Quantum Factoring Algorithm

1. f is efficiently computable classically

   $\Rightarrow$ eff. quantum ckt. which on input $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle|y\rangle$ outputs $\sum_x \alpha_x |x\rangle|y \oplus f(x)\rangle$

2. QFT mod $N = 2^n$

   $F_N = \frac{1}{\sqrt{2^n}}\left(\omega^{ab} \right)$ $\quad |a\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{b=0}^{N-1} \omega^{ab} |b\rangle$ $\quad |\phi\rangle \rightarrow \boxed{F_N} \rightarrow F_N|\phi\rangle$

   size $O(n^2)$

Factoring: Given number $N = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, split $N = N_1 N_2$.

length of N is $\lceil \log N \rceil = n$.

trying divisors $2, 3, 4, 5, \ldots$, stopping at $\sqrt{N}$ takes $2^{n/2}$.

since # primes $\leq M$ is $\frac{M}{\log M}$ just trying primes only removes a log factor

Best classical algorithms: $2^{\sqrt{n}}$ proven

$2^{\sqrt[3]{n}}$ proven assuming number thy. conjectures

Say $N = p \cdot q$.

1) Find a nontrivial $\sqrt{1}$ mod N.

eg. $N = 15$ $\quad \pm 1, \pm 4$ $\quad -1 \equiv 14 \quad -4 \equiv 11$ $\qquad x^2 \equiv 1 \pmod N$, $x \not\equiv \pm 1 \bmod N$

$N \mid (x^2 - 1) = (x-1)(x+1)$, $\quad N \nmid x+1$, $N \nmid x-1$.

eg. $15 \mid 4^2 - 1 = \underset{\substack{\shortparallel \\ 5}}{(4+1)}\underset{\substack{\shortparallel \\ 3}}{(4-1)}$, $\quad 15 \mid 11^2 - 1 = \underset{\substack{\shortparallel \\ 2\cdot 5}}{10} \cdot \underset{\substack{\shortparallel \\ 4\cdot 3}}{12}$

let $N_1 = \gcd(N, x+1)$, $\quad N = N_1 \cdot N_2$.

Quantum: poly(n) steps, in particular $O(n^3)$, can be optimized

Overview: $f(N, a)$ easy to compute $\quad 0 < a < N^2$

we'll create a large superposition, from which we can extract a pattern $\equiv \sqrt{1}$ mod N.

Chinese Remainder Theorem $\qquad \mathbb{Z}_{pq} \simeq \mathbb{Z}_p \times \mathbb{Z}_q$

$a \bmod N \leftrightarrow (a \bmod p, a \bmod q)$

$1 \bmod N \leftrightarrow (1, 1)$

$-1 \leftrightarrow (-1, -1)$

$\left.\begin{array}{l}(1,-1) \\ (-1,1)\end{array}\right\}$ the other two $\sqrt{\ }$s of 1.

since $a \leftrightarrow (x, y)$, $b \leftrightarrow (u, v)$, $ab \leftrightarrow (xu, yv)$

symmetry between p & q broken so we can factor N.

Lemma: N odd, x mod N picked at random. If $\gcd(x, N) = 1$, then with prob. $\geq 1/2$,

1. order$(x) = r$ is even $\quad$ (r the minimum # : $x^r \equiv 1$ mod N) $\quad$ eg. $4^2 \equiv 1$, $7^4 \equiv 1$
2. $x^{r/2} \not\equiv -1$ mod N

~ since equivalent to picking random #s mod p, and mod q

The function we compute is $f(N, x, a) = x^a \bmod N$. (fixed: N, x)

eg. $N=15$, $x=7$

$a = 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad \ldots$

$x^a = 1 \quad 7 \quad 4 \quad 13 \quad 1 \quad 7 \quad 4$

the period of this pattern is the order of x (which is exponentially large). If we compute this order, then with probability $1/2$ we're done.

Computing $x^a \bmod N$ is efficient, $O(n^3)$.

$x \cdot y \bmod N$ — $O(n^2)$

multiplying $\underbrace{x \cdot x \cdot x \cdots x}_{a \text{ times}} \bmod N$ is $O(an^2)$

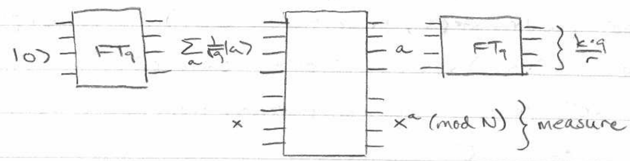
so subdivide it

$$\left.\begin{array}{l} x^2 \bmod N \\ (x^2)^2 = x^4 \bmod N \\ (x^4)^2 = x^8 \bmod N \\ \vdots \end{array}\right\} O(\log a \cdot n^2) = O(n^3)$$

x^{00001_2}, x^{00010_2}, x^{00100_2}, $\vdots$

to add exponents, multiply the numbers
eg. $a = 10010_2$

Simplifying assumption: Know large q: $r \mid q$.



eg. $N=15$, $x=7$, measure $|4\rangle$, the first register collapses to

$|2\rangle + |6\rangle + |10\rangle + |14\rangle$

in general, a sequence with period r

Applying FT_q, get $\frac{k \cdot q}{r}$

k random, so $\gcd(k, r) = 1$ whp.

$\gcd(k\frac{q}{r}, q) = \frac{q}{r} \Rightarrow$ know r

$\Rightarrow \gcd(N, x^{r/2}+1)$

Indeed, start with

$\frac{1}{\sqrt{q/r}} \sum_{\ell=0}^{\frac{q}{r}-1} |k+\ell r\rangle$ $\quad 0 \quad k \quad k+r \quad k+2r \quad \ldots$

$\xrightarrow{FT_q} \sum_{\ell=0}^{\frac{q}{r}-1} \frac{\sqrt{r}}{q} \sum_{b=0}^{q-1} \omega_q^{b(k+\ell r)} |b\rangle$

amplitude of b is $\alpha_b = \frac{\sqrt{r}}{q} \omega_q^{kb} \sum_{\ell=0}^{\frac{q}{r}-1} \omega_q^{\ell r b}$

when is $|\alpha_b|$ large? if $b = \frac{kq}{r}$, $\frac{\sqrt{r}}{q} \sum_{\ell=0}^{\frac{q}{r}-1} \omega_q^{\ell r \frac{kq}{r}} = \frac{\sqrt{r}}{q} \cdot \frac{q}{r} = \frac{1}{\sqrt{r}}$

there are exactly r such numbers, each w/prob. $\frac{1}{r}$ → so always get one of th

Summary — period changes from r to q/r