

# Quantum Computation

Mathias Niepert

M555

## Homework 9

### Exercise A4.16

$x$  and  $N$  positive Integers and  $x$  co-prime to  $N$

The order of  $x$  modulo  $N$  is defined to be the least positive integer  $r$  such that

$$x^r = 1(\text{mod } N)$$

Because of Theorem A4.9 it is also:

$$x^{\varphi(N)} = 1(\text{mod } N)$$

**Prove that the order  $r$  of  $x$  modulo  $N$  must divide  $\varphi(N)$ .**

Assume  $r$  does not divide  $\varphi(N)$  then one can write:

$$\varphi(N) = kr + l \text{ (with } k, l \in \mathbb{N} \text{ and } l < r \text{) and with that}$$

$$x^{kr+l} = 1(\text{mod } N) \Rightarrow x^{kr} \cdot x^l = 1(\text{mod } N) \Rightarrow (x^r)^k \cdot x^l = 1(\text{mod } N)$$

$$\text{It is } x^r = 1(\text{mod } N) \text{ and thus } (x^r)^k \cdot x^l = 1(\text{mod } N) \equiv x^l = 1(\text{mod } N).$$

This stands in contradiction to the assumption that  $r$  is the order of  $x$  mod  $N$ .

### Exercise A4.18

$$\frac{19}{17} = 1 + \frac{2}{17} = 1 + \frac{1}{\frac{17}{2}} = 1 + \frac{1}{8+\frac{1}{2}}.$$

$$\frac{77}{65} = 1 + \frac{12}{65} = 1 + \frac{1}{\frac{65}{12}} = 1 + \frac{1}{5+\frac{5}{12}} = 1 + \frac{1}{5+\frac{1}{\frac{12}{5}}} = 1 + \frac{1}{5+\frac{1}{2+\frac{2}{5}}} = 1 + \frac{1}{5+\frac{1}{2+\frac{1}{\frac{5}{2}}}} =$$

$$1 + \frac{1}{5+\frac{1}{2+\frac{1}{2+\frac{1}{2}}}}.$$

### Exercise A4.19

$p_0 \equiv a_0, q_0 \equiv 1$  and  $p_1 \equiv 1 + a_0a_1, q_1 \equiv a_1$  and for  $2 \leq n \leq N$ ,

$$\begin{aligned} p_n &\equiv a_n p_{n-1} + p_{n-2} \\ q_n &\equiv a_n q_{n-1} + q_{n-2} \end{aligned}$$

Show that  $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$  for  $n \geq 1$ .

Proof by Induction

Base case:  $n = 1$ :

$$q_1 p_{n-1} - p_n q_{n-1} = q_1 p_0 - p_1 q_0 = a_1 a_0 - (1 + a_0 a_1) = -1 = (-1)^1$$

Induction step:  $n \rightarrow n + 1$

Induction hypothesis:  $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$

To show:  $q_{n+1} p_n - p_{n+1} q_n = (-1)^{n+1}$

$$\begin{aligned} q_n p_{n-1} - p_n q_{n-1} = (-1)^n &\Leftrightarrow p_n q_{n-1} - q_n p_{n-1} = (-1)^{n+1} \Leftrightarrow p_n q_{n-1} - \\ q_n p_{n-1} + q_n a_{n+1} p_n - p_n a_{n+1} q_n &= (-1)^{n+1} \Leftrightarrow p_n (a_{n+1} q_n + q_{n-1}) - q_n (a_{n+1} p_n + \\ p_{n-1}) &= (-1)^{n+1} \end{aligned}$$

It is  $p_{n+1} \equiv a_{n+1} p_n + p_{n-1}$  and  $q_{n+1} \equiv a_{n+1} q_n + q_{n-1}$  and thus:

$$p_n (a_{n+1} q_n + q_{n-1}) - q_n (a_{n+1} p_n + p_{n-1}) = (-1)^{n+1} \Leftrightarrow q_{n+1} p_n - p_{n+1} q_n = (-1)^{n+1} \square$$

For all  $p_n, q_n$  it is either  $q_n p_{n-1} - p_n q_{n-1} = 1$  or  $p_n q_{n-1} - q_n p_{n-1} = 1$  with  $p_{n-1}, q_{n-1}, q_n$  and  $p_n$  are positive integers. Thus:

$$\begin{aligned} q_n \cdot k_1 + p_n \cdot l_1 &= 1 \text{ with } k_1, l_1 \text{ integers } k_1 = p_{n-1}, l_1 = -q_{n-1} \text{ or} \\ q_n \cdot k_2 + p_n \cdot l_2 &= 1 \text{ with } k_2, l_2 \text{ integers } k_2 = -p_{n-1}, l_2 = q_{n-1} \end{aligned}$$

