SENAI CIMATEC

# QUANTUM COMPUTING CENTER
## LATIN AMERICA

SENAI CIMATEC

LATIN AMERICA

**QUANTUM COMPUTING CENTER**

# K·U·A·T·O·M·U

SIMULADOR QUÂNTICO

# Algoritmo Quântico de Shor para Fatoração



- Shor apresentou dois algoritmos para fatoração e cálculo de logaritmo discreto em 1994 no *35th Annual Symposium on Foundations of Computer Science*.
- Publicou uma versão mais completa no artigo

  P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5):1484–1509, 1997.
- Publicou a versão final em

  P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Review, 41(2):303–332, 1999.

# Problema da fatoração de números inteiros

Problema:

Seja $N$ número inteiro composto. Encontre um fator não-trivial de $N$. Se $N$ é composto, existem números naturais $p_1$ e $p_2$ tais que $N = p_1 p_2$, onde $1 < p1$, $p2 < N$. O objetivo é encontrar $p_1$ e então $p_2$ é obtido calculando eficientemente $N/p_1$.

# Redução do problema de fatoração para cálculo de ordem

A ordem multiplicativa do número $a$ modulo $N$ é o menor inteiro positivo $r$ tal que

$$a^r \equiv 1 \mod N.$$

Por exemplo, para $N = 21$ e $a = 2$ temos que

$$\begin{aligned}
a &\equiv 2 \mod 21 & a^7 &\equiv 2 \mod 21 \\
a^2 &\equiv 4 \mod 21 & a^8 &\equiv 4 \mod 21 \\
a^3 &\equiv 8 \mod 21 & a^9 &\equiv 8 \mod 21 \\
a^4 &\equiv 16 \mod 21 & a^{10} &\equiv 16 \mod 21 \\
a^5 &\equiv 11 \mod 21 & a^{11} &\equiv 11 \mod 21 \\
a^6 &\equiv 1 \mod 21 & a^{12} &\equiv 1 \mod 21
\end{aligned} \quad \ldots$$

Portanto, a ordem de $a$ modulo $N$ é $r = 6$.

Se $r$ é par, então

$$\begin{aligned}\left(a^{\frac{r}{2}}+1\right)\left(a^{\frac{r}{2}}-1\right) &\equiv a^r-1 \mod N\\ &\equiv 0 \mod N.\end{aligned}$$

Temos dois números $a^{r/2}+1$ e $a^{r/2}-1$ cujo produto é múltiplo de $N$. Então, $\text{mdc}\left(a^{r/2}+1, N\right) > 1$ e $\text{mdc}\left(a^{r/2}-1, N\right) > 1$.

Por exemplo, para $a = 2$ and $r = 6$, temos $a^{r/2}+1 = 9$ and $a^{r/2}-1 = 7$, $\text{mdc}(9, 21) = 3$ e $\text{mdc}(7, 21) = 7$.

Exercício: mostre que o método falha para $a = 5$ e $N = 21$.

# Como selecionar $a$?



No algoritmo, $a$ é escolhido aleatoriamente no conjunto

$$\mathbb{Z}_N^* = \{a \in \mathbb{Z} : 1 \leq a < N \text{ and } \text{mdc}(a, N) = 1\}.$$

que é um grupo multiplicativo módulo $N$

Por exemplo, para $N = 21$ e $a = 2$, temos

$$\mathbb{Z}_N^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}.$$

# Como selecionar um bom valor de $a$?



Fato 3 (Teorema A4.13 do Nielsen&Chuang) Suponha que $N = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ é a fatoração prima de um inteiro positivo ímpar composto. Seja $a$ escolhido uniformemente ao acaso de $\mathbb{Z}_N^*$, e seja $r$ a ordem de $a$ módulo $N$. Então probilidade($r$ é par e $a^{r/2} + 1 \not\equiv 0 \mod N$) $\geq 1 - 1/2^m \geq 3/4$.

# Parte quântica do algoritmo de Shor



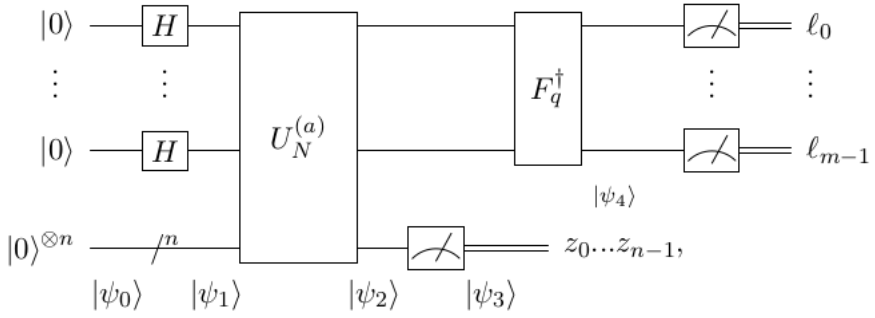
**Entrada:** $N$ e um inteiro $1 < a < N$ tal que $\text{mdc}(a, N) = 1$.

**Saída:** Uma cadeia de $m$ bits $\ell$, onde $\ell$ é o inteiro mais próximo de um múltiplo de $2^m/r$ com probabilidade maior que $4/\pi^2$, onde $2^m$ é a menor potência de 2 maior do que $N^2$.

