Shor's Algorithm - In Depth Analysis

To Factor an odd integer N (Let's choose 15) :

1. Determine if the number n is a prime
2. Or a even number,
3. or an integer power of a prime number 2.
4. If it is 2 we will not use Shor's algorithm.
5. There are efficient classical methods.
6. Choose an integer q such that $N^2 < q < 2N^2$ **let's pick 256** → 8 qubits
7. Choose a random integer x such that GCD(x, N) = 1 **let's pick 7**

atleast 1 period or sth like that

and Enough qubits to represent

- An important result from Number Theory:

$$F(a) = x^a \bmod N$$ is a periodic function in 'a'

- Choose N = 15 and x = 7 and we get the following:

We need to find the period

$$7^0 \bmod 15 = 1$$
$$7^1 \bmod 15 = 7$$
$$7^2 \bmod 15 = 4$$
$$7^3 \bmod 15 = 13$$
$$7^4 \bmod 15 = 1$$
$$\vdots$$

Shor's Algorithm - In Depth Analysis

4. Create two quantum registers (these registers must also be entangled so that the collapse of the input register corresponds to the collapse of the output register)
   - Input register: must contain enough qubits to represent numbers as large as q-1. up to 255, so we need 8 qubits
   - Output register: must contain enough qubits to represent numbers as large as N-1. up to 14, so we need 4 qubits

Shor's Algorithm - Preparing Data

5. Load the input register with an equally weighted superposition of all integers from 0 to q-1. **0 to 255**
6. Load the output register with all zeros.

The total state of the system at this point will be:

$$\underbrace{\frac{1}{\sqrt{256}}\sum_{a=0}^{255}}_{\text{Input Register}} |a, \underbrace{000}_{\text{Output Register}}>$$

Note: the comma here denotes that the registers are entangled

7. Apply the transformation x^{a} mod N to each number in the input register, storing the result of each computation in the output register.

Input Register	7^a Mod 15	Output Register
|0>	7^0 Mod 15	1
|1>	7^1 Mod 15	7
|2>	7^2 Mod 15	4
|3>	7^3 Mod 15	13
|4>	7^4 Mod 15	1
|5>	7^5 Mod 15	7
|6>	7^6 Mod 15	4
|7>	7^7 Mod 15	13

:

8. Now take a measurement on the output register. This will collapse the superposition to represent ***just one*** of the results of the transformation, let's call this value *c*.

Our output register will collapse to represent one of the following:

|1>, |4>, |7>, or |13>

For sake of example, lets choose |1>

Now things really get interesting !

9. Since the two registers are entangled, measuring the output register will have the effect of partially collapsing the input register into an **equal superposition** of each state between 0 and *q*-1 that yielded *c* (the value of the collapsed output register.)

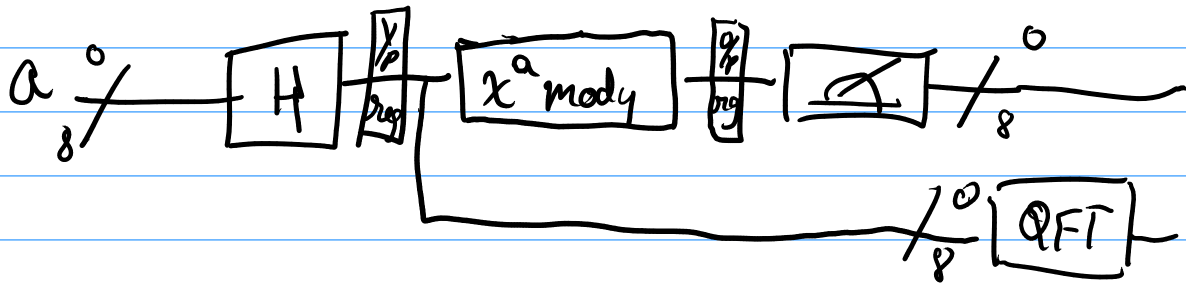
Since the output register collapsed to |1>, the input register will partially collapse to:

$$\frac{1}{\sqrt{64}}\,|0> + \frac{1}{\sqrt{64}}\,|4> + \frac{1}{\sqrt{64}}\,|8> + \frac{1}{\sqrt{64}}\,|12>, \ldots$$

The probabilities in this case are $\frac{1}{\sqrt{64}}$ since our register is now in an equal superposition of 64 values (0, 4, 8, . . . 252)

We now apply the Quantum Fourier transform on the partially collapsed input register. The fourier transform has the effect of taking a state |a> and transforming it into a state given by:

$$\frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} |c> * e^{2\pi i a c / q}$$


a
0
8
H
x^a mod y
QFT
0
8
0
8

$$|x\rangle = \frac{1}{\sqrt{256}} \Big[|0,1\rangle + |1,4\rangle + |2,7\rangle + |3,13\rangle + |4,1\rangle + |5,4\rangle + |6,7\rangle + |7,13\rangle\, |8,1\rangle \; \vdots \Big]$$

Shor's Algorithm - The Factors :)

10. Now that we have the period, the factors of N can be determined by taking the greatest common divisor of N with respect to *x ^ (P/2)* + 1 and *x ^ (P/2)* - 1. The idea here is that this computation will be done on a classical computer.

$a^P = 1 \bmod N$

$(a^P - 1) = 0 \bmod N$

$(a^{P/2} - 1)(a^{P/2} + 1) = 0 \bmod N$

We compute:

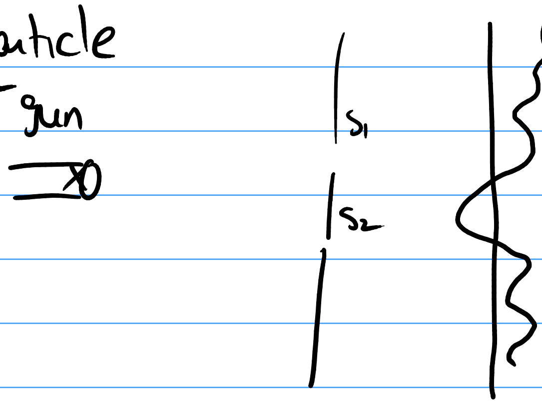
Gcd($7^{4/2}$ + 1, 15) = **5**

Gcd($7^{4/2}$ - 1, 15) = **3**

We have successfully factored 15!

Particle

e^- gun

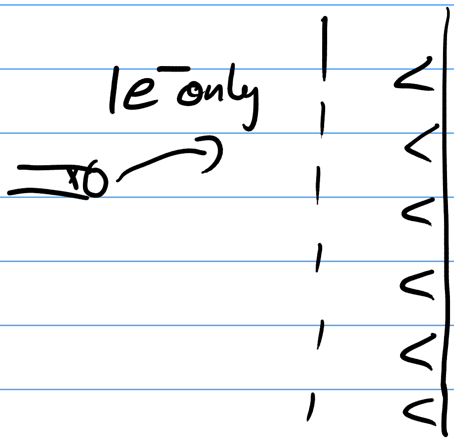


wave

wave particle duality

"probability" as to when it's striking

$1e^-$ only



will pinpoint it out, when it's striking