Algoritmo de Shor

Alonso Toro

Noviembre 2026

1. Introducción a las funciones periódicas

Una función $f(x)$ es periódica si sus valores se van repitiendo a intervalos regulares a lo largo de su dominio. Formalmente, una función $f(x)$ es periódica si existe un $p > 0$ tal que para todo x en el dominio de f se cumple:

$$f(x + kp) = f(x), \quad k \in \mathbb{Z}$$

A este valor p se le llama **periodo**.

En un sistema de N-qubits, se pueden representar $M = 2^N$ estados de la base computacional de manera simultánea gracias a la superposición. Consideremos que el dominio de nuestra función periódica $f(x)$ está compuesto por estos M elementos.

¿Cómo podemos usar la computación cuántica para hallar el periodo p de $f(x)$? El algoritmo ocupa de forma directa el entrelazamiento para ganar información midiendo qubits. Partimos de un estado de superposición total:

$$|\psi\rangle = \frac{1}{\sqrt{M}}(|0\rangle + |1\rangle + \cdots + |M-1\rangle)$$

Para evaluar $f(x)$ cuánticamente de forma reversible (y por ende unitaria), se define formalmente el oráculo cuántico U_f actuando sobre dos registros mediante la operación suma módulo 2 bit a bit ($\oplus$, equivalente a XOR):

$$\boxed{U_f|x\rangle|z\rangle = |x\rangle|z \oplus f(x)\rangle}$$

Al inicializar el segundo registro en el estado $|z\rangle = |0\rangle$, la acción del oráculo se simplifica directamente a:

$$U_f|x\rangle|0\rangle \to |x\rangle|0 \oplus f(x)\rangle = |x\rangle|f(x)\rangle$$

De modo que al aplicarlo a nuestra superposición, obtengamos:

$$|\psi\rangle = \frac{1}{\sqrt{M}}\left(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle + \cdots + |M-1\rangle|f(M-1)\rangle\right)$$

2. El problema de la medición y el colapso

Imaginemos, a modo de modelo pedagógico simplificado (en un registro físico de N qubits se tendría siempre $M = 2^N$), que tenemos una función $f(x)$ con periodo $p = 2$ y un dominio de $M = 6$ elementos. Los mapeos serían, por ejemplo:

$$\begin{aligned} |0\rangle &\to |f(0)\rangle = |3\rangle \qquad |1\rangle \to |f(1)\rangle = |5\rangle \\ |2\rangle &\to |f(2)\rangle = |3\rangle \qquad |3\rangle \to |f(3)\rangle = |5\rangle \\ |4\rangle &\to |f(4)\rangle = |3\rangle \qquad |5\rangle \to |f(5)\rangle = |5\rangle \end{aligned}$$

Si medimos el primer qubit (registro de entrada), el segundo colapsará a $|f(x_0)\rangle$. No ganamos nada interesante, solo un valor aleatorio.

Pero, ¿qué sucede si medimos el **segundo registro** y obtenemos, por ejemplo, el valor 3? El primer registro colapsará a una superposición de todos los estados posibles que evalúan a 3. En este caso:

$$\frac{1}{\sqrt{3}}(|0\rangle + |2\rangle + |4\rangle)$$

¡Estos estados son de la forma $|x_0 + kp\rangle$! Al medir el segundo registro, el primero colapsa a una superposición de la forma:

$$\rightarrow \sum |x_0 + kp\rangle$$

Aquí ya está contenido el periodo, pero tenemos un problema: el desplazamiento x_0 molesta y, si medimos el primer registro, simplemente obtendremos un valor aleatorio de la forma $x_0 + kp$. Necesitamos una forma de extraer p.

3. Formalización del Algoritmo

Para el primer registro de entrada, digamos que tiene N qubits (con $M = 2^N$). Para el segundo registro, digamos que tiene m_q qubits; solo se requiere la cantidad necesaria para almacenar el valor más alto de $f(x)$.

Comenzamos con todos los qubits inicializados en $|0\rangle$:

$$|\psi_0\rangle = |0\rangle^{\otimes N}|0\rangle^{\otimes m_q}$$

Queremos armar una superposición uniforme de todos los estados en el primer registro. Aplicamos la compuerta de Hadamard ($H^{\otimes N}$) sobre este registro:

$$|\psi_1\rangle = (H^{\otimes N}|0\rangle^{\otimes N}) \otimes |0\rangle^{\otimes m_q} = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle|0\rangle$$

Ahora, aplicamos el oráculo U_f, sabiendo que $U_f|x\rangle|0\rangle \rightarrow |x\rangle|f(x)\rangle$:

$$|\psi_2\rangle = U_f|\psi_1\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle|f(x)\rangle$$

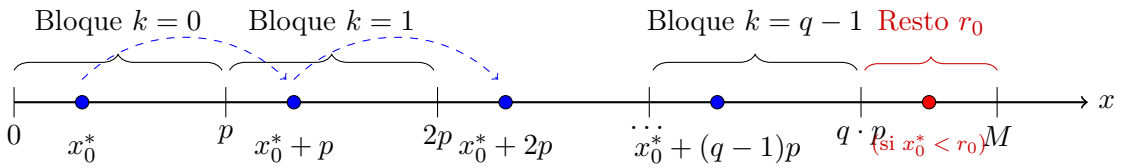
3.1. Estructura de bloques periódicos y colapso espacial general

Para analizar este estado de forma general (sin asumir todavía si M es divisible exactamente por p o no), dividimos nuestro dominio de M estados en sub-bloques de longitud p. Por el algoritmo de la división de Euclides, podemos escribir:

$$M = q \cdot p + r_0, \quad \text{donde } q = \lfloor M/p \rfloor \text{ y } 0 \leq r_0 < p$$

Cualquier índice $x \in \{0, 1, \ldots, M-1\}$ se expresa de manera única como $x = x_0 + kp$, donde $0 \leq x_0 < p$ es el desplazamiento dentro de cada periodo y k es el índice del bloque.

