IV) $$\sum_{x'} |x', y\rangle = \sum_{j} |\ell + jr\rangle |y\rangle$$

$k^{x'} \equiv y \pmod N$ $\qquad$ $j = 0, 1, 2, \ldots, \approx \frac{2^m}{r} - 1$

V) In a very simplified way, QFT (Quantum Fourier Transform) will take the state

$$\sum_{j} |\ell + jr\rangle \text{ to } \sum_{j'} |j' \tfrac{2^m}{r}\rangle$$

(very close)*

↑ an ordinary FT implemented by an efficient quantum circuit

* we didn't discuss why it is only "close to" in general

VI You measure a particular value

$$a = j' \frac{2^m}{r}, \text{ for some } j'$$

$j' \in 0, 1, \ldots, r-1$

If a has this form exactly, we can omit the continued fraction expansion based on the ratio $\frac{a}{2^m}$

and can conclude directly:

if $a \neq 0$ and $\gcd(j', r) = 1$ this happens with high probability ...

then $$r = \frac{2^m}{\gcd(a, 2^m)}$$, r with high probability even

Take $k^{r/2}$, (which is with high probability $\neq \pm 1 \pmod N$),

and $\gcd(k^{r/2} + 1, N)$ or $\gcd(k^{r/2} - 1, N)$

give(s) you a factor of N.

a) factorize 15 in this way

b) Read the article on IBM's factorization of 15

they use some tricks in order to go with 7 qubits ~~only~~ only.