



ok, nice, me puedes hacer el analisis entrando N=7?

¡Claro! Te mostraré el análisis completo del algoritmo de Shor para **N = 7**.

Paso 1: Verificar si N es primo

Primero verificamos si 7 es primo.^{[1] [2]}

El número 7 **es primo** (solo divisible por 1 y 7).

Resultado: El algoritmo termina aquí porque 7 ya es primo.^[1]

Los factores de 7 son: **1 y 7**

¿Por qué el algoritmo de Shor no es necesario aquí?

El algoritmo de Shor está diseñado para factorizar números **compuestos** (números que son producto de dos o más primos). Para números primos como 7, no hay factorización no trivial posible.^{[3] [4]}

Alternativa: Analicemos N = 21 (número compuesto)

Para ver el algoritmo en acción, usemos **N = 21** (que es 3×7):

Paso 1: Verificar que no es primo

21 no es primo ✓

Paso 2: Elegir un número aleatorio

Elegimos **a = 2** (entre 2 y 20)

Paso 3: Calcular el máximo común divisor

$\text{mcd}(2, 21) = 1$, son coprimos ✓

Paso 4: Encontrar el período (parte cuántica)

Calculamos $f(x) = 2^x \mod 21$:

- $2^1 = 2 \mod 21$
- $2^2 = 4 \mod 21$

- $2^3 = 8 \pmod{21}$
- $2^4 = 16 \pmod{21}$
- $2^5 = 32 = 11 \pmod{21}$
- $2^6 = 64 = 1 \pmod{21}$

El período es $r = 6$ ^[5]

Paso 5: Verificar que r es par

$r = 6$ es par ✓

Paso 6: Calcular los factores

- $2^{6/2} = 2^3 = 8$
- Factor 1: $\text{mcd}(8 - 1, 21) = \text{mcd}(7, 21) = 7$
- Factor 2: $\text{mcd}(8 + 1, 21) = \text{mcd}(9, 21) = 3$

Resultado Final

Los factores de 21 son 3 y 7^[1]

Verificación: $3 \times 7 = 21$ ✓

Conclusión

Para $N = 7$, el algoritmo de Shor no se ejecuta porque detecta inmediatamente que es primo. El algoritmo solo es útil para números compuestos donde la factorización clásica es computacionalmente costosa.^{[2] [1]}

**

1. https://es.wikipedia.org/wiki/Algoritmo_de_Shor
2. <https://www.caminantecuantico.com/2025/04/algoritmo-shor.html>
3. <https://keepcoding.io/blog/algoritmo-de-shor-y-sus-aplicaciones/>
4. https://diposit.ub.edu/dspace/bitstream/2445/217048/2/tfg_benavente_de_lucas_beatriz.pdf
5. https://www.youtube.com/watch?v=6SIX_FR4wOM