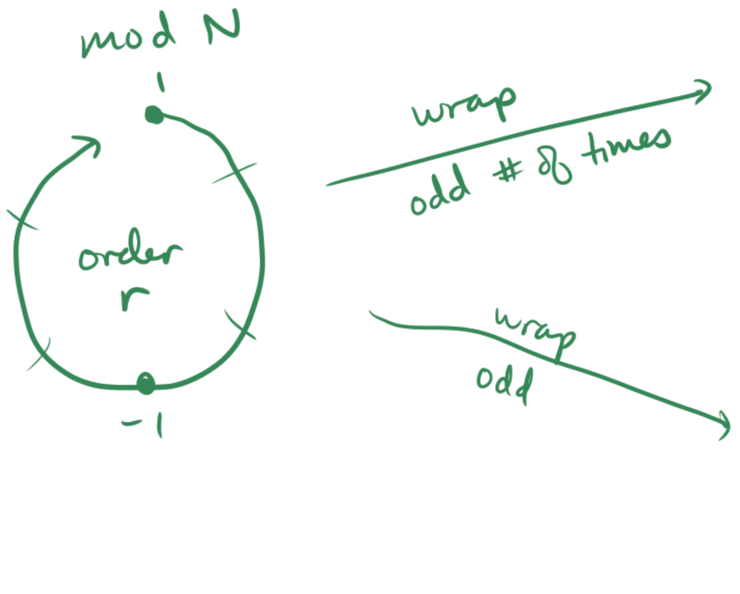
Proposition Let $N = pq$, p, q odd primes.

Then $\text{Prob}\left(\text{ord}(x) \text{ is even and } x^{\frac{\text{ord}(x)}{2}} \not\equiv -1 \pmod N \right) \geq \frac{1}{2}$ as x ranges over $(\mathbb{Z}/N\mathbb{Z})^*$.

Proof. Suppose $\text{ord}(x)$ is even and $x^{\frac{\text{ord}(x)}{2}} \equiv -1 \pmod N$. (bad case #1)

Mult. dyn. of x: $\left[(\mathbb{Z}/N\mathbb{Z})^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^* \text{ Ch. Re. Thm.} \right]$



-1 appears in a cycle mod p

$\iff x^{r/2} \equiv -1 \equiv g^{\frac{p-1}{2}}$

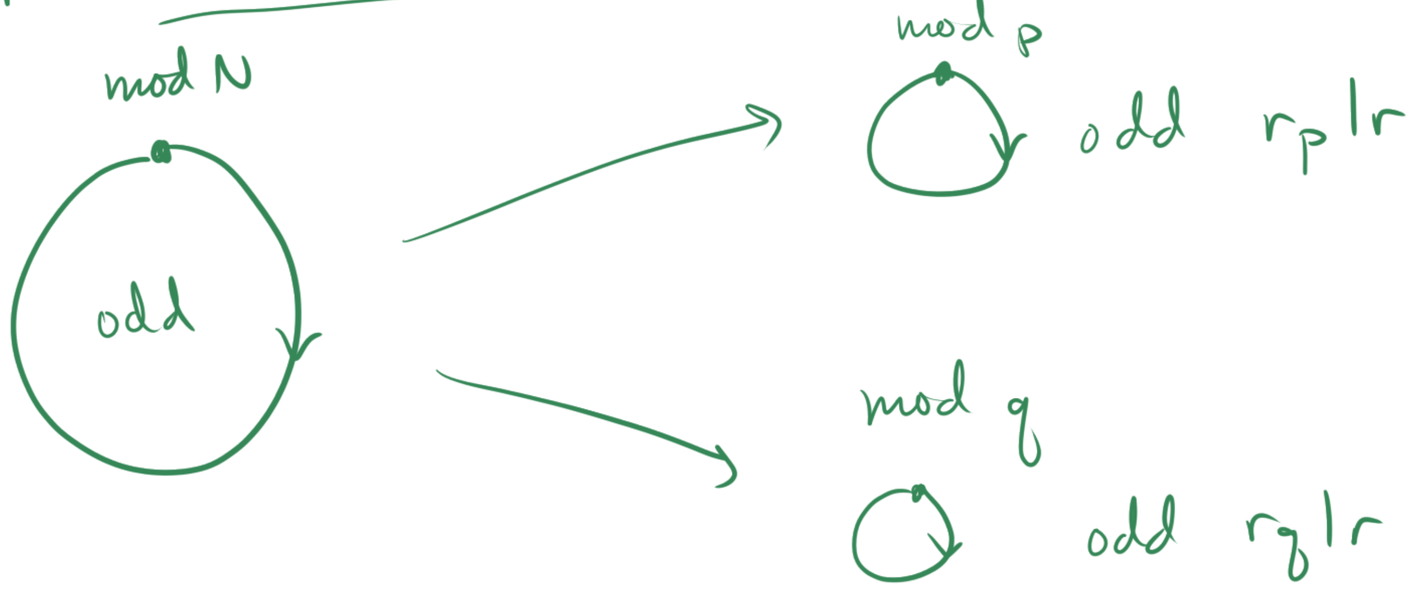
$\iff x = g^s$ where $s \mid \frac{p-1}{2}$.

