Homework for section 6B (approximate due date: Oct 5th, 2020)

Question 1:

Pick two prime numbers p and q (between 5 and 37), N=pq;

Use Shor algorithm to find p and q from N:

a) Pick a number ***a*** smaller than N

b) Find the integer **r** verifying **f(r)** = $\mathbf{a^r}$ **mod N**

c) If r odd find a different ***a***

d) Compute $\mathbf{a^{r/2} - 1}$ and $\mathbf{a^{r/2} + 1}$

e) If the gcd is not uncovering **p**, and **q**, pick a different ***a***

Answer:

Taking p and q between 5 and 37:

p = 7, q = 11

so, N = p * q = 7 * 11 = 77

a)

Taking a = 12

b)

Finding integer r verifying **f(r)** = $\mathbf{a^r}$ **mod N**

r	0	1	2	3	4	5	6	7	8	9	10
f(r)	1	12	67	34	23	45	1	12	67	34	23

c)

Pick r = 6 (not odd)

$a^r = 12^6$

2985984 mod 77 ≡ 1 mod 77

d)

$a^{r/2} = 12^{6/2}$

$f(r) \equiv 12^{6/2} \bmod 77$

$f(r) \equiv 1728 \bmod 77$

$\equiv 34 \bmod 77$

Then,

$a^{r/2} - 1 = 34 - 1 = 33$

$a^{r/2} + 1 = 35$

e)

$p = \gcd(a^{r/2} - 1, N)$

$= \gcd(33, 77) \Rightarrow 11$

$q = \gcd(a^{r/2} + 1, N)$

$= \gcd(35, 77) \Rightarrow 7$

$N = 7 * 11 = 77$

Hence, p and q has been uncovered

Question 2:

Find the Discrete Fourier Transform (DFT) matrix for N=2, then for N=4:

$$\text{DFT} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & w & w^2 & w^3 & \dots & w^{N-1} \\ 1 & w^2 & w^4 & w^6 & \dots & w^{2N-2} \\ 1 & w^2 & w^6 & w^9 & \dots & w^{3N-3} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & w^{N-1} & w^{2N-2} & w^{3N-3} & \dots & w^{(N-1)(N-1)} \end{pmatrix}$$

$w = e^{2\pi i/N}$

Answer:

DFT for N=2 in matrix form:

$w = e^{2\pi i/N}$ => cos(2π/N) + i sin(2π/N)

$\text{DFT}_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 \\ 1 & w \end{pmatrix}$

$w^1 = e^{2\pi i/2}$ => $e^{\pi i}$ => cos(π) + I sin(π) => -1 + 0 => -1

$\text{DFT}_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & w \end{pmatrix}$ => $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

DFT for N=4 in matrix form:

$\text{DFT}_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \text{w\^1} & w\text{\^2} & w\text{\^3} \\ 1 & w\text{\^2} & w\text{\^4} & w\text{\^6} \\ 1 & w\text{\^3} & w\text{\^6} & w\text{\^9} \end{pmatrix}$

$\text{DFT}_4 = \frac{1}{\sqrt{4}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \text{w\^1} & w\text{\^2} & w\text{\^3} \\ 1 & w\text{\^2} & w\text{\^4} & w\text{\^6} \\ 1 & w\text{\^3} & w\text{\^6} & w\text{\^9} \end{pmatrix}$

$\text{DFT}_4 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \text{i} & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$