1. f is efficiently computable classically

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

2. QFT mod $N=2^n$

$F_N = \frac{1}{\sqrt{2^n}}\left(\omega^{ab}\right)$ $\quad |a\rangle \to \frac{1}{\sqrt{N}}\sum_{b=0}^{N-1}\omega^{ab}|b\rangle$ $\quad |\phi\rangle \to \boxed{F_N} \to F_N|\phi\rangle$ 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 $\le M$ 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. $N=15$ $\quad \pm 1, \pm 4$ $\quad -1\equiv 14 \quad -4\equiv 11$ $\quad x^2\equiv 1 \pmod N$, $x \not\equiv \pm 1 \bmod N$

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

eg. $15 \mid 4^2-1 = (4+1)(4-1)$ (11: 5, 11: 3), $15 \mid 11^2-1 = 10\cdot 12$ (11: $2\cdot 5$, 11: $4\cdot 3$)

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

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

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

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

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

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

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

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

$(1,-1)$ } the other two $\sqrt{1}$s of 1.

$(-1,1)$ 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. $\ge 1/2$,

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

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

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

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

$a=$	0	1	2	3	4	5	6	...
$x^a=$	1	7	4	13	1	7	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

$x^2 \bmod N$ — x^{00001_2}

$(x^2)^2 = x^4 \bmod N$ — x^{00010_2}

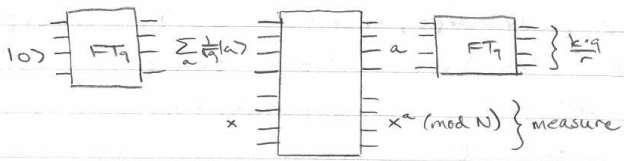
$(x^4)^2 = x^8 \bmod N$ — $O(\log a \cdot n^2) = O(n^3)$

x^{00101_2}

to add exponents, multiply the numbers

eg. $a = 100101_2$

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.

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

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

Indeed, start with

$\frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} |k + \ell r\rangle$ (0, k, k+r, k+2r, ...)

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

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

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

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

Summary — period changes from r to q/r