Para visualizar esto de forma general, observemos la siguiente recta que representa nuestro espacio de M elementos divididos en bloques de longitud p (donde el último tramo se completa exactamente si $r_0 = 0$, o queda truncado si $r_0 > 0$):



¿Dónde interviene el resto r_0? En que el último bloque queda incompleto y solo contiene r_0 estados (correspondientes a los primeros desplazamientos $x_0 \in \{0, \ldots, r_0 - 1\}$). Por lo tanto, la cantidad total de veces $m(x_0)$ que el valor $f(x_0)$ se repite dentro del dominio $\{0, \ldots, M-1\}$ es:

$$m(x_0) = \begin{cases} q+1, & \text{si } 0 \leq x_0 < r_0 \\ q, & \text{si } r_0 \leq x_0 < p \end{cases} \tag{1}$$

(Nótese que si M es múltiplo exacto de p, entonces $r_0 = 0$ y todos los desplazamientos tienen exactamente $m(x_0) = q = M/p$). Aprovechando que por periodicidad $f(x_0 + kp) = f(x_0)$, reescribimos el estado $|\psi_2\rangle$:

$$|\psi_2\rangle = \frac{1}{\sqrt{M}} \sum_{x_0=0}^{p-1} \sum_{k=0}^{m(x_0)-1} |x_0 + kp\rangle |f(x_0)\rangle$$

Ahora, al medir el segundo registro en una ejecución del circuito, este colapsa a un valor específico $|f(x_0^*)\rangle$. A partir de este instante, tanto x_0^* como su número de bloques $m = m(x_0^*)$ quedan completamente fijos, dejando al primer registro en una superposición periódica de exactamente m términos:

$$|\psi_3^{\text{no norm.}}\rangle = \sum_{k=0}^{m-1} |x_0^* + kp\rangle$$

Como hay m estados ortogonales con peso 1, dividimos por $\sqrt{m}$ para normalizar y obtenemos el estado general pre-QFT:

$$|\psi_3\rangle = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0^* + kp\rangle \tag{2}$$

¡Notemos que este estado contiene el periodo p en el espaciamiento de sus términos, pero aún depende del desplazamiento aleatorio x_0^*!

4. Aplicando la Transformación de Fourier Cuántica (QFT): formulación general

Sabemos que la Transformación de Fourier Cuántica actúa sobre cualquier estado de la base computacional $|x\rangle$ proyectándolo en una superposición de fases complejas:

$$\text{QFT}|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{x \cdot y}{M}} |y\rangle$$

Aplicamos la QFT una única vez a nuestro estado general normalizado $|\psi_3\rangle$:

$$|\psi_4\rangle = \text{QFT}|\psi_3\rangle = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} \left(\frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{(x_0^* + kp)y}{M}} |y\rangle \right)$$

Intercambiando el orden de las sumatorias y separando la exponencial compleja en el factor que depende de x_0^* y el que depende del índice de bloque k, llegamos a la **ecuación maestra del estado final**:

$$|\psi_4\rangle = \sum_{y=0}^{M-1} \alpha_y |y\rangle = \frac{1}{\sqrt{mM}} \sum_{y=0}^{M-1} e^{2\pi i \frac{x_0^* y}{M}} \underbrace{\left(\sum_{k=0}^{m-1} e^{2\pi i \frac{kpy}{M}} \right)}_{S(y)} |y\rangle \tag{3}$$

Observemos la estructura de la amplitud α_y para cada estado de salida $|y\rangle$:

- **Eliminación de la fase lineal de x_0^*:** El desplazamiento aleatorio x_0^* ha salido de la sumatoria sobre k como el factor de fase unitario $e^{2\pi i \frac{x_0^* y}{M}}$. Al calcular la probabilidad de medir cualquier estado $|y\rangle$ (dado el colapso en x_0^*) mediante la regla de Born, el módulo al cuadrado de este factor de fase es $\left|e^{2\pi i \frac{x_0^* y}{M}}\right|^2 = 1$ y desaparece por completo.

- **El filtro de interferencia $S(y)$:** Toda la distribución de probabilidad $P(y \mid x_0^*)$ queda gobernada exclusivamente por la serie geométrica interna de m términos con razón $r = e^{2\pi i \frac{py}{M}}$:

$$S(y) = \sum_{k=0}^{m-1} \left(e^{2\pi i \frac{py}{M}}\right)^k, \quad \text{de modo que } P(y \mid x_0^*) = |\alpha_y|^2 = \frac{1}{mM}|S(y)|^2 \tag{4}$$

A partir de esta única expresión general (ecuaciones 3 y 4), extraemos de inmediato qué ocurre al medir en el **Caso Ideal** (deltas exactos) y en el **Caso Real** (dispersión espectral).

5. Caso 1: El Escenario Ideal (M es múltiplo exacto de p)

Comencemos analizando qué ocurre bajo la hipótesis ideal de que M es un múltiplo exacto del periodo p ($r_0 = 0$). Aquí caben exactamente $m = \frac{M}{p}$ bloques completos, por lo que $\frac{1}{\sqrt{mM}} = \frac{\sqrt{p}}{M}$.

Al evaluar la suma geométrica $S(y)$ de la ecuación (4) con $m = M/p$, existen únicamente dos posibilidades para cada estado entero $y \in \{0, 1, \ldots, M-1\}$:

- **Subcaso 1A (y es múltiplo exacto de M/p):** Si $y = c\frac{M}{p}$ para algún entero $c \in \{0, 1, \ldots, p-1\}$, la fracción en el exponente se simplifica a un entero:

$$\frac{py}{M} = \frac{p\left(c\frac{M}{p}\right)}{M} = c \in \mathbb{Z} \implies e^{2\pi i k c} = 1$$

  Todos los fasores apuntan en ángulo 0 y se suman constructivamente:

$$S\left(c\frac{M}{p}\right) = \sum_{k=0}^{(M/p)-1} 1 = \frac{M}{p}$$

- **Subcaso 1B (y NO es múltiplo de M/p):** La razón cumple $r = e^{2\pi i \frac{py}{M}} \neq 1$. Evaluando la suma geométrica finita $\sum_{k=0}^{m-1} r^k = \frac{1-r^m}{1-r}$ con $m = M/p$:

$$S(y) = \frac{1 - e^{2\pi i \frac{py}{M} \cdot \frac{M}{p}}}{1 - e^{2\pi i \frac{py}{M}}} = \frac{1 - e^{2\pi i y}}{1 - e^{2\pi i \frac{py}{M}}} = 0$$

  Como y es siempre un número entero, $e^{2\pi i y} = 1$ y el numerador vale $1 - 1 = 0$. Las fases se cancelan de manera **perfectamente destructiva**.

