

# Exploring Shor's Algorithm

David Radcliffe

MinneQuantum

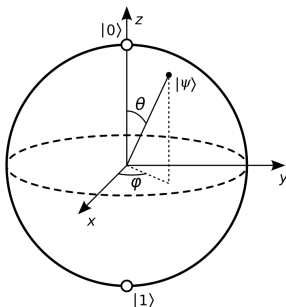
November 19, 2024

# Outline

- Review of quantum information theory
- Timeline of integer factorization
- Shor's algorithm
- Quantum order finding
  - Quantum Fourier transform
  - Quantum phase estimation
  - Continued fractions

# Qubits

- 1 A qubit (quantum bit) is the basic unit of quantum information
- 2 While a classical bit can only be  $|0\rangle$  or  $|1\rangle$ , a qubit can exist in a superposition of  $|0\rangle$  and  $|1\rangle$
- 3 When a qubit is measured, the outcome is either  $|0\rangle$  or  $|1\rangle$



# Qubit measurement

- 1 If we have a qubit in the state  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ , where  $\alpha$  and  $\beta$  are complex numbers, then:
- 2 The probability of measuring  $|0\rangle$  is  $|\alpha|^2$
- 3 The probability of measuring  $|1\rangle$  is  $|\beta|^2$
- 4  $|\alpha|^2 + |\beta|^2 = 1$  because probabilities must add to 1
- 5 After measurement, the qubit is in the state that was observed

# $n$ -qubit systems

- 1 A quantum system with  $n$  qubits has  $2^n$  basis states.
- 2 Each basis state corresponds to a possible classical configuration of the qubits, represented as a binary string of length  $n$ .

Examples:

- 1 A 1-qubit system has 2 basis states:  $|0\rangle$  and  $|1\rangle$
- 2 A 2-qubit system has 4 basis states:  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$ ,  $|11\rangle$
- 3 A 3-qubit system has 8 basis states:  $|000\rangle$  through  $|111\rangle$

We often write these states using decimal notation:  $|0\rangle$ ,  $|1\rangle$ ,  $|2\rangle$ ,  $|3\rangle$ , and so on.

# Quantum superposition

- 1 A quantum state is a superposition of basis states
- 2 Each basis state has an associated complex number called its amplitude
- 3 The sum of their squared magnitudes equals 1

When we measure a quantum state:

- 1 The result is always one of the basis states
- 2 The probability of measuring a particular basis state  $|s\rangle$  is  $|\alpha|^2$ , where  $\alpha$  is that state's amplitude
- 3 The measurement disturbs the quantum state, collapsing it to the observed basis state

# History of integer factorization

- Euclid (c. 300 BC) - Unique factorization, GCD algorithm
- Fermat (1643) - Fermat Factorization Method.  
$$M = a^2 - b^2 = (a - b)(a + b)$$
- Euler (1763) - Euler's totient function
- Gauss (1801) - Modular arithmetic, congruences
- Kraitchik (1920s) - Congruence of squares method:  
If  $M$  divides  $a^2 - b^2$  but not  $a \pm b$ , then  $\gcd(a - b, M)$  and  $\gcd(a + b, M)$  are non-trivial factors of  $M$

# Recent history of integer factorization

- Miller (1976) - Reduction of factorization to order finding
- Rivest, Shamir, Adleman (1977) - RSA encryption
- Dixon (1981) - Quadratic sieve algorithm (up to 100 digits)
- Shor (1994) - Quantum algorithm for integer factorization
- Pollard (1998) - Number field sieve algorithm (over 100 digits)
- Boudot, et al (2020) - RSA-250 factored using GNFS



# RSA encryption

RSA encryption is used to secure communications over the internet.

