\cos(\frac{9}{2}\pi) + j\sin(\frac{9}{2}\pi))$
$= -j - 2 + 3j = 2j - 2$

$\therefore$ 對 $\begin{bmatrix} 0 \\ 1 \\ 2 \\ 3 \end{bmatrix}$ 做DFT為 $\begin{bmatrix} 6 \\ -2-2j \\ -2 \\ -2+2j \end{bmatrix}$ #

b. 先做 Bit-Reverse $(0,4,3,7,2,5,-1,9)$

$s=1,\ m=2^1=2,\ W_2=e^{2\pi\frac{i}{2}}=-1$

step $=2$

$k=0,\ w=1,\ j=0:\ t=wA[1]=4,\ u=A[0]=0,\ A[0]=4,\ A[1]=-4$

$k=2,\ w=1,\ j=0:\ t=wA[3]=7,\ u=A[2]=3,\ A[2]=10,\ A[3]=-4$

$k=4,\ w=1,\ j=0:\ t=wA[5]=5,\ u=A[4]=2,\ A[4]=7,\ A[5]=-3$

$k=6,\ w=1,\ j=0:\ t=wA[7]=9,\ u=A[6]=-1,\ A[6]=8,\ A[7]=-10$

$$A=[4,-4,10,-4,7,-3,8,-10]$$

$s=2,\ m=4,\ W_4=e^{\frac{2\pi i}{4}}=e^{\frac{1}{2}\pi i}=i$

step $=4$

$k=0,\ w=1,\ j=0:\ t=wA[2]=10,\ u=A[0]=4,\ A[0]=14,\ A[2]=-6$

$k=0,\ w=i,\ j=1:\ t=wA[3]=-4i,\ u=A[1]=-4,\ A[1]=-4-4i,\ A[3]=-4+4i$

$k=4,\ w=1,\ j=0:\ t=wA[6]=8,\ u=A[4]=7,\ A[4]=15,\ A[6]=-1$

$k=4,\ w=i,\ j=1:\ t=wA[7]=-10i,\ u=A[5]=-3,\ A[5]=-3-10i,\ A[7]=-3+10i$

$$A=[14,-4-4i,-6,-4+4i,15,-3-10i,-1,-3+10i]$$

$s=3,\ m=8,\ W_8=e^{2\pi i/8}=\cos(\frac{\pi}{4})+i\sin(\frac{\pi}{4})=\frac{1}{\sqrt{2}}+\frac{i}{\sqrt{2}}$

step $=8$

$k=0,\ w=1,\ j=0:\ t=wA[4]=15,\ u=A[0]=14,\ A[0]=29,\ A[4]=-1$

$k=0,\ w=\frac{1}{\sqrt{2}}+\frac{i}{\sqrt{2}},\ j=1:\ t=wA[5]=\frac{7}{\sqrt{2}}-\frac{13i}{\sqrt{2}},\ u=A[1]=-4-4i,\ A[1]=-4-4i+\frac{7}{\sqrt{2}}-\frac{13i}{\sqrt{2}}$