Sustituyendo en la ecuación (4), la probabilidad colapsa en un peine de **Deltas de Kronecker exactas**:

$$P(y \mid x_0^*) = \begin{cases} \frac{1}{(M/p)M}\left(\frac{M}{p}\right)^2 = \frac{1}{p} & \text{si } y = c\frac{M}{p} \\ 0 & \text{en otro caso} \end{cases} \tag{5}$$

5.1. Extracción del periodo en el Caso Ideal mediante el MCD

En este escenario ideal, medimos exclusivamente múltiplos exactos $y = c\frac{M}{p}$.

- **Con una sola medición y:** Formamos la fracción conocida $\frac{y}{M} = \frac{c}{p}$. Al simplificarla dividiendo por $\text{MCD}(y, M)$, obtenemos el denominador reducido:

$$\boxed{p' = \frac{p}{\text{MCD}(c, p)}}$$

  Si c y p son coprimos ($\text{MCD}(c, p) = 1$), entonces $p' = p$ entrega el periodo de inmediato. Si $\text{MCD}(c, p) > 1$, p' es un divisor de p, por lo que se verifica clásicamente si $f(x+p') = f(x)$ y, de no cumplirse, se repite o combina con otra lectura.

- **Combinando múltiples mediciones $y_1, \ldots, y_k$:** Calculando el MCD entre varias lecturas no nulas mediante el algoritmo de Euclides:

$$\text{MCD}(y_1, y_2, \ldots, y_k) = \frac{M}{p} \underbrace{\text{MCD}(c_1, c_2, \ldots, c_k)}_{=1 \text{ con alta prob.}} = \frac{M}{p} \implies p = \frac{M}{\text{MCD}(y_1, \ldots, y_k)}$$

6. Caso 2: El Escenario Real (M no es múltiplo de p)

Veamos ahora qué ocurre en la ecuación (4) cuando $M = 2^N$ no es múltiplo de p ($r_0 > 0$). Aquí el número de bloques $m \in \{q, q+1\}$ ya no es igual a M/p.

6.1. Deducción del Núcleo de Dirichlet (sinc^2): ¿Por qué se dispersa la probabilidad?

Como la razón $r = e^{2\pi i \frac{py}{M}} \neq 1$ para todo $y \neq 0$, evaluamos la suma geométrica $S(y)$ de la ecuación (4) llamando $\theta_y = 2\pi\frac{py}{M}$:

$$S(y) = \sum_{k=0}^{m-1} e^{ik\theta_y} = \frac{1 - e^{im\theta_y}}{1 - e^{i\theta_y}}$$

Factorizando el ángulo mitad en el numerador ($e^{im\theta_y/2}$) y en el denominador ($e^{i\theta_y/2}$) y usando la identidad de Euler $e^{-i\phi} - e^{i\phi} = -2i\sin(\phi)$:

$$S(y) = \frac{e^{i\frac{m\theta_y}{2}}\left(e^{-i\frac{m\theta_y}{2}} - e^{i\frac{m\theta_y}{2}}\right)}{e^{i\frac{\theta_y}{2}}\left(e^{-i\frac{\theta_y}{2}} - e^{i\frac{\theta_y}{2}}\right)} = e^{i\frac{(m-1)\theta_y}{2}} \frac{\sin\left(\frac{m\theta_y}{2}\right)}{\sin\left(\frac{\theta_y}{2}\right)}$$

Al elevar al cuadrado en la ecuación (4), la fase $e^{i\frac{(m-1)\theta_y}{2}}$ tiene módulo 1 y desaparece, entregando la distribución condicional exacta:

$$P(y \mid x_0^*) = \frac{1}{mM} \frac{\sin^2\left(\pi m\frac{py}{M}\right)}{\sin^2\left(\pi\frac{py}{M}\right)} \tag{6}$$

Esta función es el **Núcleo de Dirichlet**, el equivalente discreto de la función sinc^2. Comparando las ecuaciones (5) y (6), queda completamente claro por qué la probabilidad se dispersa:

- **En el Caso Ideal ($m = M/p$):** El producto $m\frac{p}{M} = 1$ hacía que el numerador fuera $\sin^2(\pi y) = 0$ para todo entero y, cancelando a cero todos los estados salvo las deltas exactas donde el denominador también se anulaba.

- **En el Caso Real ($m \neq M/p$):** Como $m\frac{p}{M} \neq 1$, el argumento $\pi m\frac{py}{M}$ en el numerador **ya no es un múltiplo entero de** π. Los fasores no alcanzan a cerrar un ciclo exacto y la suma no se anula por completo, provocando que la probabilidad se "derrame" alrededor de los valores ideales fraccionarios $c\frac{M}{p}$.

- **Concentración en los enteros más cercanos y_c:** A pesar de esta dispersión, el numerador está acotado entre 0 y 1, mientras que el denominador $\sin^2\left(\pi\frac{py}{M}\right)$ no depende de m ni de x_0^*, y se hace mínimo (cercano a cero) cuando $\frac{py}{M} \approx c \implies y \approx c\frac{M}{p}$. Si llamamos y_c al entero más cercano a $c\frac{M}{p}$ y definimos la pequeña desviación $\delta = \frac{py_c}{M} - c$ (donde $|\delta| \leq \frac{p}{2M}$), entonces $\sin(\pi\delta) \approx \pi\delta$ y la ecuación (6) toma la forma de una campana sinc^2:

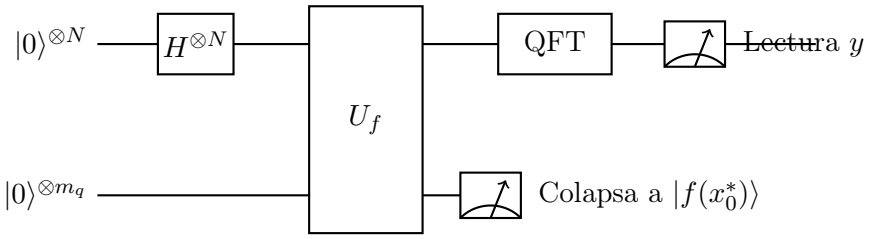
$$P(y_c \mid x_0^*) = \frac{1}{mM}\frac{\sin^2(\pi m\delta)}{\sin^2(\pi\delta)} \approx \frac{m}{M}\left(\frac{\sin(\pi m\delta)}{\pi m\delta}\right)^2 = \frac{m}{M}\text{sinc}^2(m\delta)$$