- 1 Compute  $M = p \cdot q$ , where  $p$  and  $q$  are large primes
- 2 Compute the totient:  $\phi(M) = (p - 1)(q - 1)$
- 3 Choose a public exponent  $e$  such that  $1 < e < \phi(M)$  and  $\gcd(e, \phi(M)) = 1$
- 4 Compute the private exponent  $d$  such that  $(d \cdot e) \bmod \phi(M) = 1$
- 5 The public key is  $(M, e)$  and the private key is  $d$
- 6 To encrypt a message  $m$ , compute  $c = m^e \bmod M$
- 7 To decrypt a ciphertext  $c$ , compute  $m = c^d \bmod M$
- 8 The security of RSA relies on the difficulty of factoring large numbers

# Multiplicative order

Assume that  $\gcd(a, M) = 1$ . If we compute successive powers

$$1, a, a^2, a^3, \dots$$

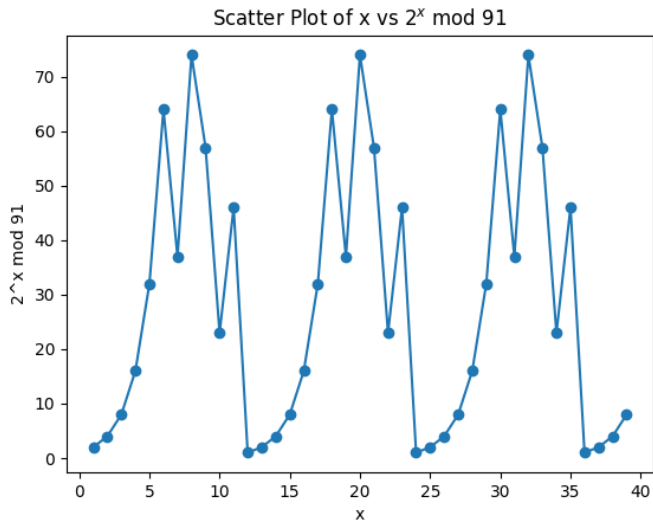
we will eventually see a repetition.

The order of  $a \bmod M$  is the smallest positive integer  $r$  such that  $a^r \equiv 1 \pmod{M}$ .

Example: Compute the order of 2 mod 15.

- $2^1 \equiv 2$
- $2^2 \equiv 4$
- $2^3 \equiv 8$
- $2^4 \equiv 1 \pmod{15}$ , so  $r = 4$ .

# Example: Powers of 2 mod 91



# Outline of Shor's Algorithm

Given a composite integer  $M$ , Shor's algorithm finds a non-trivial factor of  $M$  with high probability.

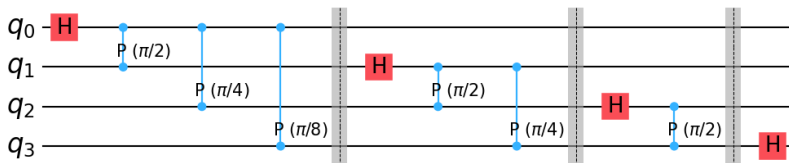
- 1 Choose a random integer  $a$  such that  $1 < a < M$ .
- 2 Compute the greatest common divisor of  $a$  and  $M$ .  
If  $\gcd(a, M) > 1$ , then we are done.
- 3 Compute the order  $r$  of  $a \bmod M$ . (How???)
- 4 If  $r$  is even, then  $M$  divides  $a^r - 1 = (a^{r/2} - 1)(a^{r/2} + 1)$ .  
Compute  $x = a^{r/2} \pmod{M}$ .
- 5 If  $m$  is odd, or if  $x = M - 1$ , go back to step 1.
- 6 Compute  $\gcd(x - 1, M)$  and  $\gcd(x + 1, M)$ .

# Quantum Fourier Transform

The quantum Fourier transform (QFT) is defined by

$$|j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k / N} |k\rangle$$

where  $N = 2^n$  is the number of basis states in the system.



# Matrix form of the QFT

$$\text{QFT}_n = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \dots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \dots & \omega^{2(N-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \dots & \omega^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \dots & \omega^{(N-1)^2} \end{bmatrix}$$

where  $\omega = e^{2\pi i/N}$  and  $N = 2^n$ .

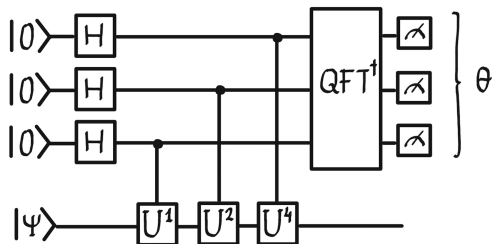
# Quantum Phase Estimation

The quantum phase estimation algorithm estimates the phase of an eigenvector of a unitary operator.