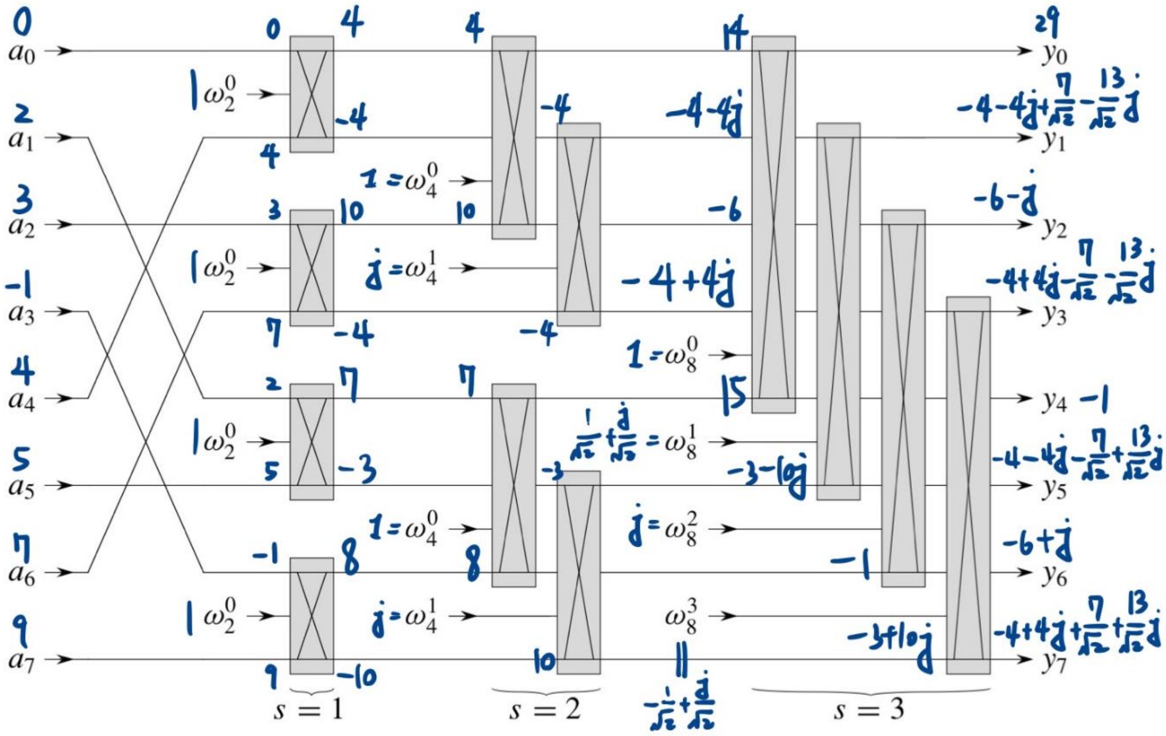
$A[5]=-4-4i-\frac{7}{\sqrt{2}}+\frac{13}{\sqrt{2}}i$

$k=0,\ w=i,\ j=2:\ t=wA[6]=-i,\ u=A[2]=-6,\ A[2]=-6-i,\ A[6]=-6+i$

$k=0,\ w=\frac{i}{\sqrt{2}}-\frac{1}{\sqrt{2}},\ j=3:\ t=wA[7]=\frac{-7}{\sqrt{2}}-\frac{13i}{\sqrt{2}},\ u=A[3]=-4+4i,\ A[3]=-4+4i-\frac{7}{\sqrt{2}}-\frac{13}{\sqrt{2}}i$

$A[7]=-4+4i+\frac{7}{\sqrt{2}}+\frac{13}{\sqrt{2}}i$

$$A=(29,-4-4i+\frac{7}{\sqrt{2}}-\frac{13}{\sqrt{2}}i,-6-i,-4+4i-\frac{7}{\sqrt{2}}-\frac{13}{\sqrt{2}}i,-1,-4-4i-\frac{7}{\sqrt{2}}+\frac{13}{\sqrt{2}}i,-6+i,-4+4i+\frac{7}{\sqrt{2}}+\frac{13}{\sqrt{2}}i)$$



a_0 0
a_1 2
a_2 3
a_3 -1
a_4 4
a_5 5
a_6 7
a_7 9
$1\ \omega_2^0$
$1 = \omega_4^0$
$j = \omega_4^1$
$1 = \omega_8^0$
$\frac{1}{\sqrt{2}} + \frac{j}{\sqrt{2}} = \omega_8^1$
$j = \omega_8^2$
ω_8^3
$-\frac{1}{\sqrt{2}} + \frac{j}{\sqrt{2}}$
0 4 -4 4
3 10 7 -4
2 7 5 -3
-1 8 9 -10
4 -4 10 -4
7 -3 8 10
14 $-4-4j$ -6 $-4+4j$ 15 $-3-10j$ -1 11 $-3+10j$
y_0 29
y_1 $-4-4j+\frac{7}{\sqrt{2}}-\frac{13}{\sqrt{2}}j$
y_2 $-6-j$
y_3 $-4+4j-\frac{7}{\sqrt{2}}-\frac{13}{\sqrt{2}}j$
y_4 -1
y_5 $-4-4j-\frac{7}{\sqrt{2}}+\frac{13}{\sqrt{2}}j$
y_6 $-6+j$
y_7 $-4+4j+\frac{7}{\sqrt{2}}+\frac{13}{\sqrt{2}}j$
$s = 1$
$s = 2$
$s = 3$

