Then $\hat{f} = \sum_{x=0}^{m-1} \frac{1}{\sqrt{r}} |x, f_x\rangle$ if $x = 0 \bmod m/r$, $0|x\rangle$ otherwise

Why?

$$\frac{1}{j} \times \left(\overbrace{\omega^{jk}}^{QFT_k} \right) \left(f \right) = \left(\hat{f} \right)$$

f is

$$\begin{pmatrix} \sqrt{r/m} \\ 0 \\ 0 \\ 0 \\ 0 \\ \sqrt{r/m} \\ 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \begin{matrix} \text{at } 0 \cdot r \\ \\ \\ \\ \\ 1 \cdot r \\ \\ \\ \\ \\ (m/r - 1) \cdot r \end{matrix}$$

So the ω that matter for QFT at entry x are

$$\omega^{0rx} \quad \omega^{1rx} \cdots \omega^{(m-1)rx}$$

row ↓ col ↓

$$\hat{f}(x) = \sqrt{r/m} \sum_{l=0}^{m/r-1} \omega^{x\,l\,r}$$

$$\sum_{l=0}^{m/r-1} \omega^{xlr} = \frac{\omega^{mx}-1}{\omega^{rx}-1}$$

$$\omega^m = 1 \quad \text{so} \quad (\omega^m)^x = \omega^{mx} = 1$$

Numerator is always 0!

When do pos. amplitude come from?
When denom is 0

$$\omega^{rx} = 1 \quad \text{when } x = {}^{k\,m}/_{r}$$
for some k

$$\lim_{x \to {}^{k\,m}/_{r}} \frac{\omega^{mx}-1}{\omega^{rx}-1} \cdots = {}^{m}/_{r}$$

We see pos amplitude @ $x = {}^{m}/_{r}$ only
& there are r entries like that

$$\hat{f}(x) = \begin{cases} 1/r & x = 0 \bmod m/r \\ 0 & \text{otherwise} \end{cases}$$

□

So sampling $\hat{f}$ gives us some mult of m/r

$m = 100$ (we choose) $\quad r = 5$ (secret) $\quad m/r = 20$

we see 60 maybe

If we start over, we get some f whose pos ampl. are at different places But the distance between them is the same, $r = 5$

If we sample the new $\hat{f}$ we see some mult of m/r, say 60

$\gcd(60, 40) = 20$ so we know this now

$r = m/(m/r) = 100/20 = 5$!

We need to show that period-finding can help with factoring [Shor]

Factoring

Given $N = 60$

Factor $2^2 \cdot 3 \cdot 5$

$$p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

$p_1 - p_k$ prime factors

Most difficult $N = P \cdot Q$

P & Q odd & of same size

RSA a/g public/private Key

$P \cdot Q \to N$ easy

Finding P & Q hard!

Best known $\in O(2^n)$ a/g to factor

n = # bits

We don't know if it can be done in poly time

Ex $N = 21 = 3 \cdot 7$

Write $a \equiv b \pmod N$
remainder after div by $N = b$

$24 \equiv 3 \pmod{21}$
$35 \equiv 14 \pmod{21}$
$20 \equiv 20 \pmod{21}$
$\equiv -1 \pmod{21}$

$+ \; - \; \cdot$ preserved in mod. arith

Arith mod N efficient
gcd(a,b)

gcd(15, 21) $= 3$
$3 \cdot 1 \quad 3 \cdot 7$

Euclid's alg
$21 = 1 \cdot 15 + 6$
$15 = 2 \cdot 6 + 3 \leftarrow$ gcd
$6 = 2 \cdot 3 + 0$

gcd is fast too

$N = 21$

Key soln $x^2 = 1 \mod 21$

FIND x

x is a non-trivial root of N

If $x^2 \equiv 1 \pmod N$
and $x \neq \pm 1$

$x = 8 \quad 64 \mod 21 \equiv 1$

$\gcd(8+1, 21)$ & $\gcd(8-1, 21)$

will be factors of 21

$\gcd(9, 21) = 3$ voila!
$\gcd(7, 21) = 7$

Lemma Factoring is equiv to finding Nontrivial x | $x^2 = 1 \pmod N$

Pf $x \neq \pm 1$ & $x^2 = 1 \pmod N$

then $x^2 - 1 = 0 \pmod N$
So $x^2 - 1$ is a multiple of N
63 is a mult of 21

$x^2 - 1 = (x+1)(x-1)$
N $(x+1)(x-1) = kN$
$9 \cdot 7 = 3 \cdot 21$

$$N = \frac{(x+1)(x-1)}{K}$$

GCD $(x+1, N)$ } factors of N
GCD $(x-1, N)$ }

We need to find x

the order of int x mod N is the smallest $r > 0$ such that

$$x^r = 1 \pmod N$$

Examples

2 mod 3

$2^1 \bmod 3 = 2$
$2^2 \bmod 3 = 1$ ✓

3 mod 5

$3^1 \bmod 5 = 3$
$3^2 \bmod 5 = 4$
$3^3 \bmod 5 = 2$
$3^4 \bmod 5 = 81 = 1$ ✓

$f(i) = x^i \bmod N$ is periodic

$f(i) = 2^i \bmod 3$

i	$2^i \bmod 3$	
0	1	Next "1" at period of $f(i)$
1	2	
2	1	
3	2	
4	1	

i	$3^i \bmod 5$	
0	1	period 4
1	3	
2	4	$3^4 \bmod 5 = 1$
3	2	
4	1	
5	3	
6	4	
⋮	⋮	

How do we find an

$$x \mid x^2 = 1 \bmod N ?$$

Find

$$x^s \mid x^s = 1 \bmod N$$

this is the order of x

If s is even we get

$(x^{s/2})^2 = 1 \bmod N$ & win

Otherwise need to try again
For random x
$P(s \text{ even}) \sim 1/2$

So we can keep trying

Shor
Need m qubits / $2^m >> N^2$
Because we need to see the period of $x^i \bmod N$ & it could be as large as N

1) Pick random x
2) Quantum $f(i) = x^i \bmod N$
3) Fourier sample to get period (order) of f [may take a few runs]
4) Order even? Try again

Compute $\frac{gcd(N, x+1)}{gcd(N, x-1)}$ to get Factors

Time to compute period poly in m qubits
Time to factor is poly in $\log N$ (# bits for N)