The greatest common divisor of two integers  $q_n$  and  $p_n$  is the least positive integer that can be written in the form  $q_n k + p_n l$ , where  $k$  and  $l$  are integers.  $\square$

### Exercise 5.17

1.  $a, b$  integers and if  $N > 1$  then  $a > 1$ . Thus  $b \leq \lceil \log_2(N) \rceil = L$

2.  $\log_2 N$  and  $2^x$  are computed (with the Taylor expansion of  $\ln x = \frac{x-1}{x} + \frac{1}{2}(\frac{x-1}{x})^2 + \frac{1}{3}(\frac{x-1}{x})^3 + \dots$ ,  $\log_2 x = \ln(x)/\ln(2)$  and  $e^x, 2^x = e^{2\ln 2} = 1 + \frac{x \ln 2}{1!} + \frac{(x \ln 2)^2}{2!} + \dots$ ) which is possible  $\in O(L)$  for the precision we need

( $u_1 \leq 2^x \leq u_2, u_1, u_2$  integers). Division and multiplication are in  $O(L)$   
 $\Rightarrow$  The number of operations is in  $O(L^2)$ .

3. To compute  $u_1^b, u_2^b$  first write  $b$  in binary. E.g.  $b = 10110111 = 183$  then  $x^{183} = x^{10110111} = x^{128}x^{32}x^{16}x^4x^2x^1$  where the powers  $x^2, x^4, x^8, \dots$  are found by successively squaring, then multiplied together – two at a time. This way computes  $x^b$  in at most  $2\log_2(b)$  steps which is in  $O(L)$ . Because the multiplication is in  $O(L)$  it takes  $O(L^2)$  steps.
4. The algorithm can enumerate every possible  $b$  ( $b \leq L$ ) and for every  $b$  do the steps 2 and 3. This is possible in  $O(L \cdot L^2) = O(L^3)$ .

### Exercise 5.18

**N = 91**

1. 91 is not even
2. Test if  $91 = a^b$  with  $a \geq 1, b \geq 2$ .  
 We know that  $b \leq \lceil \log_2(91) \rceil = 7$

$$y = \log_2(91) = 6.5078$$

$$\mathbf{b = 2:} \quad x = \frac{y}{b} = \frac{6.5078}{2} = 3.2539 \Rightarrow 2^x = 9.5394 \Rightarrow u_1 = 9 \text{ and } u_2 = 10.  
 u_1^b = 81 \text{ and } u_2^b = 100.$$

$$\mathbf{b = 3:} \quad x = \frac{y}{b} = \frac{6.5078}{3} = 2.1693 \Rightarrow 2^x = 4.4981 \Rightarrow u_1 = 4 \text{ and } u_2 = 5.  
 u_1^b = 64 \text{ and } u_2^b = 125.$$

$$\mathbf{b = 4:} \quad x = \frac{y}{b} = \frac{6.5078}{4} = 1.6270 \Rightarrow 2^x = 3.0887 \Rightarrow u_1 = 3 \text{ and } u_2 = 4.  
 u_1^b = 81 \text{ and } u_2^b = 256.$$

$$\mathbf{b = 5:} \quad x = \frac{y}{b} = \frac{6.5078}{5} = 1.3016 \Rightarrow 2^x = 2.4650 \Rightarrow u_1 = 2 \text{ and } u_2 = 3.  
 u_1^b = 32 \text{ and } u_2^b = 243.$$

$$\mathbf{b = 6:} \quad x = \frac{y}{b} = \frac{6.5078}{6} = 1.0846 \Rightarrow 2^x = 2.1210 \Rightarrow u_1 = 2 \text{ and } u_2 = 3.  
 u_1^b = 64 \text{ and } u_2^b = 729.$$

$$\mathbf{b = 7:} \quad x = \frac{y}{b} = \frac{6.5078}{7} = 0.9297 \Rightarrow 2^x = 1.9049 \Rightarrow u_1 = 1 \text{ and } u_2 = 2.  
 u_1^b = 1 \text{ and } u_2^b = 128.$$

3.  $4^1 = 4 \pmod{91}$   
 $4^2 = 16 \pmod{91}$   
 $4^3 = 64 \pmod{91}$   
 $4^4 = 74 \pmod{91}$   
 $4^5 = 23 \pmod{91}$

$$4^6 = 1 \pmod{91}$$

$$\Rightarrow r = 6$$

$$x^{r/2} = 64 (\neq -1) \pmod{91}; \gcd(4^3 - 1, 91) = 7$$