  Así, sin importar si en el colapso tocó $m = q$ o $m = q + 1$, **los picos principales de probabilidad siempre caen en los enteros y_c inmediatamente adyacentes a los múltiplos ideales $c\frac{M}{p}$.**

7. Implementación Cuántica del Circuito y Caso de Estudio en Qiskit

Una vez comprendida la teoría tanto del caso ideal como de la dispersión espectral en el caso real, veamos el circuito cuántico que implementaremos en código para verificar estos comportamientos en el proyector.

Esquema Cuántico General del Algoritmo



7.1. ¿Por qué es posible omitir la medición del segundo registro?

Aunque medir el segundo registro es sumamente útil desde el punto de vista pedagógico para visualizar el colapso hacia un desplazamiento fijo x_0^*, en la práctica esta medición interna es opcional y puede omitirse sin alterar la distribución de los picos en el primer registro:

- **Ausencia de interferencia cruzada:** Antes de medir, el estado conjunto es $|\psi_2\rangle = \frac{1}{\sqrt{M}}\sum_{x_0=0}^{p-1}\left(\sum_k |x_0 + kp\rangle\right)|f(x_0)\rangle$. Como para distintos desplazamientos x_0 los valores de $f(x_0)$ son distintos, los estados del segundo registro $|f(x_0)\rangle$ son mutuamente ortogonales y sus ramas jamás interfieren entre sí al aplicar la QFT sobre el primer registro.

- **Marginalización directa (Caso Ideal):** Si no medimos el segundo registro, por la ley de probabilidad total sumamos sobre los p desplazamientos posibles (cada uno con probabilidad uniforme $P(x_0) = \frac{1}{p}$). Como $P(y \mid x_0) = \frac{1}{p}$ en los múltiplos $y = c\frac{M}{p}$ sin depender de x_0:

$$P\left(c\frac{M}{p}\right) = \sum_{x_0=0}^{p-1} P(x_0)\cdot P\left(c\frac{M}{p}\,\middle|\, x_0\right) = \sum_{x_0=0}^{p-1}\left(\frac{1}{p}\right)\left(\frac{1}{p}\right) = p\cdot\frac{1}{p^2} = \frac{1}{p}$$

y $P(y) = 0$ en cualquier otro estado, recuperando exactamente el mismo peine de Deltas de Kronecker.

- **En el Caso Real:** De igual forma, como el denominador $\sin^2\left(\pi \frac{py}{M}\right)$ de la ecuación (6) no depende de x_0, todas las ramas ortogonales concentran sus campanas sinc^2 exactamente sobre los mismos enteros cercanos a $c\frac{M}{p}$.

7.2. La Función de Prueba $f(x) = x \pmod p$ y Topología en Qiskit

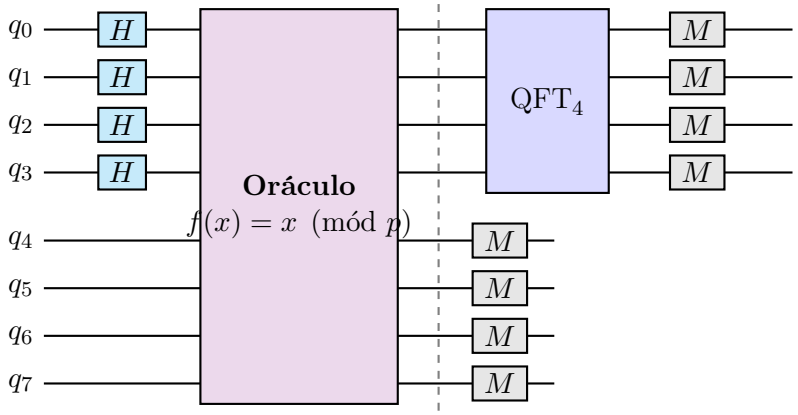
Para demostrar en código que esta subrutina cuántica es un detector universal de frecuencias y periodos antes de introducir la aritmética modular del algoritmo de Shor ($a^x \pmod N$), resulta sumamente pedagógico emplear la función periódica de prueba más limpia posible:

$$f(x) = x \pmod p$$

¿Por qué nos sirve $f(x) = x \pmod p$ como caso de estudio?

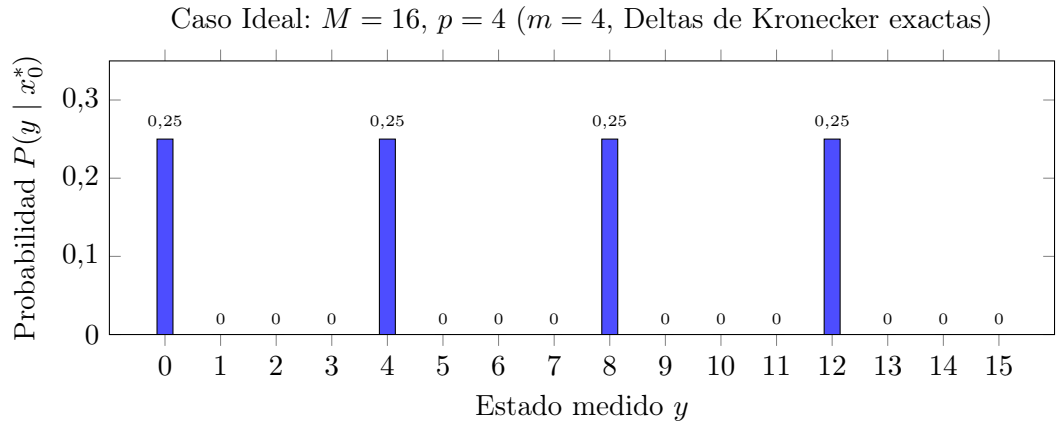
1. **Aísla el fenómeno físico:** Nos permite elegir a voluntad cualquier periodo p que deseemos probar en el simulador cuántico sin depender de las restricciones de coprimalidad de la exponenciación modular.
2. **Biyección dentro de cada periodo:** En cada bloque de tamaño p, la función toma exactamente los valores $\{0, 1, \ldots, p-1\}$ sin repeticiones internas, garantizando que el colapso del segundo registro seleccione exactamente los estados separados por múltiplos de p: $|x_0^* + kp\rangle$.
3. **Contraste directo entre Deltas y sinc^2:** Con un mismo circuito de $N = 4$ qubits ($M = 16$), basta cambiar el parámetro del oráculo de $p = 4$ a $p = 3$ para visualizar en vivo en un Jupyter Notebook la transición desde un peine de Deltas de Kronecker hacia el Núcleo de Dirichlet (sinc^2).

