



Ejemplo Práctico: Factorizar el Número 15

Voy a mostrarte cómo funciona el algoritmo de Shor usando el ejemplo clásico de factorizar 15.
^[1] ^[2]

Paso 1: Elegir un número aleatorio

Queremos factorizar $N = 15$, entonces elegimos un número aleatorio a entre 2 y 13. Vamos a seleccionar $a = 2$.^[1]

Paso 2: Verificar si es coprimo

Calculamos $\text{mcd}(2, 15) = 1$, por lo tanto 2 y 15 son coprimos y podemos continuar.^[3]

Paso 3: Encontrar el período

Construimos la función $f(x) = 2^x \mod 15$ y buscamos el período r :^[3] ^[1]

- $2^1 = 2 \mod 15$
- $2^2 = 4 \mod 15$
- $2^3 = 8 \mod 15$
- $2^4 = 16 \equiv 1 \mod 15$

El período es $r = 4$ porque $2^4 \equiv 1 \mod 15$.^[1]

Paso 4: Calcular los factores

Una vez encontrado el período par, calculamos:^[2] ^[3]

- $2^{r/2} = 2^2 = 4$
- Factor 1: $\text{mcd}(4 - 1, 15) = \text{mcd}(3, 15) = 3$
- Factor 2: $\text{mcd}(4 + 1, 15) = \text{mcd}(5, 15) = 5$

Por lo tanto, los factores primos de 15 son **3 y 5**.^[2]

Casos de Uso del Algoritmo de Shor

Criptografía RSA

El caso de uso más significativo es romper el sistema criptográfico RSA. RSA se basa en la dificultad de factorizar números grandes (productos de dos números primos p y q). El algoritmo de Shor puede descifrar estos sistemas exponencialmente más rápido que cualquier algoritmo clásico, amenazando la seguridad de las comunicaciones cifradas actuales. ^[4] ^[5]

Implementación en Qiskit

El algoritmo se puede implementar en computadoras cuánticas usando frameworks como Qiskit de IBM. El código básico utiliza la Transformada Cuántica de Fourier (QFT) para encontrar el período y luego aplica el máximo común divisor para extraer los factores. ^[6]



1. https://www.youtube.com/watch?v=6SIX_FR4wOM
2. <https://github.com/juanki98/Algoritmo-de-Shor-y-variantes>
3. <https://www.caminantecuantico.com/2025/04/algoritmo-shor.html>
4. https://diposit.ub.edu/dspace/bitstream/2445/217048/2/tfg_benavente_de_lucas_beatriz.pdf
5. <https://keepcoding.io/blog/algoritmo-de-shor-y-sus-aplicaciones/>
6. <https://tecnologia.euroinnova.com/algoritmo-de-shor>
7. https://es.wikipedia.org/wiki/Algoritmo_de_Shor
8. <https://www.youtube.com/watch?v=I9OE5N5TBQk>
9. <https://www.youtube.com/watch?v=ufC7x1zFYbo>
10. <https://www.youtube.com/watch?v=wsxGUkxwKkY>