1. Prepare o estado inicial $|0\rangle^{\otimes m}|0\rangle^{\otimes n}$, onde $m = \lceil 2\log_2 N \rceil$ e $n = \lceil \log_2 N \rceil$;
2. Aplique $H^{\otimes m}$ ao primeiro registrador;
3. Aplique $U_a$ aos dois registradores, onde $U_a|\ell\rangle|y\rangle = |\ell\rangle\big|y \oplus \left(a^\ell \mod N\right)\big\rangle$;
4. Meça o segundo registrador na base computacional (assuma a saída $z_0 ... z_{n-1}$);
5. Aplique a transformada de Fourier $F^\dagger_{2^m}$ ao primeiro registrador;
6. Meça o primeiro registrador na base computacional.

# Circuito do algoritmo de Shor






onde $q = 2^m$

# Início do algoritmo de Shor



No primeiro passo:

$$|\psi_0\rangle = |0\rangle^{\otimes m}|0\rangle^{\otimes n}$$

onde $m = \lceil 2\log_2 N \rceil$.

No segundo passo:

$$\begin{aligned} |\psi_1\rangle &= \big(H|0\rangle\big)^{\otimes m} \otimes |0\rangle^{\otimes n} \\ &= \frac{1}{\sqrt{2^m}} \sum_{\ell=0}^{2^m-1} |\ell\rangle \otimes |0\rangle^{\otimes n} \end{aligned}$$

onde $\ell$ está na notação decimal.

# Algoritmo de Shor antes da QFT

No terceiro passo:

$$
\begin{aligned}
|\psi_2\rangle &= U_a|\psi_1\rangle \\
&= \frac{1}{\sqrt{2^m}} \sum_{\ell=0}^{2^m-1} U_a(|\ell\rangle \otimes |0\cdots 0\rangle) \\
&= \frac{1}{\sqrt{2^m}} \sum_{\ell=0}^{2^m-1} |\ell\rangle \Big| a^\ell \mod N \Big\rangle \\
&= \frac{1}{\sqrt{2^m}} \Big( |0\rangle \big| a^0 \big\rangle + |1\rangle \big| a^1 \big\rangle + |2\rangle \big| a^2 \big\rangle + \cdots \Big)
\end{aligned}
$$

# Algoritmo de Shor na formulação do Kitaev (QPE)



Defina

$$U_a|y\rangle = |ay \mod N\rangle \tag{1}$$

Defina

$$|\psi_k\rangle = \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{-2\pi i \frac{k\ell}{r}} \left|a^\ell\right\rangle \tag{2}$$

# Algoritmo de Shor na formulação do Kitaev (QPE)

Note que

$$|\psi_k\rangle = \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{-2\pi i \frac{k\ell}{r}} \left| a^\ell \right\rangle$$

é autovertor de $U_a$ com autovalor $e^{2\pi i \frac{k}{r}}$ para $0 \leq k < 2^n$. De fato,

$$\begin{aligned} U_a|\psi_k\rangle &= \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{-2\pi i \frac{k\ell}{r}} \left| a^{\ell+1} \right\rangle \\ &= \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{-2\pi i \frac{k(\ell-1)}{r}} \left| a^\ell \right\rangle \\ &= e^{2\pi i \frac{k}{r}} |\psi_k\rangle. \end{aligned}$$

# Algoritmo de Shor na formulação do Kitaev (QPE)



Se

$$|\psi_k\rangle = \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{-2\pi i \frac{k\ell}{r}} \left| a^\ell \right\rangle$$

então

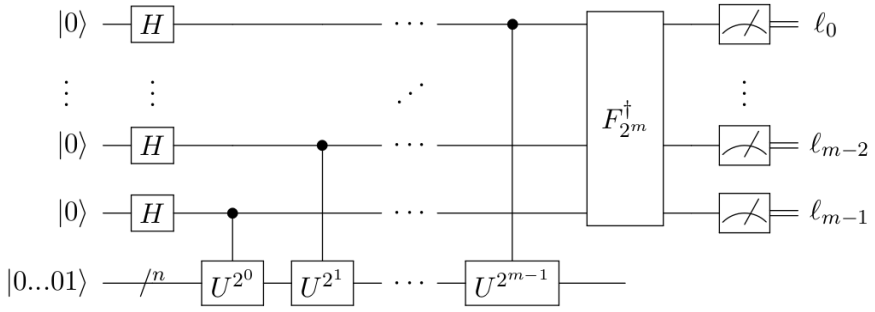
$$\left| a^\ell \right\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{2\pi i \frac{k\ell}{r}} |\psi_k\rangle.$$

Se $\ell = 0$ então $\left|a^0\right\rangle = |1\rangle$, e

$$|1\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |\psi_k\rangle.$$

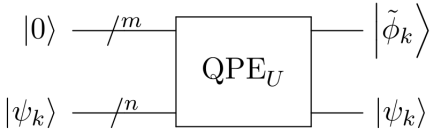
# Circuito do algoritmo de Shor na versão de Kitaev





# Revisão breve da estimativa de fase (QPE)






Suponha que $$U|\psi_k\rangle = e^{2\pi i \phi_k}|\psi_k\rangle$$

Se a entrada do segundo registrador é

$$|1\rangle = \frac{1}{\sqrt{r}} \sum_{j=1}^{r-1} |\psi_k\rangle.$$

então a saída é

$$|0\rangle|1\rangle \xrightarrow{\mathrm{QPE}_U} \frac{1}{\sqrt{r}} \sum_{j=1}^{r-1} |\tilde{\phi}_k\rangle|\psi_k\rangle$$

onde $\tilde{\phi}_k = \phi_k 2^m = \frac{k}{r} 2^m$ para algum $0 \leq k < r$.

# Saída do algoritmo de Shor



Para algum $0 \leq k < r$ uniformemente aleatório

$$\ell = \frac{k}{r} 2^m$$