Vinayak Pai ; 2nd sem ;
19094R003 ; CSIS
Vinayak Pai 24-05-2020

$N = 15$

Step 1: choose x

$x = 7$, $GCD(7, 15) = 1$

Step 2: Determine q

$n^2 < q = 2^t < 2n^2$

$225 < 2^t < 450$

$q = 256$

Step 3 : Initialize first register

$$|\phi\rangle = \frac{1}{\sqrt{256}} \sum_{a=0}^{255} |a\rangle |0\rangle$$

Step 4: Initialize second register

$$|\phi_1\rangle = \frac{1}{\sqrt{256}} \sum_{a=0}^{255} |a\rangle |7^a \pmod{15}\rangle$$

$$|\phi_1\rangle = \frac{1}{\sqrt{256}} \sum_{a=0}^{255} |0\rangle|1\rangle \; |1\rangle|7\rangle \; |2\rangle|4\rangle \; |3\rangle|13\rangle \; |4\rangle|1\rangle \; |5\rangle|7\rangle \; |6\rangle|4\rangle \; |7\rangle|13\rangle$$

Hence period = 4

Step 5 : check r

r is even

$x^{r/2} \bmod n \neq -1$

Factors are

$(x^{r/2} + 1 \bmod 15, N) = (7^2 + 1 \bmod 15, 15) = (5, 15) = 5$

$(x^{r/2} - 1 \bmod 15, N) = (7^2 - 1 \bmod 15, 15) = (3, 15) = 3$

∴ Factors are 5 and 3