Wrap-up of quantum factoring.

We have $x \in \mathbb{Z}_n^*$

Trying to find the order of x.

Main tool: Quantum Fourier Transform

Start with $q =$ a power of 2

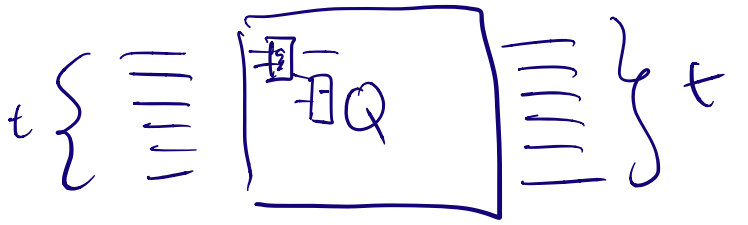
$\approx n^2$.

$$F = \frac{1}{\sqrt{q}} \begin{array}{c} \\ a \end{array} \begin{array}{c} \begin{array}{c} q \quad\quad b \end{array} \\ \begin{bmatrix} & \vdots \\ & \\ \cdots & \omega^{a \cdot b} \end{bmatrix} \end{array} \qquad \omega = e^{\frac{2\pi i}{q}}.$$

F is Unitary.

Fact: Let $t = \log_2 q$.

F is a $2^t \times 2^t$ matrix representing a transformation on t bits, computable by a quantum ckt of size poly(t).



Start with the state

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle|0\rangle$$

some $\log n$ bit register with all 0's.

$|a\rangle$: all t bit strings.

↓

Classical alg for computing modular exponentiation

$a \mapsto (x^a \bmod n)$

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle |x^a \bmod n\rangle$$

$\downarrow$ QFT on the first register.

$$|a\rangle \to \frac{1}{\sqrt{q}} \sum_{b=0}^{q-1} \omega^{ab} |b\rangle$$

$$\frac{1}{q} \sum_{a=0}^{q-1} \sum_{b=0}^{q-1} \omega^{ab} |b\rangle |x^a \bmod n\rangle$$

$$\| $$

$$\frac{1}{q} \cdot \sum_{h \in \langle x \rangle \subseteq \mathbb{Z}_n^*} \sum_{b=0}^{q-1} \left(\sum_{\substack{a \text{ s.t.} \\ x^a \bmod n \\ = h}} \omega^{ab} \right) |b\rangle |h\rangle$$

Question: For which (b, h) is

$$\frac{1}{q^2}\left|\sum_{\substack{0\le a\le q-1\\ x^a\equiv h \pmod n}} \omega^{ab}\right|^2 \quad \text{big / small.?}$$

View $h \in \{0,1,\dots,n-1\}$. Let $r = \mathrm{ord}_n(x)$

$$\{a:\ x^a \equiv h \pmod n\} = \{a_0, a_0+r, a_0+2r, \dots, a_0+\left(\approx\frac{q}{r}\right)r\}$$

$$\frac{1}{q^2}\left|\sum_{\substack{0\le a\le q-1\\ x^a\equiv h \pmod n}} \omega^{ab}\right|^2$$

$$= \frac{1}{q^2}\left|\sum_{j\le \approx\frac{q}{r}} \omega^{(a_0+jr)\cdot b}\right|^2$$

$$= \frac{1}{\quad}\left|< \quad \omega^{jrb}\right|^2$$

$$q^2 \Big| \sum_{j \le \alpha \frac{q}{n}} \sim 1$$

$$= \frac{1}{q^2} \left| 1 + \omega^{nb} + \omega^{2nb} + \cdots + \omega^{\left(\alpha \frac{q}{n}\right) \cdot nb} \right|^2$$

$$\cdots \quad (*)$$

If b is s.t. nb is $\in \{0, \pm 1, \pm 2, \ldots, \pm \frac{n}{10}\}$ mod q,

then $(*)$ has magnitude

$$\geq \alpha \frac{1}{10} \left(\frac{q}{n}\right)^2 \cdot \frac{1}{q^2} \approx \frac{1}{10} \cdot \frac{1}{n^2}.$$

—

Summary b's s.t. $\exists$ u with

(0) $$|nb - uq| < \frac{n}{10}$$

have the property that $\forall h \in \langle x \rangle \subseteq \mathbb{Z}_n^*$

$$\Pr[(b,h) \text{ is seen}]$$

$$\geq \frac{1}{10} \cdot \frac{1}{10}.$$

$$< \frac{1}{10n^2}$$

Given such a b, satisfying (*);

let us find a.

$$\left| \frac{b}{q} - \frac{a}{n} \right| < \frac{1}{10q} < \frac{1}{n^2}$$

Run continued fraction alg to find good rational approximations to b/q with denominator $< n$.

There is at most one with dist $< \frac{1}{n^2}$ from $\frac{b}{q}$.

That must be $\frac{u}{r}$, but with common factors between u, r cancelled.

If we knew that u is relatively prime to r, then we would be happy., and we found r.

Final Claim There are many (b,h) pairs s.t. $\exists\, u$ relatively prime to r s.t.

$$|rb - uq| < \frac{r}{10}.$$

Proof Pick any $u < r$ which is relatively prime to r.

Consider $uq \pmod{r}$

Claim: About $1/5$th of the u's like this are s.t. $|rb - uq| < \frac{r}{10}$.

where rb is the multiple of r closest to uq.

$$\left| \{ u : u < r, \quad GCD(u, r) = 1 \} \right|$$

$$\geq \Omega\left(\frac{r}{\log \log r} \right)$$

$\frac{1}{5}$th of these u's give rise to a b with the desired property.

For Each b, any of the values of h make (b, ba) a good pair.

So $\geq \Omega\left(\frac{r^2}{\log\log r}\right)$ such (b,h) pairs.

Total prob. that one such (b,h) pair is sampled by the alg.

is $\geq \Omega\left(\frac{r^2}{\log\log r}\right) \cdot \frac{1}{10 r^2}$

$$\geq \frac{1}{\log\log r} \geq \frac{1}{\log\log n}$$

So $(\log\log n)$ repetitions will likely give such a (b,h) pair.