Quiz-6 Quantum Computing

Time: 10 minutes

Marks: 10

1. Demonstrate all the steps (except quantum order finding) Shor's integer factorization for N=143. Please make sure not to choose a random number which is already a factor of it. [10 Marks]

   Solution: No solution is given as multiple solutions based on different value of random x are possible.

2. Demonstrate all the steps (except quantum order finding) Shor's integer factorization for N=143. Please choose a random number $x = 5$. [10 Marks]

   Solution:

   (a) Choose random $x = 5$

   (b) Check if x is a factor of N by pure luck. To that end, compute $GCD(143, 5) = GCD(4, 143 \mod 5) = GCD(4, 3) = GCD(3, 4 \mod 3) = GCD(3, 1) = GCD(1, 0) = 1$. Hence x is not a factor of N.

   (c) We calculate r, such that $x^r \equiv 1 \mod n$

$$
\begin{aligned}
5^1 &\equiv 5 \mod 143\\
5^2 &\equiv 25 \mod 143\\
5^3 &\equiv 125 \mod 143\\
5^4 &\equiv 53 \mod 143\\
5^5 &\equiv 53 * 5 \equiv 122 \mod 143\\
5^6 = 5^4 \times 5^2 &\equiv 53 \times 25 \equiv 38 \mod 143\\
5^7 = 5^6 \times 5 &\equiv 38 \times 5 \equiv 47 \mod 143\\
5^8 = 5^7 \times 5 &\equiv 47 \times 5 \equiv 92 \mod 143\\
5^9 = 5^7 \times 5^2 &\equiv 47 \times 25 \equiv 31 \mod 143\\
5^{10} = 5^9 \times 5 &\equiv 31 \times 5 \equiv 12 \mod 143\\
5^{11} = 5^{10} \times 4 &\equiv 12 \times 5 \equiv 60 \mod 143\\
&\cdots\\
5^{20} = 5^{10} \times 5^{10} &\equiv 12 \times 12 \equiv 1 \mod 143
\end{aligned}
$$

   So our $r = 18$

   (d) Check if our r is even. It is even. Check if $GCD(5^{10} - 1, 143) = 1$ if not then our one factor is that GCD.

$GCD(9765624, 143) = GCD(143, 9765624 \mod 143) = GCD(11, 143 \mod 11) = GCD(11, 0) = 11$. This shows our one factor say $p = 11$. The our other factor $q = \frac{N}{p} = 13$

3. Demonstrate all the steps (except quantum order finding) Shor's integer factorization for N=247. Please choose a random number $x = 3$. [10 Marks]

   Solution:

   (a) Choose random $x = 3$

   (b) Check if x is a factor of N by pure luck. To that end, compute $GCD(247, 3) = GCD(3, 247 \mod 3) = GCD(3, 1) = GCD(1, 0) = 1$. Hence x is not a factor of N.

   (c) We calculate r, such that $x^r \equiv 1 \mod n$

$$
\begin{aligned}
3^1 &\equiv 3 \mod 247 \\
3^2 &\equiv 9 \mod 247 \\
3^3 &\equiv 27 \mod 247 \\
3^4 &\equiv 81 \mod 247 \\
3^5 &\equiv 243 \mod 247 \\
3^6 &\equiv 235 \mod 247 \\
3^7 &\equiv 211 \mod 247 \\
3^8 &\equiv 139 \mod 247 \\
3^9 &\equiv 170 \mod 247 \\
&\dots \\
3^{18} = 3^9 \times 3^9 &\equiv 1 \mod 247
\end{aligned}
$$

   So our $r = 18$

   (d) Check if our r is even. It is even. Check if $GCD(3^9 - 1, 247) = 1$ if not then our one factor is that GCD.

   $GCD(19682, 247) = GCD(247, 19682 \mod 247) = GCD(169, 247) = GCD(169, 247 \mod 169) = GCD(78, 169) = GCD(13, 78) = GCD(13, 0) = 13$

   It shows that our one factor say $p = 13$. We can find our other factor $q = \frac{N}{p} = 19$