$p - 1 = 2^{\sim}(\text{odd})$

This occurs at most $\frac{1}{2}$ of the time.

So at most $\frac{1}{4}$ of the residues of $(\mathbb{Z}/N\mathbb{Z})^*$ have this property mod p & mod q i.e. land in this case.

Suppose ord(x) is odd. (bad case #2)



cycle size is odd mod p

$\Rightarrow$ $x = g^k$ where k is even

} if k odd, then $k r_p \equiv 0 \pmod{p-1}$ ↶ even. →←.

This occurs $\frac{1}{2}$ the time.

So this "bad case" (mod N) occurs $\leq \frac{1}{4}$ of the time.

□

Shor's Algorithm (to factor N)

classical (1) Take a random α mod N, $\alpha \neq 0$.

quantum (2) Find the order of r in $(\mathbb{Z}/N\mathbb{Z})^*$. ($\alpha^r \equiv 1 \bmod N$)

ie. period of $x \mapsto \alpha^x \bmod N$

classical (3) Check if r is even, and $\alpha^{r/2} \not\equiv \pm 1 \pmod N$. } Luck (If not, change α, try again.)

classical (4) If so, take $\gcd(\alpha^{r/2} - 1, N)$.

Period Finding on a Quantum Computer

Given: $f: \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ s.t. $\boxed{f(x)=f(y) \iff x \equiv y \pmod r}$

Goal: find r.

Initialize 2 registers of qubits: { 1st register m_0 qubits; 2nd register n_0 qubits } to $|0\rangle|0\rangle$

$|x\rangle = |\overbrace{\text{binary exp of } x}^{m_0}\rangle$ $\quad m = 2^{m_0}$ $\quad n = 2^{n_0}$

$$|0\rangle|0\rangle \xrightarrow[\text{on 1st reg.}]{QFT_m} \frac{1}{\sqrt{m}} \sum_{x=0}^{m-1} |x\rangle|0\rangle$$

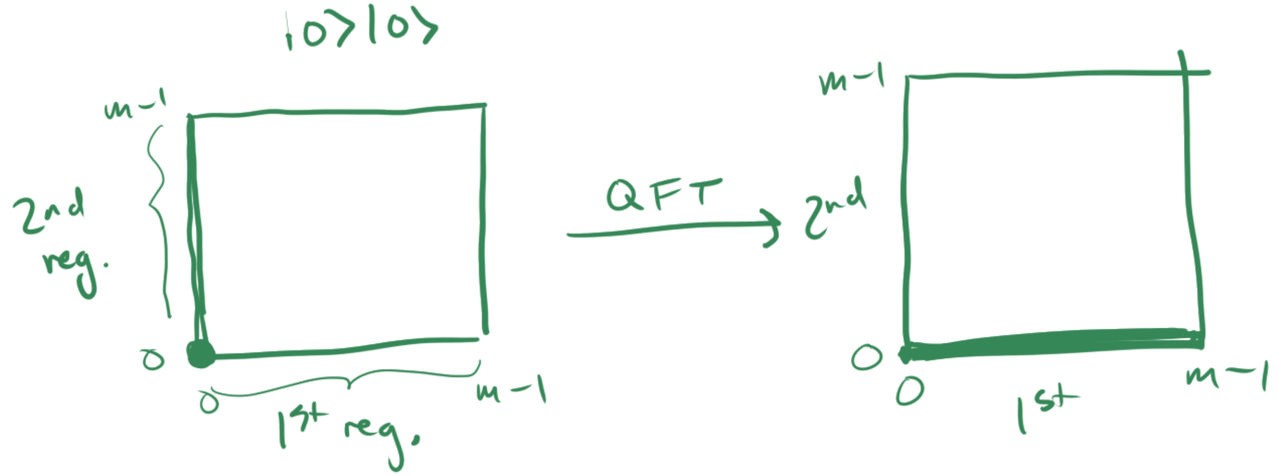
$$\xrightarrow{U_f} \frac{1}{\sqrt{m}} \sum_{x=0}^{m-1} |x\rangle|f(x)\rangle$$

