# Pràctica: Simulació de l'algorisme de Shor

Assignatura: *Seguretat d'Aplicacionas i Comunicacions*
Grau en Enginyeria Informàtica – Universitat de Lleida

## Objectius

- Comprendre els conceptes bàsics de la computació quàntica aplicats a la factorització.
- Implementar una simulació pas a pas de l'algorisme de Shor.
- Entendre la relació entre la transformada de Fourier quàntica (QFT) i el càlcul del període d'una funció modular.
- Aplicar la part clàssica de l'algorisme per obtenir els factors d'un enter compost $N = p \cdot q$.

## Context teòric

L'algorisme de Shor és un dels resultats més importants de la computació quàntica. Permet factoritzar un enter $N$ en temps polinòmic utilitzant les propietats de la **superposició** i de la **transformada de Fourier quàntica**.

El seu nucli consisteix en trobar el període $r$ de la funció

$$f(x) = a^x \bmod N,$$

on $a$ és un enter coprimer amb $N$. Conegut $r$, és possible obtenir factors de $N$ resolent

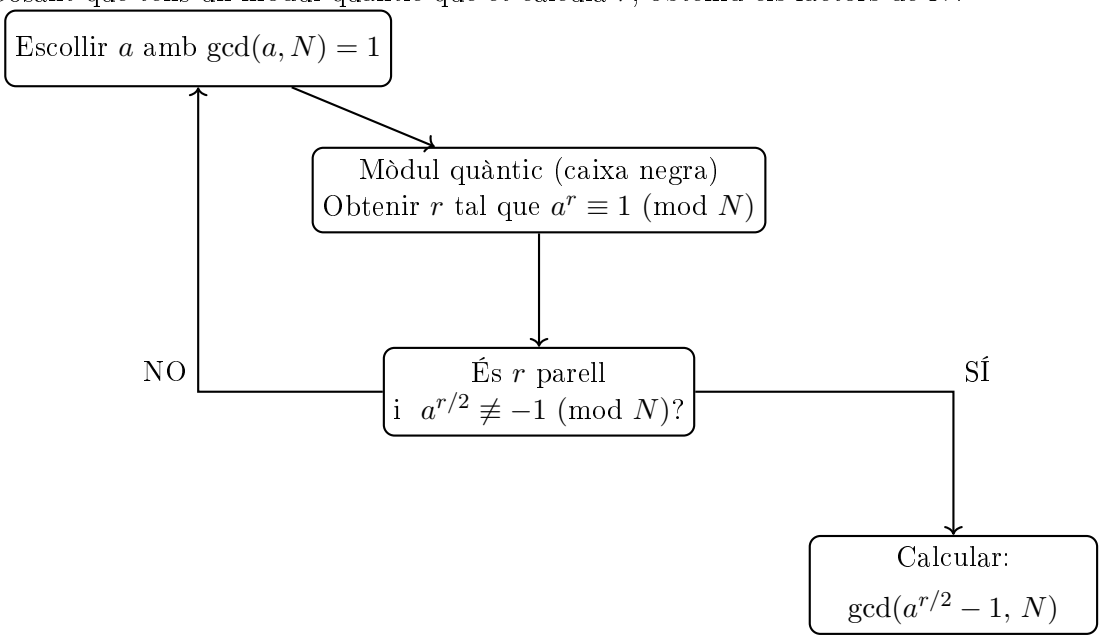
$$p = \gcd(a^{r/2} - 1, N), \quad q = \gcd(a^{r/2} + 1, N).$$

En aquesta pràctica simularem cada pas quàntic de l'algorisme utilitzant eines clàssiques.

## Desenvolupament de la pràctica

### Part clàssica de l'algorisme de Shor

Suposant que tens un mòdul quàntic que et calcula $r$, obteniu els factors de $N$:



### Simulació del mòdul quàntic

1. **Creació d'un registre quàntic uniforme**

   Implementeu una funció que simuli un registre quàntic de mida $n$ amb amplituds uniformes.

2. **Entrellaçament: Exponenciació modular**

   Simuleu l'operació quàntica que transforma $|x\rangle \to |x, a^x \bmod N\rangle$ mitjançant, per exemple, una taula on la primera columna és un registre i la segona l'altre.

3. **Mesura del segon registre**

   Simuleu la mesura del segon registre i la conseqüent reducció del primer:

4. **Aplicació de la QFT**

   Simule la transformada de Fourier quàntica (QFT) mitjançant una FFT estàndard:

5. **Càlcul del període mitjançant fraccions continues**

   Utilitzeu fraccions continues per aproximar $k/2^m$ i trobar el període $r$:

### Integració completa

Combineu totes les parts per obtenir una simulació funcional de l'algorisme de Shor: