An Application of QPE: Order-Finding

Renato Neves

Universidade do Minho

HASLab
HIGH-ASSURANCE
SOFTWARE LABORATORY

Table of Contents

Period-Finding

The Problem

A periodic function f. Find its period.

Period-Finding

The Problem

A periodic function f. Find its period.

Problem can be difficult (particularly if f has no obvious structure, such as being trigonometric)

We will see how quantum computation tackles it

Order-Finding

Actually we tackle only a specific case $\Rightarrow$ order-finding

The latter is handled efficiently via QPE

Integer factorisation reduces to it

The only quantum component in Shor's algorithm

Table of Contents

A Handful of Definitions

Definition

We call the integer x a divisor of the integer y if $k \cdot x = y$ for some integer k

Examples

2 is a divisor of 10 and 5 is a divisor of 15. What are the divisors of a prime number?

Definition

For two integers x and y, $gcd(x, y)$ is the greatest divisor common to x and y

Examples

$gcd(8, 12) = 4$ and $gcd(10, 15) = 5$

A Handful of Definitions pt. II

Definition

Two integers x and y are called co-prime if $gcd(x, y) = 1$

Examples

8 and 9 are co-prime and 13 and 15 are co-prime as well. The integers 12 and 15 are not co-prime.

Modular Arithmetic

Definition

Given an integer N the set of integers mod N is $\{0, 1, \ldots, N-1\}$

We can think of this set as a circular circuit with different positions and where the position after $N-1$ is 0

Definition

For two integers x and y we write $x \equiv y \pmod{N}$ if $x \bmod N = y$

Examples

$5 \equiv 0 \pmod{5}$ and $6 \equiv 1 \pmod{5}$

Order-Finding

Definition

For co-prime integers $a < N$ the order of $a \pmod N$ is the smallest integer $r > 0$ s.t. $a^r \equiv 1 \pmod N$

Example

If $N = 5$ the sequence $3^0, 3^1, 3^2, 3^3, 3^4, 3^5, 3^6, \ldots$ leads to the sequence $1, 3, 4, 2, 1, 3, 4, \ldots$

Order of $3 \pmod 5$ is thus 4

Exercise

What is the order of $2 \pmod{11}$?

Table of Contents

Order-Finding

The Problem

Co-prime integers $a < N$

What is the order of $a \pmod N$?

Order-Finding

The Problem

Co-prime integers $a < N$

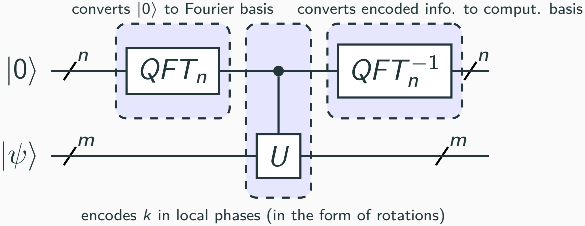
What is the order of $a \pmod N$?

Classically, problem can be difficult for large integers

Quantumly, it can be solved efficiently via QPE

QPE Revisited

Recall the QPE circuit



Need to choose suitable U and $|\psi\rangle$ to disclose the order

Table of Contents

Choosing the Right Unitary

Take co-prime integers $a < N$

Let $m = \lceil \log_2 N \rceil$ and define $U : \mathbb{C}^{2^m} \to \mathbb{C}^{2^m}$

$$U\,|x\rangle = \begin{cases} |xa \pmod N\rangle & \text{if } 0 \leq x \leq N-1 \\ |x\rangle & \text{otherwise} \end{cases}$$

Exercise

Show that $U\,|a^n \pmod N\rangle = |a^{n+1} \pmod N\rangle$

Choosing the Right Unitary

Take co-prime integers $a < N$

Let $m = \lceil \log_2 N \rceil$ and define $U : \mathbb{C}^{2^m} \to \mathbb{C}^{2^m}$

$$U \left| x \right\rangle = \begin{cases} \left| xa \pmod N \right\rangle & \text{if } 0 \leq x \leq N - 1 \\ \left| x \right\rangle & \text{otherwise} \end{cases}$$

Exercise

Show that $U \left| a^n \pmod N \right\rangle = \left| a^{n+1} \pmod N \right\rangle$

Next step is to identify suitable eigenvectors