2. Consider the product of two polynomials as follows and answer the following questions:

$$A(x) = 4x - 5$$
$$B(x) = 10x + 9$$

(a) Find $C(x) = A(x)B(x)$ with the conventional method.

(b) Find the product with the DFT/IDFT method.

(c) Verify your results.

(a)

	4	-5		
9	10			40
	9	10		-14
		9	10	-45

$$C(x) = (4x-5)(10x+9)$$
$$= 40x^2 + 36x - 50x - 45$$
$$\Rightarrow \quad = 40x^2 - 14x - 45$$

$$\begin{array}{rrrr} & & 4x & -5 \\ \times & & 10x & +9 \\ \hline & & 36x & -45 \\ & 40x^2 & -50x & \\ \hline & 40x^2 & -14x & -45 \end{array} \quad \#$$

(b) $x[n] \xrightarrow{DFT} X[m] \rightarrow Y[m] = X[m]H[m] \xrightarrow{IDFT} y[n]$

$h[n] \xrightarrow{DFT} H[m]$

$C[m] = A[m] * B[m]$

$A[n] = \begin{bmatrix} -5 \\ 4 \\ 0 \\ 0 \end{bmatrix} \Rightarrow DFT(A) \Rightarrow$

$A[0] = -5 + 4 + 0 + 0 = -1$

$A[1] = -5 + 4e^{j\frac{2\pi}{4}} = -5 + 4\left(\cos(\frac{\pi}{2}) + j\sin(\frac{\pi}{2})\right) = -5 + 4j$

$A[2] = -5 + 4e^{j\frac{4}{4}\pi} = -5 - 4 = -9$

$A[3] = -5 + 4e^{j\frac{6}{4}\pi} = \cos(\frac{3}{2}\pi) + j\sin(\frac{3}{2}\pi) - 5$

$= -5 - 4j$

$B[n] = \begin{bmatrix} 9 \\ 10 \\ 0 \\ 0 \end{bmatrix} \Rightarrow DFT(B) \Rightarrow$

$B[0] = 9 + 10 = 19$

$B[1] = 9 + 10e^{j\frac{2\pi}{4}} = 9 + 10j$

$B[2] = 9 + 10e^{j\pi} = -1$

$B[3] = 9 + 10e^{j\frac{2}{3}\pi} = 9 - 10j$

$$A[m] * B[m] = \begin{bmatrix} -19 \\ -85 - 14j \\ 9 \\ -85 + 14j \end{bmatrix} = C[m]$$

$IDFT(C[m]) \Rightarrow C[0] = \frac{1}{4}(-19 - 85 - 14j + 9 - 85 + 14j) = -45$

$C[1] = \frac{1}{4}(-19 + (-85 - 14j)e^{-j\frac{2\pi}{4}} + 9e^{-j\frac{4\pi}{4}} + (-85 + 14j)e^{-j\frac{6\pi}{4}} = -14$

$C[2] = \frac{1}{4}(-19 + (-85 - 14j)e^{-j\frac{4\pi}{4}} + 9e^{-j\frac{8\pi}{4}} + (-85 + 14j)e^{-j\frac{12\pi}{4}} = 40$