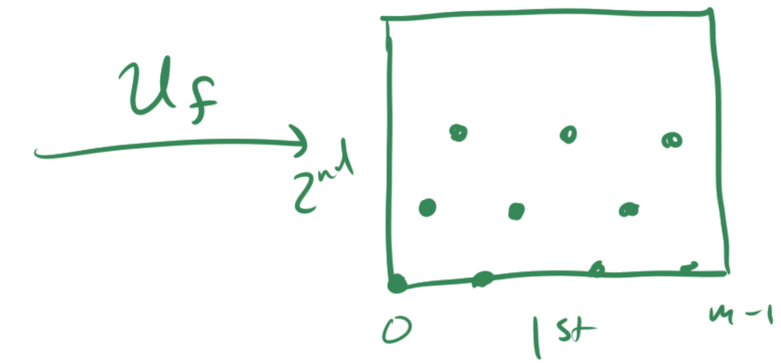
$$\xrightarrow[2^{nd}]{\text{measure}} \frac{1}{\sqrt{m/r}} \sum_{k=0}^{m/r-1} |\ell+kr\rangle|f(\ell)\rangle$$

for some ℓ we can't control

$$\xrightarrow[\text{on 1st reg.}]{QFT_m} \frac{1}{\sqrt{m}} \frac{1}{\sqrt{m/r}} \sum_{y=0}^{m-1} \sum_{k=0}^{m/r-1} \omega_n^{(\ell+kr)y} |y\rangle|f(\ell)\rangle \xrightarrow[1^{st}]{\text{msr}}$$

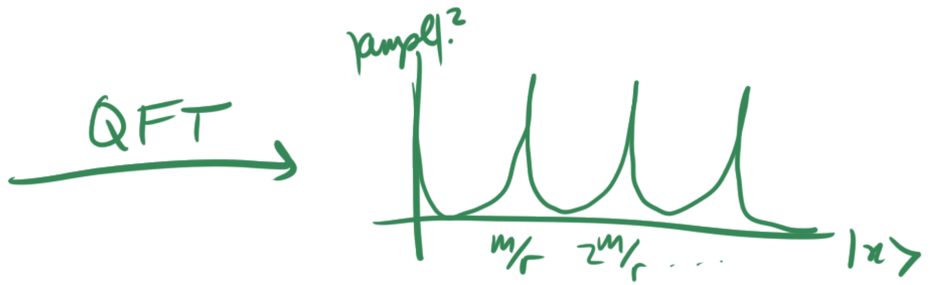
get a peak value for y





graph $f(x)$

$|x\rangle|f(x)\rangle$

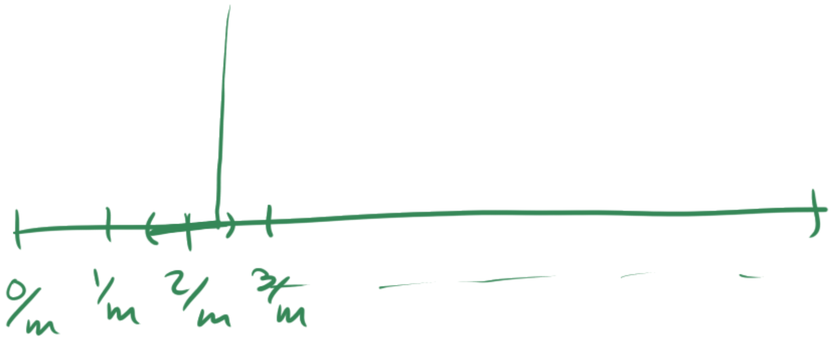


msr → get a peak in $\frac{m}{r}\mathbb{Z}$

Question: Having measured y, how to get r?

We are most likely to measure y s.t.

$$\left|\frac{y}{m} - \frac{c}{r}\right| < \frac{1}{2m}.$$



Diophantine Approximation & Continued Fractions

$\exists$ an efficient algorithm (continued fractions) given $\alpha \in \mathbb{R}$,

to find all $p/q \in \mathbb{Q}$ s.t. $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$

(Finds $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_k}{q_k}, \ldots$ in time $O(k)$ for $\frac{p_k}{q_k}$)

So take $m > r^2$ (enough qubits)

then $\left|\frac{y}{m} - \frac{c}{r}\right| < \frac{1}{2m} < \frac{1}{2r^2}$ i.e. $\frac{c}{r}$ will appear in the list.

$$\pi = 3 + 0.1415\ldots$$

$$= 3 + \frac{1}{7.0625\ldots}$$

$$= 3 + \frac{1}{7 + 0.0625\ldots}$$

$$= 3 + \frac{1}{7 + \frac{1}{15.996\ldots}}$$

3

$$3 + \frac{1}{7} = \frac{22}{7}$$

$$3 + \frac{1}{7 + \frac{1}{15}} = \frac{333}{106}$$

etc.