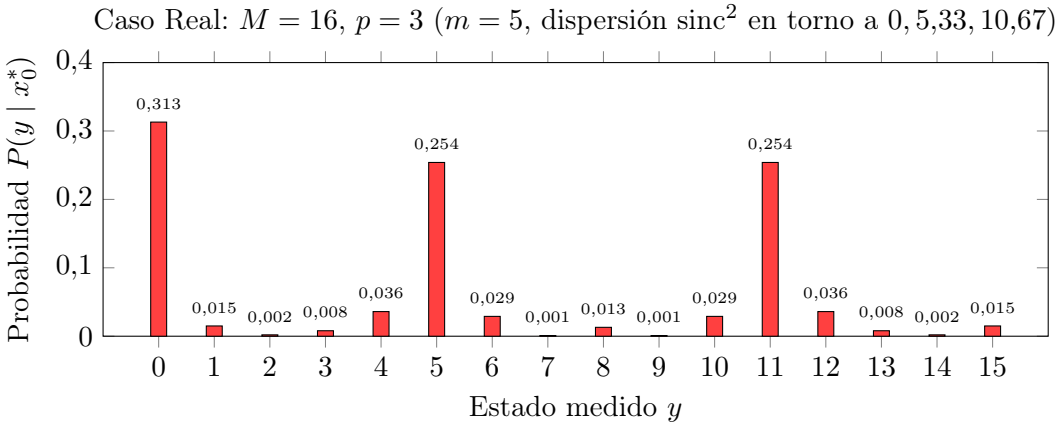
Implementamos el circuito con 4 qubits en el registro de entrada $(q_0, \ldots, q_3)$ y 4 qubits en el registro de salida $(q_4, \ldots, q_7)$. El bloque del oráculo codifica la operación reversible $|x\rangle|0\rangle \to |x\rangle|x \pmod p\rangle$:



8. Resultados de los Gráficos de Probabilidad y Extracción con Fracciones Continuas

Al ejecutar en el simulador `AerSimulator` ambos casos ($p = 4$ con 100 repeticiones y $p = 3$ con 1000 repeticiones), obtenemos los histogramas experimentales que contrastan directamente nuestras ecuaciones (5) y (6) en un registro de $M = 16$ estados ($N = 4$ qubits) entre el Caso Ideal ($p = 4$, donde $m = 4$) y el Caso Real ($p = 3$, ilustrando un colapso típico con $m = q = 5$ bloques completos, p. ej. $x_0^* \in \{1, 2\}$):





Análisis de ambos gráficos:

- En el **gráfico azul** ($f(x) = x \pmod 4$), la probabilidad vale exactamente $1/4 = 0{,}25$ en los múltiplos de $M/p = 4$: el simulador mide únicamente los estados `0000` (0), `0100` (4), `1000` (8) y `1100` (12), y es 0 absoluto en todos los demás estados, de donde $\text{MCD}(4, 8, 12) = 4 = M/p \implies p = 4$.

- En el **gráfico rojo** ($f(x) = x \pmod 3$, evaluado en la ecuación 6 con $m = 5$), como $16/3 = 5{,}33$ no es entero, las deltas se dispersan en tres campanas sinc^2: la mayor probabilidad se concentra en los enteros más cercanos a los múltiplos ideales, que son `0000` (0, con $P(0) = 5/16 = 0{,}3125$), `0101` (5) y `1011` (11, con $P(5) = P(11) \approx 0{,}254$), acompañados de pequeños lóbulos laterales en $4, 6, 10$ y 12. *(Nota: Si no se condiciona a un x_0^* específico, el promedio ponderado entre $m = 5$ y $m = 6$ produce exactamente la misma forma con picos en $0, 5$ y 11 de alturas 0,336 y 0,230).*

8.1. Extracción práctica con Fracciones Continuas para $M = 16, p = 3$

En el Caso Real, sabemos que el entero medido y satisface $y \approx c\frac{M}{p}$. Al dividir ambos lados por M (que es conocido), despejamos los datos medidos a la izquierda y las incógnitas a la derecha:

$$\underbrace{\frac{y}{M}}_{\text{Conocido}} \approx \underbrace{\frac{c}{p}}_{\text{Incógnita (denominador pequeño)}}$$

Como el registro cuántico tuvo que redondear el pico ideal (5,33 o 10,67) al entero más cercano ($y = 5$ o $y = 11$), la fracción $\frac{y}{M}$ no se puede simplificar directamente con el MCD. Para "deshacer" ese redondeo, desarrollamos $\frac{y}{M}$ en **fracciones continuas** (invirtiendo y separando la parte entera sucesivamente) y truncamos el último residuo pequeño:

- **Si medimos el pico $y = 5$:** Construimos la fracción conocida $\frac{y}{M} = \frac{5}{16}$ y la invertimos:

$$\frac{5}{16} = \frac{1}{\frac{16}{5}} = \frac{1}{3 + \underbrace{\frac{1}{5}}_{\text{error de redondeo}}} \approx \mathbf{\frac{1}{3}}$$

Al descartar el último residuo pequeño $\frac{1}{5}$, recuperamos la fracción simple $\frac{c}{p} = \frac{1}{3}$, cuyo denominador nos entrega directamente el periodo $p = 3$.