$C[3] = \frac{1}{4}(-19 + (-85 - 14j)e^{-j\frac{6}{4}\pi} + 9e^{-j\frac{12}{4}\pi} + (-85 + 14j)e^{-j\frac{18\pi}{4}} = 0$

step 1 : Double-degree bound

$$A(x) = (-5, 4, 0, 0)$$

$$B(x) = (9, 10, 0, 0)$$

$$\quad\;\; x^0 \;\; x^1 \;\; x^2 \;\; x^3$$

step 2 : Discrete Fourier transform

$$\begin{array}{l} W_4^0 = 1 \\ W_4^1 = j \\ W_4^2 = -1 \\ W_4^3 = -j \end{array} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & j & -1 & -j \\ 1 & -1 & 1 & -1 \\ 1 & -j & -1 & j \end{bmatrix} \begin{bmatrix} -5 \\ 4 \\ 0 \\ 0 \end{bmatrix} = (-1, -5+4j, -9, -5-4j)$$

$$\begin{array}{l} W_4^0 = 1 \\ W_4^1 = j \\ W_4^2 = -1 \\ W_4^3 = -j \end{array} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & j & -1 & -j \\ 1 & -1 & 1 & -1 \\ 1 & -j & -1 & j \end{bmatrix} \begin{bmatrix} 9 \\ 10 \\ 0 \\ 0 \end{bmatrix} = (19, 9+10j, -1, 9-10j)$$

step 3: Multiply values at roots

$$\begin{array}{r} (-1, -5+4j, -9, -5-4j) \\ \times \; (19, 9+10j, -1, 9-10j) \\ \hline (-19, -85-14j, 9, -85+14j) \end{array}$$

$$(a+jb)(c+jd)$$
$$= ac + j(bc+ad) - bd$$
$$= (ac-bd) + j(bc+ad)$$

step4 : Inverse discrete Fourier transform

$$\frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -j & -1 & j \\ 1 & -1 & 1 & -1 \\ 1 & j & -1 & -j \end{bmatrix} \begin{bmatrix} -19 \\ -85-14j \\ 9 \\ -85+14j \end{bmatrix} = (-45, -14, 40, 0)$$

$$C(x) = A(x)B(x) = 40x^2 - 14x - 45 \;\#$$

C.由 a 跟 b 得知，不論是 conventional 方法還是 DFT/IDFT 方法，兩者得出的

答案相同。

3. Considering an RSA key set with $p = 11$, $q = 29$, $n = 319$, and $e = 3$, answer the following questions:

(a) What value of d should be used in the secret key?

(b) Compute the ciphertext $P(M)$, where $M = 100$ with the public key.

(c) Compute the message M from the ciphertext with the secret key.

(d) Verify their results.

$n = p \times q = 11 \times 29 = 319$

$\gcd(e, \phi(n)) = 1 \quad \phi(n) = 10 \times 28 = 280$

$C = m^3 \bmod 319$

(a) $d \to ed \equiv 1 \bmod 280$

$d = 187$ #

(b) $P(100) = M^e \bmod n \Rightarrow 100^3 \bmod 319 \equiv 254$

(c) $S(C) = C^d \bmod n = 254^{187} \bmod 319 \equiv 100$

i	7	6	5	4	3	2	1	0
b_i	1	0	1	1	1	0	1	1
d	254	78	100	122	67	23	67	100

(d) Proof: $m = C^d \% n$

已知 $m < n$, $C^d \% n - m = 0 = (m^e \% n)^d \% n - m$

$\Rightarrow m^{ed} \% n - m = m^{k(P-1)(q-1)+1} \% n - m \; (ed \equiv 1 \bmod \phi(n) \Rightarrow ed = k\phi(n)+1, k \in R)$

$= m(m^{k(P-1)(q-1)} - 1) \% n$

$\because a^{P-1} \equiv 1 \pmod P \Rightarrow (m^{k(P-1)})^{q-1} \equiv 1 \pmod q \Rightarrow (m^{k(q-1)})^{P-1} \equiv 1 \pmod p$

$\Rightarrow m^{k(p-1)(q-1)} \equiv 1 \pmod{pq} \Rightarrow m^{k(p-1)(q-1)} \equiv 1 \pmod n$

$\therefore m(m^{k(p-1)(q-1)} - 1) \% n = m(1-1) \% n = 0$，$\therefore$(C)(d)結果會一致 #QED