El algoritmo de Shor — Parte 1

Computación Cuántica: Algorítmica y Software

Joaquín Keller

2026 UCV

Factorizar N en factores primos

0. Utilizar un test de primalidad, si N es primo el resultado es N, y sino
1. conseguir un factor d de N con $1 < d < N$
2. aplicar el algoritmo a d y N/d

Conseguir un factor d de N:

1. Tomar un $a < N$ al azar
2. si $d = mcd(a, N) \neq 1$ entonces d es un factor de N con $1 < d < N$
3. Si $mcd(a, N) = 1$ ...

Orden de a módulo N (1)

Si $mcd(a, N) = 1$ se define el orden de a módulo N:

$$ord_N(a) = min\{k > 0 \mid a^k \equiv 1 \pmod{N}\}$$

Podemos notar que: $\{k > 0 \mid a^k \equiv 1 \pmod{N}\} \neq \varnothing$

Demostración: $\left|\{k > 0 \mid a^k \bmod N\}\right| \leq N \Rightarrow \exists i > j \mid a^i \equiv a^j \pmod{N}$

Como a es invertible mod N $\quad a^k \equiv a^{i-j} \equiv a^i(a^{-1})^j \equiv a^j(a^{-1})^j \equiv 1 \pmod{N}$

Orden de a módulo N (2)

$k \xmapsto{f} a^k \bmod N$ f es periódica y $r = ord_N(a)$ es el período más corto

r es un período de f: $\forall 0 \leq k < r \qquad f(k+r) = f(k)$

$$f(k+r) = a^{k+r} = a^k a^r = a^k \times 1 = f(k)$$

No existe un periodo $r' < r$ sino $a^{r'} = f(r') = f(0+r') = f(0) = a^0 = 1$

Y también: Euler nos dice $a^{\varphi(N)} \equiv 1 \pmod{N}$ de ahí deducimos $r | \varphi(N)$

Calcular $ord_N(a)$, el orden de a módulo N

```
def orden_modulo(N, a):
    k=1
    t=a
    while t!=1:
        t*=a # calcular a**k
        t%=N # el resto modulo N
        k+=1
    return k
```

$\mathcal{O}(N) = \mathcal{O}(2^n)$

n: nro de dígitos de N

$n = log_2 N$

Es decir calcular a^1, a^2, a^3, ..., mod N hasta topar con $a^k \equiv 1 \pmod{N}$

Conseguir un factor de N (1)

1. Tomar un $a < N$ al azar — Hipótesis 1: $mcd(a, N) = 1$

Si $r = ord_N(a)$ es impar, tomar otro a al azar — Hipótesis 2: r es par

$$a^r \equiv 1 \pmod{N} \Leftrightarrow a^r - 1 \equiv 0 \pmod{N} \Leftrightarrow (a^{r/2})^2 - 1^2 \equiv 0 \pmod{N}$$

$$\Leftrightarrow (a^{r/2} - 1)(a^{r/2} + 1) \equiv 0 \pmod{N}$$

Si $a^{r/2} + 1 \equiv 0 \pmod{N}$
tomar otro a al azar — Hipótesis 3: $a^{r/2} + 1 \not\equiv 0 \pmod{N}$

Conseguir un factor de N (2)

Como $\frac{r}{2} < r$ $\quad a^{r/2} \not\equiv 1 \pmod{N} \Leftrightarrow a^{r/2} - 1 \not\equiv 0 \pmod{N}$

Sean $\begin{matrix} u = a^{r/2}-1 \bmod N \\ v = a^{r/2}+1 \bmod N \end{matrix}$ tenemos $\begin{matrix} u \not\equiv 0 \pmod{N} \\ v \not\equiv 0 \pmod{N} \end{matrix}$ y $uv \equiv 0 \pmod{N}$

N no es un divisor de u entonces $mcd(u, N) \neq N$

Como $N|uv$ entonces $mcd(u, N) \neq 1$ porque sino $N|v$

$\begin{matrix} d = mcd(u, N) \\ d' = mcd(v, N) \end{matrix}$ son factores de N no triviales (ie $\neq 1$, $\neq N$)

Conseguir un factor de N (3)

1. Tomar $a < N$ al azar
   Si $mcd(a, N) \neq 1$ | Factor de N: $mcd(a, N)$
2. Calcular $r = ord_N(a)$
   Si r es impar $\longrightarrow$ 1.
   Si $a^{r/2} + 1 \equiv 0 \pmod{N} \longrightarrow$ 1.
3. $mcd(a^{r/2} - 1, N)$ y $mcd(a^{r/2} + 1, N)$

Descomposición en factores primos: $N = \prod_{i=1}^{k} p_i^{\alpha_i}$ con $p_i > 2$

Probabilidad de r par y $a^{r/2} + 1 \not\equiv 0 \pmod{N}$ es $1 - \frac{1}{2^{k-1}}$