- **Si medimos el pico $y = 11$:** Construimos $\frac{y}{M} = \frac{11}{16}$ y repetimos el proceso:

$$\frac{11}{16} = \frac{1}{\frac{16}{11}} = \frac{1}{1 + \frac{5}{11}} = \frac{1}{1 + \frac{1}{\frac{11}{5}}} = \frac{1}{1 + \cfrac{1}{2 + \underbrace{\frac{1}{5}}_{\text{error de redondeo}}}} \approx \frac{1}{1 + \frac{1}{2}} = \mathbf{\frac{2}{3}}$$

Nuevamente, al truncar el residuo $\frac{1}{5}$, el convergente principal es $\frac{c}{p} = \frac{2}{3}$, revelando el denominador $p = 3$. *(Nota: En general, si c y p tuvieran un factor común, la fracción reducida entregaría un divisor $p' = p/MCD(c, p)$, por lo que siempre se verifica clásicamente que el candidato cumpla $f(x + p') = f(x)$).*

9. El Algoritmo de Shor: Reducción Clásica de Factorización a Búsqueda de Periodo

Habiendo construido nuestro módulo cuántico capaz de hallar el periodo de una función genérica, veamos ahora la parte clásica del algoritmo de Shor: **¿por qué factorizar un número compuesto $N = p_1 \cdot q_1$ es equivalente a encontrar el periodo de una función modular?**

9.1. Aritmética Modular y Raíces Cuadradas No Triviales

Recordemos primero el concepto de congruencia modular. Decimos que $a \equiv b \pmod{N}$ si ambos números dejan el mismo resto al dividirse entre N, lo cual equivale a decir que su diferencia $a - b$ es un múltiplo exacto de N:

$$a \equiv b \pmod{N} \iff a - b = k \cdot N, \quad k \in \mathbb{Z}$$

Por ejemplo, $7 \equiv 1 \pmod{3}$ puesto que $7 = 3 \cdot 2 + 1$ (deja resto 1), o equivalentemente, $7 - 1 = 6 = 2 \cdot 3$ es múltiplo de 3.

Definición (Raíz cuadrada no trivial módulo N):
Todo número N tiene dos raíces cuadradas "triviales" de 1, que son $x = 1$ y $x = N - 1 \equiv -1 \pmod{N}$, dado que $(\pm 1)^2 \equiv 1 \pmod{N}$. Decimos que un entero x es una **raíz cuadrada no trivial de 1 módulo N** si cumple simultáneamente dos condiciones:

$$x^2 \equiv 1 \pmod{N} \quad \text{y} \quad x \in [2, N - 2] \tag{7}$$

Ejemplo: Para $N = 8$, el número $x = 3$ es una raíz cuadrada no trivial módulo 8, ya que $3 \in [2, 6]$ y además $3^2 = 9 \equiv 1 \pmod{8}$ (pues $9 - 1 = 8 = 1 \cdot 8$).

9.2. Teorema Fundamental: De una raíz no trivial a los factores primos de N

Supongamos que queremos factorizar un número compuesto $N = p_1 \cdot q_1$ (producto de dos primos) y hemos logrado encontrar una raíz cuadrada no trivial $x \in [2, N - 2]$ tal que $x^2 \equiv 1 \pmod{N}$. Entonces:

$$x^2 - 1 \equiv 0 \pmod{N} \implies x^2 - 1 = k \cdot N \implies (x - 1)(x + 1) = k(p_1 \cdot q_1)$$

Por el Teorema Fundamental de la Aritmética, todo número entero se descompone de forma única en factores primos:

$$x - 1 = u_1 \cdot u_2 \cdots u_r, \qquad x + 1 = v_1 \cdot v_2 \cdots v_s$$

Como por hipótesis $x \in [2, N-2]$, se cumple estrictamente que:

$$1 \leq x - 1 < N - 1 < N \quad \text{y} \quad 3 \leq x + 1 < N$$

¡Esto es crucial! Como tanto $(x-1)$ como $(x+1)$ son estrictamente menores que N, **ninguno de los dos puede ser múltiplo de N por sí solo** (es imposible que un solo paréntesis contenga simultáneamente a p_1 y a q_1). Por lo tanto, la única forma de que su producto $(x-1)(x+1)$ sea múltiplo de $N = p_1 \cdot q_1$ es que los factores primos de N se hayan repartido: uno de ellos (digamos p_1) debe dividir a $(x-1)$, y el otro (q_1) debe dividir a $(x+1)$.

Así, aplicando el algoritmo clásico de Euclides para calcular el Máximo Común Divisor, atrapamos directamente ambos factores primos de N:

$$p_1 = \text{MCD}(x - 1, N), \qquad q_1 = \text{MCD}(x + 1, N) \tag{8}$$

9.3. ¿Cómo hallamos esa raíz cuadrada no trivial? Orden Modular y Periodicidad

Para construir esa raíz no trivial x, elegimos al azar un número entero $a \in [2, N-2]$. (Primero verificamos clásicamente si $\text{MCD}(a, N) > 1$; si lo es, ya encontramos un factor de N por pura suerte. De lo contrario, a y N son coprimos).

Por el **Teorema de Euler**, si a y N son coprimos, al multiplicar a por sí mismo sucesivamente $(a^1, a^2, a^3, \dots \pmod N)$, es ley matemática que existe un menor entero positivo r (llamado el **orden de a módulo N**) tal que:

$$a^r \equiv 1 \pmod N$$

Ejemplo de orden modular: Tomemos $a = 3$ y $N = 7$. Calculamos sus potencias módulo 7:

$$3^1 \equiv 3 \pmod 7 \qquad 3^4 = 3^2 \cdot 3^2 \equiv 4 \pmod 7$$
$$3^2 = 9 \equiv 2 \pmod 7 \qquad 3^5 = 3^4 \cdot 3 = 12 \equiv 5 \pmod 7$$
$$3^3 = 27 \equiv 6 \pmod 7 \qquad 3^6 = 3 \cdot 3^5 \equiv 3 \cdot 5 = 15 \equiv 1 \pmod 7$$

Vemos que el orden es $r = 6$, y a partir de ahí la secuencia $3, 2, 6, 4, 5, 1$ se repite indefinidamente.