Given a unitary operator  $U$  and an eigenvector  $|\psi\rangle$  such that  $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$ , the quantum phase estimation algorithm estimates  $\theta$ .

If  $|\psi\rangle$  is not an eigenvector of  $U$ , then the algorithm will estimate the phase of a random eigenvector of  $U$ .

## QPE Circuit - Step 1

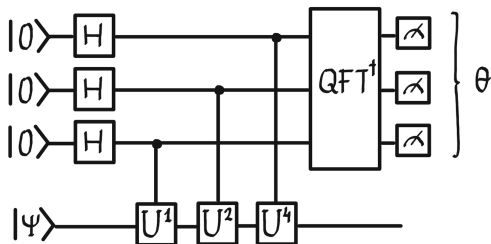


Step 1: Apply Hadamard gates to the top register, placing it in an equal superposition of all basis states.

$$|0\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle$$



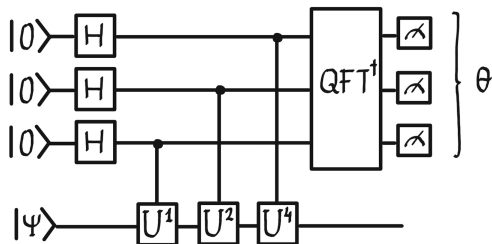
## QPE Circuit - Step 2



Step 2: Apply controlled- $U^{2^j}$  gates to the bottom register, controlled on the top register.

$$\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle |\psi\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle U^k |\psi\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i k \theta} |k\rangle |\psi\rangle$$

## QPE Circuit - Step 2



After applying the controlled- $U^{2^j}$  gates, the system state is

$$\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i k \theta} |k\rangle$$

# QPE Circuit - Step 3

Suppose that  $\theta = j/N$  for some integer  $j$ . Then the state of the top register after step 2 is

$$\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k / N} |k\rangle$$

But this is the same as applying the QFT to the state  $|j\rangle$ . Therefore, applying the inverse QFT to the top register will yield the state  $|j\rangle$ .

If  $N\theta$  is not an integer then  $j/N$  will be an approximation to  $\theta$ , with high probability.

# Quantum Order Finding

Let  $M$  be a number to be factored, and let  $a$  be a number such that  $1 < a < M - 1$  and  $\gcd(a, M) = 1$ .

We wish to find the order  $r$  of  $a \bmod M$ . We can do this using the quantum phase estimation algorithm.

Let  $U$  be a unitary operator defined by  $U|x\rangle = |ax \bmod M\rangle$  for  $x < M$ , and  $U|x\rangle = |x\rangle$  for  $x \geq M$ .

Note that since  $U^r = I$ , the eigenvalues of  $U$  are  $e^{2\pi i j / r}$  for  $j = 0, 1, \dots, r - 1$ .

# Quantum Order Finding

Apply the QPE algorithm to  $U$  and the state  $|1\rangle$ .

This yields the state  $|c\rangle$ , where  $c/N \approx j/r$  for some integer  $j$ .

To compute  $r$ , we need to find the best approximation to  $c/N$  whose denominator  $r$  is less than  $M$ . This is done using continued fractions.

# Continued fraction example

Suppose that we are factoring  $M = 21$  with  $a = 2$  and  $N = 2^{10} = 1024$ .  
QPE yields the approximation  $c/N = 171/1024 = 0.1669921875$ .

Compute the continued fraction expansion of  $171/1024$ .

$$\frac{171}{1024} = [0; 5, 1, 84, 2] = 0 + \frac{1}{5 + \frac{1}{1 + \frac{1}{84 + \frac{1}{2}}}}$$

# Continued fraction example

Truncating the continued fraction expansion yields the approximation

$$\frac{j}{r} = [0; 5, 1] = 0 + \frac{1}{5 + \frac{1}{1}} = \frac{1}{6}$$

Therefore, the order of 2 mod 21 is 6.