Quantum Computing - Solutions 9

Abbas Edalat

1. Find the regular continued fraction expansion of 37/17.

Solution:

$$\begin{aligned}\tfrac{37}{17} &= 2+\tfrac{3}{17} = 2+\tfrac{1}{\frac{17}{3}}\\ &= 2+\tfrac{1}{5+\frac{2}{3}} = 2+\tfrac{1}{5+\frac{1}{\frac{3}{2}}}\\ &= 2+\tfrac{1}{5+\frac{1}{1+\frac{1}{2}}}\end{aligned}$$

It follows that $\frac{37}{17} = [2,5,1,2]$.

2. Show by induction that

$$p_{j-1}q_j - q_{j-1}p_j = (-1)^j$$

and deduce that $\gcd(p_j, q_j) = 1$.

Solution: For $j = 1$ we have:

$$p_0q_1 - q_0p_1 = a_0a_1 - 1 \times (1 + a_0a_1) = -1,$$

which verifies the basic step.

Assume that $p_{j-1}q_j - q_{j-1}p_j = (-1)^j$, then by Proposition 11.8 (page 114) of the lecture notes which expresses p_{j+1} and q_{j+1} in terms of p_j, q_j, p_{j-1} and q_{j-1}, we get:

$$\begin{aligned}p_jq_{j+1} - q_jp_{j+1} &= p_j(a_{j+1}q_j + q_{j-1}) - q_j(a_{j+1}p_j + p_{j-1})\\ &= -p_{j-1}q_j + q_{j-1}p_j = -(-1)^j = (-1)^{j+1},\end{aligned}$$

by the inductive hypothesis.

3. Find $\gcd(231, 315)$.

Solution: We have:

$$\begin{aligned}315 &= (231) \times 1 + 84\\ 231 &= (84) \times 2 + 63\\ 84 &= (63) \times 1 + 21\\ 63 &= (21) \times 3.\end{aligned}$$

Hence, $\gcd(231, 315) = 21$.

4. Consider Shor's algorithm on page 123 of the lecture notes, for factoring 15 with the assumption that in step (i) we choose $x = 13$. Find the order of 13 modulo 15 for step (iii) and verify that step (v) leads to the factorization of 15. Repeat for factoring $N = 91$ with $x = 4$ and for $N = 18$ with $x = 5$.

Solution:

N=15 (i) $x = 13$.

(ii) $\gcd(13, 15) = 1$.

(iii) We find the order of 13 (mod 15). We have:

$$13^2 = (-2)^2 = 4 \pmod{15}$$
$$13^3 = (-2)^3 = -8 = 7 \pmod{15}$$
$$13^4 = (-2)^4 = 16 = 1 \pmod{15}$$

Hence, $r = 4$.

(iv) $r = 4$ is even and $13^2 = (-2)^2 = 4 \neq -1 \pmod{15}$.

(v) $\gcd((13)^{4/2} - 1, 15) = \gcd((13)^2 - 1, 15) = \gcd(168, 15) = 3$

$\gcd((13)^{4/2} + 1, 15) = \gcd((13)^2 + 1, 15) = \gcd(170, 15) = 5$.

Hence, 3 and 5 are factors of 15.

N=91 (i) $x = 4$.

(ii) 91,4 = 1.

(iii) We find the order of 4 modulo 91. We have:

$$4^2 = 16 \pmod{91}$$
$$4^3 = 64 \pmod{91}$$
$$4^4 = 256 = 74 \pmod{91}$$
$$4^5 = 296 = 23 \pmod{91}$$
$$4^6 = 92 = 1 \pmod{91}$$

Hence, $r = 6$.

(iv) We have $4^{6/2} = 4^3 = 64 \neq -1 \pmod{91}$.

(v) $\gcd((4)^{6/2} - 1, 91) = \gcd((4)^3 - 1, 91) = \gcd(63, 91) = 7$

$\gcd((4)^{6/2} + 1, 91) = \gcd(65, 91) = 13$.

Hence, 7 and 13 are factors of 91.

N=18 (i) $x = 5$

(ii) $\gcd(18, 5) = 1$.

(iii) We find the order of 5 (mod 18). We have:

$$5^2 = 25 = 7 \pmod{18}$$
$$5^3 = 45 = -1 \pmod{18}$$
$$5^6 = 1 \pmod{18}$$

Hence, $r = 6$.

(iv) $r = 6$ is even but $5^{6/3} = 5^3 = -1 \pmod{18}$. So this round of the algorithm fails.