Es decir, si definimos la función de exponenciación modular:

$$f(i) = a^i \pmod N$$

observamos que $f(0) = 1, f(1) = a, \dots, f(r) = a^r \equiv 1 \pmod N$, y para $r+1$ se tiene $f(r+1) = a^{r+1} = a^r \cdot a \equiv 1 \cdot a = a \pmod N$. **¡El orden r es exactamente el periodo p de la función $f(i) = a^i \pmod N$!**

Si usamos nuestro circuito cuántico para hallar este periodo r, y resulta que r **es un número par**, podemos reescribir la congruencia $a^r \equiv 1 \pmod N$ como:

$$\left(a^{r/2}\right)^2 \equiv 1 \pmod N$$

Por lo tanto, definimos nuestro candidato a raíz cuadrada no trivial como:

$$x = a^{r/2} \pmod N \tag{9}$$

Siempre que r sea par y $x \not\equiv -1 \pmod N$ (lo cual la teoría de números garantiza que ocurre con probabilidad $> 50\,\%$ al elegir a al azar; si falla, simplemente se elige otro a), este valor x cumplirá $x^2 \equiv 1 \pmod N$ con $x \in [2, N-2]$, y las ecuaciones $\text{MCD}(x \pm 1, N)$ nos entregarán los factores primos de N.

9.4. Ejecución de Prueba Completa del Algoritmo de Shor: Factorizando $N = 15$

Apliquemos ahora todo el algoritmo de principio a fin sobre nuestro ejemplo práctico para descomponer $N = 15$ en sus factores primos:

1. **Elección de la base aleatoria a:** Escogemos un número al azar en el intervalo $[2, N-2] = [2, 13]$, por ejemplo $a = 7$. Verificamos que $\text{MCD}(7, 15) = 1$ (son coprimos).

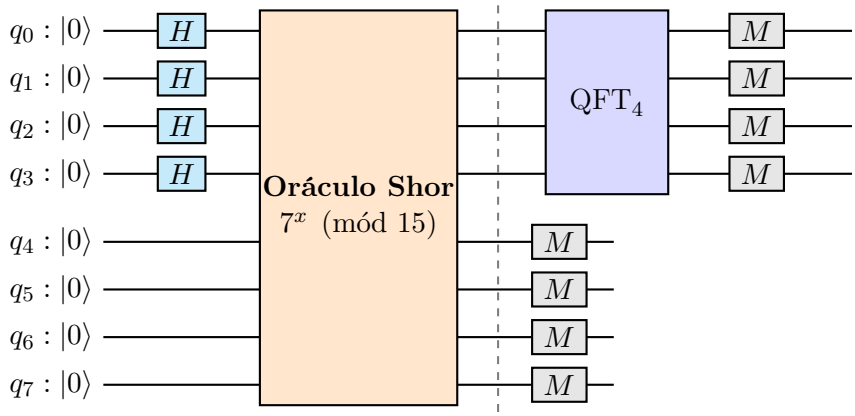
2. **Planteamiento de la función periódica:** Debemos encontrar el periodo r de la función:

$$f(x) = 7^x \pmod{15}$$

Evaluando los primeros valores para entender qué ocurre internamente en el oráculo:

x	0	1	2	3	4	5	6	7	...
$f(x) = 7^x \pmod{15}$	1	7	4	13	1	7	4	13	...

3. **Ejecución del Circuito Cuántico:** Diseñamos nuestro circuito con 4 qubits en el registro de entrada ($M = 2^4 = 16$ estados en superposición) y 4 qubits en el segundo registro para almacenar $7^x \pmod{15}$:



4. **Medición y extracción del periodo r:** Al ejecutar este circuito en Qiskit (tal como hicimos en el notebook), el registro de salida mide con igual probabilidad los estados $y \in \{0, 4, 8, 12\}$. Tomando las lecturas no nulas y aplicando el MCD:

$$\text{MCD}(4, 8, 12) = 4 \implies \frac{M}{r} = 4 \implies r = \frac{16}{4} = 4$$

5. **Cálculo de la raíz cuadrada no trivial y los factores primos:** Como el periodo hallado $r = 4$ es **par**, calculamos nuestra raíz cuadrada no trivial $x = a^{r/2} \pmod{N}$:

$$x = 7^{4/2} \pmod{15} = 7^2 \pmod{15} = 49 \pmod{15} = 4$$

Efectivamente, $x = 4 \in [2, 13]$ y cumple $4^2 = 16 \equiv 1 \pmod{15}$. Finalmente, aplicamos el MCD clásico de Euclides con $x - 1 = 3$ y $x + 1 = 5$:

$$p_1 = \text{MCD}(4 - 1, 15) = \text{MCD}(3, 15) = 3$$

$$q_1 = \text{MCD}(4 + 1, 15) = \text{MCD}(5, 15) = 5$$

¡Hemos factorizado $15 = 3 \times 5$!

10. Eficiencia del Algoritmo de Shor

Para evaluar qué tan eficiente es el algoritmo de Shor, medimos el costo en función de $n = \lceil \log_2 N \rceil$, el número de bits necesarios para escribir el entero N que queremos factorizar. Para que las fracciones continuas funcionen sin ambigüedad ($M \geq N^2$), el primer registro cuántico requiere $2n$ qubits y el segundo requiere n qubits.

Tal como plantean Rieffel y Polak, demostrar la eficiencia del algoritmo exige responder dos preguntas: **¿cuánto cuesta una ejecución?** y **¿cuántas veces hay que repetirla si algo falla?**

10.1. 1. Costo de una ejecución: El oráculo U_f es el cuello de botella

Analicemos el costo de cada etapa del algoritmo en una sola corrida:

- **Los pasos clásicos (Euclides y Fracciones Continuas):** Tanto verificar si $\text{MCD}(a, N) = 1$ al inicio, como extraer el candidato r con fracciones continuas y hallar $\text{MCD}(a^{r/2} \pm 1, N)$ al final, utilizan variantes del **algoritmo de Euclides**. Sobre números de n bits, Euclides realiza a lo sumo $\mathcal{O}(n)$ divisiones sucesivas (y como cada división clásica cuesta $\mathcal{O}(n^2)$ operaciones de bit, el trabajo clásico total es $\mathcal{O}(n^3)$).

- **La Transformada de Fourier Cuántica (QFT):** Aplicar la QFT sobre los $2n$ qubits del primer registro requiere escalonar compuertas Hadamard y rotaciones de fase controladas, sumando $\mathcal{O}(n^2)$ compuertas elementales (o $\mathcal{O}(n)$ pasos de tiempo si se ejecutan en paralelo).

