Lecture I : Introduction

25/07/19

multiplication : easy – $O(n^2)$ for grade school

factorisation : hard – $O(N) = O(2^n)$; $N \lesssim 2^n$

N ← number, n ← number of binary digits.

Shor's Algorithm : (based on Simon's algorithm)

"Rotate, Compute, Rotate" ⇑

- "P" algorithm for factoring on a quantum computer (QC)
- Can factor RSA-1024 in 1 sec with a cell phone equivalent compute capacity
- $O(n^2)$ to factor a n-digit number
- Uses quantum mechanics (QM)
  - ↳ 1000 photons/electrons have a "state"
  - ↳ combined state is represented by $\underbrace{2^{1000}}$ numbers
    - ↳ complex amplitudes

David Deutsch ← one of the founders of QC

- Many Worlds Interpretation, Hugh Everett
  - 2^{1000} numbers in 2^{1000} parallel universes
  - most mathematically elegant although extravagant

QC can do FT on enormous numbers (1000 digits long)

Prerequisites : Linear Algebra