Factoring

Fundamental thm. of arithmetics

$\forall$ integer N, $\exists$ unique decomposition into prime numbers

$12 = 2 \times 2 \times 3$
$21 = 3 \times 7$
$17 = 17$

"Factoring" $\rightarrow$ finding these primes

Many ways: - trial division - very inefficient
- number field sieve - still ineff.

$L_N \sim e^{L/3}$

$\log_2 N$

RSA
- best known classical alg. require exper work
- easy to multiply

$\rightarrow$ "hard" problem

Results from number theory

$f(x) = a^x \bmod N$

↳ composite number

↳ any number, coprime with N

$\exists r : f(x+r) = f(x) \quad (\forall x)$

$\gcd(a^{r/2} \pm 1, N)$ is prime factors of N

Quantum algorithm: <u>find r</u>

Quantum parallelism

Say $f(x)$

$$\begin{aligned} 0 &\to 3 \\ 1 &\to 1 \\ 2 &\to 2 \\ 3 &\to 1 \\ 4 &\to 3 \\ &\vdots \end{aligned}$$

Let U_f do $|x\rangle|0\rangle \to |x\rangle|f(x)\rangle$

$$\sum_{x=0}^{7} |x\rangle|0\rangle \xrightarrow{U_f} \sum_{x=0}^{7} |x\rangle|f(x)\rangle$$

$$= |0\rangle|3\rangle + |1\rangle|1\rangle + |2\rangle|3\rangle + |3\rangle|1\rangle + |4\rangle|3\rangle + |5\rangle|1\rangle + |6\rangle|3\rangle + |7\rangle|1\rangle$$

measure 1st register : randomly 0 ... 7

2nd register : 1 or 3

FFT

$x_0, \ldots, x_{N-1} \rightarrow y_0 \cdots y_{N-1}$

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \, e^{2\pi i \left(\frac{jk}{N}\right)}$$

Examples: *

	1 0 0 0 0 0 0 0	→	1 1 1 1 1 1 1 1
	1 0 0 0 1 0 0 0	→	1 0 1 0 1 0 1 0
	1 0 1 0 1 0 1 0	→	1 0 0 0 1 0 0 0
	1 1 1 1 1 1 1 1	→	1 0 0 0 0 0 0 0
	per. Ω	→	per. N/Ω
*	1 0 0 0 1 0 0 0	→	1 0 1 0 1 0 1 0
	0 1 0 0 0 1 0 0	→	1 0 $-i$ 0 -1 0 i 0
	0 0 1 0 0 0 1 0	→	1 0 -1 0 1 0 -1 0
	0 0 0 1 0 0 0 1	→	1 0 $+i$ 0 -1 0 $-i$ 0
	0 1 0 1 0 1 0 1	→	1 0 0 0 -1 0 0 0

INVERTS PERIOD

REMOVES OFFSET

QFT

$$|x\rangle \to \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i \frac{xy}{N}} |y\rangle$$

$$|000\rangle \to |000\rangle + |001\rangle + |010\rangle + \dots + |111\rangle$$

$$|000\rangle + |100\rangle \to |000\rangle + |010\rangle + |100\rangle + |110\rangle$$

$$|001\rangle + |101\rangle \to |000\rangle - i|010\rangle - |100\rangle + i|110\rangle$$

etc.

Back to example:

After U_f: $(|0\rangle + |2\rangle + |4\rangle + |6\rangle)|3\rangle + (|1\rangle + |3\rangle + |5\rangle + |7\rangle)|1\rangle$

QFT $\to$ $(|0\rangle + |4\rangle)|3\rangle + (|0\rangle - |4\rangle)|1\rangle$

Meas. 1st register: 0, or 4 $\qquad k\frac{N}{r} = k\frac{8}{2} = k4$

$k\frac{256}{2} = k\,128$

$$\frac{1}{4}\left[\begin{array}{cccc|c} 1 & 0 & 0 & 1 & \\ 1 & & & 1 & 0 \\ \hline & & & & \\ 0 & & & 0 & \end{array}\right] + \frac{1}{4}\left(\begin{array}{cc|c} 1 & -1 & \\ -1 & 1 & \\ \hline & & \end{array}\right) = \frac{1}{2}\left[\begin{array}{cc|c} 1 & 0 & \\ 0 & 1 & 0 \\ \hline & & \\ 0 & 0 & \end{array}\right]$$

Algorithm period finding

NaC 5, Berenco, quant-ph/9612014

① Init to $\underbrace{|0\rangle}_{2L}\underbrace{|0\rangle}_{L}$

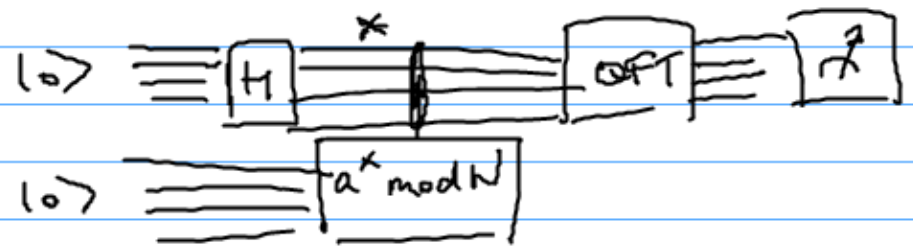
② Hadamard $\frac{1}{2^L}\sum_{x=0}^{2^{2L}-1}|x\rangle|0\rangle$

③ $U_f \rightarrow \frac{1}{2^L}\sum_{x=0}^{2^{2L}-1}|x\rangle|f(x)\rangle$ $\rightarrow$ mod. expon NaC box 5.2

$\hat{a},N$

$= \frac{1}{\sqrt{r}}\sum_{j=0}^{2^{2L}/r}|jr+\ell\rangle|f(\ell)\rangle$

④ QFT $\rightarrow \frac{1}{\sqrt{r}}\sum_{j=0}^{r}\exp\left(2\pi i\frac{\ell j}{r}\right)|j\,\tfrac{2^{2L}}{r}\rangle|f(\ell)\rangle$ $\rightarrow$ NaC 5.1



More general: hidden subgroup