- **El Oráculo de Exponenciación Modular (U_f):** Es la etapa que domina todo el tiempo de ejecución. Para calcular $a^x \pmod N$ en superposición sin hacer 2^{2n} productos, descomponemos el exponente x en sus $2n$ bits ($x = \sum_{j=0}^{2n-1} x_j 2^j$) y usamos exponenciación binaria:

$$a^x \pmod N = \prod_{j=0}^{2n-1} \left(a^{2^j}\right)^{x_j} \pmod N$$

  Esto reduce U_f a **$2n$ multiplicaciones modulares controladas** por constantes precalculadas clásicamente. Con multiplicación escolar (donde cada producto cuesta $\mathcal{O}(n^2)$ compuertas), el oráculo toma $2n \times \mathcal{O}(n^2) = \mathcal{O}(n^3)$ compuertas. Si además se emplea el algoritmo clásico más rápido conocido (multiplicación rápida de Schönhage-Strassen), este costo baja a $\mathcal{O}(n^2 \log n \log\log n)$ en tiempo y $\mathcal{O}(n \log n \log\log n)$ en espacio.

En conclusión, el tiempo de **una corrida individual** está dominado por el cálculo de U_f y es polinomial: $\mathcal{O}(n^3)$ (o $\mathcal{O}(n^2 \log n \log\log n)$ con aritmética rápida), frente al costo sub-exponencial $\mathcal{O}\left(\exp(c \cdot n^{1/3} (\log n)^{2/3})\right)$ del mejor algoritmo clásico (Criba del Cuerpo de Números).

10.2. 2. ¿Cuántas veces hay que repetir el algoritmo?

Una corrida puede no entregar los factores de N si ocurre alguno de estos cuatro eventos:

1. El periodo r hallado resulta ser **impar** (no podemos calcular $a^{r/2}$).
2. La raíz cuadrada resulta **trivial**: $a^{r/2} \equiv -1 \pmod N$, devolviendo a N como factor.
3. En el caso real, la medición y cae en una cola lateral de la sinc^2 (a distancia mayor que $1/2$ del múltiplo ideal $c\frac{M}{r}$).
4. El armónico c y el periodo r tienen un **factor común** ($\text{MCD}(c, r) > 1$), por lo que las fracciones continuas devuelven solo un divisor de r.

La teoría de números garantiza que ninguno de estos fallos obliga a repetir el proceso demasiadas veces:

- Al elegir a al azar, la probabilidad de fallar por los puntos (1) o (2) es a lo sumo 1/2 (al menos 50 % de éxito).
- En el punto (3), la campana sinc^2 concentra al menos un $\approx 40{,}5\,\%$ de probabilidad dentro de la distancia 1/2 del múltiplo ideal.
- En el punto (4), la cantidad de enteros $c < r$ coprimos con r viene dada por la función $\varphi(r)$ de Euler, que cumple $\frac{\varphi(r)}{r} \in \Omega\left(\frac{1}{\log\log r}\right)$.

Por lo tanto, basta repetir el algoritmo en promedio solo $^{**}\mathcal{O}(\log\log r)$ veces** (un número prácticamente constante en la práctica) para garantizar el éxito con alta probabilidad.

Etapa / Métrica	**Tipo de Procesamiento**	**Complejidad Asintótica** ($n = \lceil \log_2 N \rceil$)
Exponenciación Modular (U_f)	Cuántico (Oráculo)	$\mathcal{O}(n^3)$ [$\mathcal{O}(n^2 \log n \log\log n)$ rápida]
Transformada de Fourier (QFT)	Cuántico (Interferencia)	$\mathcal{O}(n^2)$ compuertas
Euclides y Fracciones Continuas	Clásico (Post-proceso)	$\mathcal{O}(n^3)$ op. de bit ($\mathcal{O}(n)$ divisiones)
Repeticiones esperadas	**Probabilístico**	$\mathcal{O}(\log\log \mathbf{r})$ **corridas**
Mejor Algoritmo Clásico (GNFS)	**Clásico**	$\mathcal{O}\left(\exp\left(\mathbf{c} \cdot \mathbf{n^{1/3}} (\log \mathbf{n})^{\mathbf{2/3}}\right)\right)$

11. Conclusiones

A lo largo de este trabajo hemos demostrado analítica y experimentalmente cómo la subrutina cuántica de búsqueda de periodo logra extraer la periodicidad global p de una función $f(x)$ en tiempo polinomial. Mediante nuestra formulación unificada, comprobamos que la Transformada de Fourier Cuántica convierte el desplazamiento desconocido x_0^* en un factor de fase unitario que se cancela al medir, concentrando la probabilidad en torno a los múltiplos de $\frac{M}{p}$. Cuando M no es divisible por p, el resto r_0 trunca el último bloque periódico y reemplaza las Deltas de Kronecker ideales por el Núcleo de Dirichlet (sinc^2), cuya cercanía al valor ideal permite recuperar candidatos p' mediante el algoritmo clásico de Fracciones Continuas.

Finalmente, esta misma arquitectura de búsqueda de periodo no se limita a la factorización de enteros: Shor demostró que una variante directa resuelve también el **Problema del Logaritmo Discreto** (comprometiendo esquemas como Diffie-Hellman, ElGamal y criptografía de Curva Elíptica), enmarcándose dentro de la clase general de **Problemas del Subgrupo Oculto**. Si bien la reducción asintótica hasta tiempo polinomial demuestra teóricamente la vulnerabilidad de la criptografía asimétrica actual, en la práctica la ejecución sobre claves reales (como RSA-2048) depende críticamente de la construcción de computadores cuánticos tolerantes a fallos con corrección de errores cuánticos.

Referencias

[1] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[2] E. G. Rieffel and W. Polak, *Quantum Computing: A Gentle Introduction*. Cambridge, MA: MIT Press, 2011.

[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th Anniversary ed. Cambridge University Press, 2010.

[4] Qiskit Contributors, "Qiskit: An Open-source Framework for Quantum Computing," IBM Quantum, 2024. [En línea]. Disponible en: `https://qiskit.org/`