

# 1 Introduction

- Problem: find the prime factors of  $N$ .
- Consider  $x$  such that  $1 < x < N$ .
- What to do when  $GCD(x, N) = 1$ ?
- Definition:

$$a \equiv b \pmod{N} \Leftrightarrow (a - b) \mid N.$$

- For  $N = 15$ , consider  $x = 2$ . Then,

$$2^2 \equiv 4 \pmod{15},$$

$$2^3 \equiv 8 \pmod{15},$$

$$2^4 \equiv 1 \pmod{15}.$$

- $(4 - 1 = \underline{3})$  and  $(4 + 1 = \underline{5})$  are factors of 15!

- Definition: the order of  $x$  modulo  $N$  is the least positive integer  $r$  such that

$$x^r \equiv 1 \pmod{N}.$$

- If  $r$  is even, we define  $y$  such that  $x^{r/2} \equiv y$ .

- In this case,

$$(x^{r/2})^2 \equiv y^2 \Rightarrow (1 \equiv y^2) \Rightarrow (y - 1)(y + 1) \equiv 0$$

and

$GCD(y-1, N)$  and  $GCD(y+1, N)$  are factors of  $N$ .

- Example: for  $N = 21$ , consider  $x = 2$ . Then,

$$2^3 \equiv 8 \pmod{21},$$

$$2^4 \equiv 16 \pmod{21},$$

$$2^5 \equiv 11 \pmod{21},$$

$$2^6 \equiv 1 \pmod{21},$$

$GCD(7, 21) = 7$  and  $GCD(9, 21) = 3$ .

## 2 Quantum calculation of the order of $x \bmod N$

- Problem: given  $x$ ,  $1 < x < N$ , find  $r$  such that

$$x^r \equiv 1 \pmod{N}.$$

- Let  $n$  be the number of qubits used to represent  $N$ , defined by

$$n = \lceil \log_2 N \rceil.$$

- Let  $V_x$  be a unitary operator defined by

$$V_x(|j\rangle_n |k\rangle_n) = |j\rangle_n |k + x^j\rangle_n,$$

where  $j = 0, \dots, 2^n - 1$  and  $k = 0, \dots, 2^n - 1$ .

- Initial state of the algorithm:

$$|\psi_0\rangle = |0\rangle_n |0\rangle_n.$$

- Applying the Hadamard operator in each qubit of the first register, we have:

$$|\psi_1\rangle = \frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} |j\rangle|0\rangle.$$

- Applying  $V_x$  on  $|\psi_1\rangle$ , we get

$$|\psi_2\rangle = \frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} |j\rangle|x^j\rangle.$$

- States with  $|1\rangle$  in the second register:

$$\{|0\rangle|1\rangle, \underline{|r\rangle|1\rangle}, |2r\rangle|1\rangle, |3r\rangle|1\rangle, \dots, | \left( \frac{2^n}{r} - 1 \right) r \rangle |1\rangle\}.$$

- All the states of the superposition:

$$\{ \underline{|0\rangle|1\rangle}, \dots, \underline{|r\rangle|1\rangle}, |r+1\rangle|x\rangle, \dots, \underline{|2r\rangle|1\rangle}, |2r+1\rangle|x\rangle, \dots, \underline{|3r\rangle|1\rangle}, |3r+1\rangle|x\rangle, \dots, \underline{| \left( \frac{2^n}{r} - 1 \right) r \rangle |1\rangle} \}.$$

- Rearranging, we get:

$$\begin{aligned} & \left\{ \left( |0\rangle + |r\rangle \dots + \left| \left( \frac{2^n}{r} - 2 \right) r \right\rangle + \left| \left( \frac{2^n}{r} - 1 \right) r \right\rangle \right) |1\rangle + \right. \\ & \left( |1\rangle + |r+1\rangle + \dots + \left| \left( \frac{2^n}{r} - 2 \right) r + 1 \right\rangle \right) |x^1\rangle + \\ & \left( |2\rangle + |r+2\rangle + \dots + \left| \left( \frac{2^n}{r} - 2 \right) r + 2 \right\rangle \right) |x^2\rangle + \\ & \left( |3\rangle + |r+3\rangle + \dots + \left| \left( \frac{2^n}{r} - 2 \right) r + 3 \right\rangle \right) |x^3\rangle + \dots \\ & \left. \left( |r-1\rangle + \dots + \left| \left( \frac{2^n}{r} - 2 \right) r + (r-1) \right\rangle \right) |x^{r-1}\rangle \right\}. \end{aligned}$$

- Rewriting  $|\psi_2\rangle$ :

$$|\psi_2\rangle = \frac{1}{2^{n/2}} \sum_{b=0}^{r-1} \left( \sum_{a=0}^{\frac{2^n}{r}-1} |ar+b\rangle |x^b\rangle \right).$$

- Measuring the second register, we obtain:

$$|\psi_3\rangle = \left(\frac{r}{2^n}\right)^{1/2} \left( \sum_{a=0}^{\frac{2^n}{r}-1} |ar + b_0\rangle |x^{b_0}\rangle \right).$$

### 3 The quantum Fourier transform

- The quantum Fourier transform  $FT$  is defined by

$$FT(|k\rangle) = \frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} e^{2\pi i j \frac{k}{2^n}} |j\rangle,$$

where  $|k\rangle$  is a state of the computational basis  $\{|0\rangle, |1\rangle, \dots, |2^n - 1\rangle\}$ .

- Applying  $FT^{-1}$  on the first register of  $|\psi_3\rangle$ ,

$$|\psi_3\rangle = \left(\frac{r}{2^n}\right)^{1/2} \left( \sum_{a=0}^{\frac{2^n}{r}-1} |ar + b_0\rangle |x^{b_0}\rangle \right),$$

we get:

$$|\psi_4\rangle = \frac{1}{r^{1/2}} \sum_{k=0}^{r-1} \left( e^{-2\pi i \frac{k}{r} b_0} |k \frac{2^n}{r}\rangle \right) |x^{b_0}\rangle.$$

- Measuring the first register, we obtain:

$$k_0 \frac{2^n}{r}.$$

- Dividing by  $2^n$ , we have:

$$\frac{k_0}{r}.$$

- We test the denominator  $r_1$  of the resulting fraction. If it satisfies the equation

$$x^{r_1} \equiv 1 \pmod{N},$$

$r_1$  is the order of  $x \pmod{N}$ .

- Otherwise, we have that

$$r_1 \mid r.$$

In this case, there is  $r_2$  such that

$$r = r_1 r_2.$$

- However,

$$x^r = x^{r_1 r_2} = (x^{r_1})^{r_2} \equiv 1 \pmod{N},$$

that is,  $r_2$  is the order of  $x^{r_1} \pmod{N}$ .

- The value of  $r$  can be found applying again the algorithm in  $O(\log_2 r)$  steps.