**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:

* + 1. Pick a number ***a*** smaller than N
    2. Find the integer **r** verifying  **mod N**
    3. If r odd find a different ***a***
    4. Compute and
    5. 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  **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)

ar = 126

2985984 mod 77 ≡ 1 mod 77

**d)**

ar/2 = 126/2

126/2 mod 77

1728 mod 77

≡ 34 mod 77

Then,

ar/2 -1 = 34 -1 = 33

ar/2 + 1 = 35

**e)**

p = gcd( ar/2 -1 , N)

= gcd(33, 77) => 11

q = gcd( ar/2 + 1 , N)

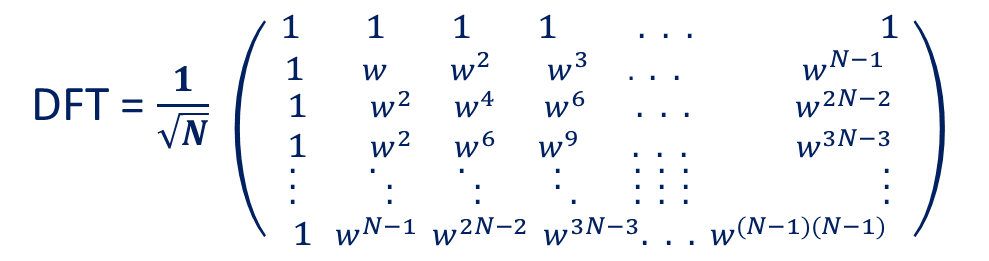
= gcd(35, 77) => 7

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:



**=**

**Answer:**

**DFT for N=2 in matrix form:**

𝑤 = 𝑒 2πi/N => cos(2π/N) + i sin(2π/N)

DFTN =

w1 = 𝑒 2πi/2 => eπi => cos(π) + I sin(π) => -1 + 0 => -1

DFT2 = =>

**DFT for N=4 in matrix form:**

DFTN =

DFT4 =

DFT4 =