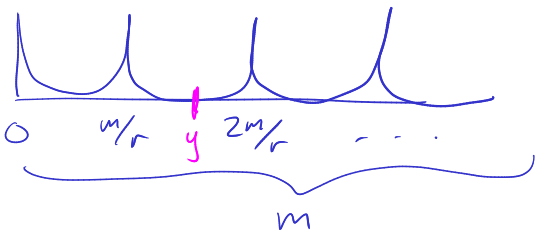
Output of Shor's Alg.

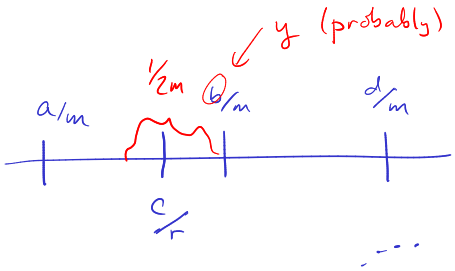


$m = 2^{m_0}$ ← # qubits

We measure $|y\rangle$ i.e. $0 \le y \le m-1$

So $\boxed{\frac{y}{m}} \approx \frac{c}{r}$ goal

Known



Question: Having measured y, how to get r?

We are likely to measure y s.t. $\left|\frac{y}{m} - \frac{c}{r}\right| < \frac{1}{2m}$ ($\frac{y}{m} = \alpha$)

Diophantine Approximation & Continued Fractions

There exists an efficient algorithm (continued fractions) given $\alpha \in \mathbb{R}$ to find all $\frac{p}{q} \in \mathbb{Q}$ (rationals) s.t. $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$

Find $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \ldots, \frac{p_k}{q_k}$ in poly(k) time.

So take $m > r^2$ (can guarantee this by taking $m > N^2$)

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

Continued Fraction

eg. $\pi = 3 + 0.141592653\ldots$ (integer part) $\qquad 3$

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

$= 3 + \cfrac{1}{7 + 0.0625\ldots}$ $\qquad 3 + \frac{1}{7} = \frac{22}{7}$

$= 3 + \cfrac{1}{7 + \cfrac{1}{15 + 0.99625\ldots}}$ $\qquad 3 + \cfrac{1}{7 + \frac{1}{15}} = \frac{333}{106}$

eg. $\frac{7}{9} = 0 + \frac{7}{9}$

$= 0 + \frac{1}{(9/7)}$

$= 0 + \frac{1}{1 + 2/7}$

$= 0 + \frac{1}{1 + \frac{1}{(7/2)}}$

$= 0 + \frac{1}{1 + \frac{1}{3 + 1/2}}$

0

$0 + \frac{1}{1} = 1$

$0 + \frac{1}{1 + \frac{1}{3}} = 0 + \frac{1}{4/3}$

$= 0 + 3/4$

$= 3/4$

last approx $= 7/9$

Shor Example. Let's factor $247 = N$.

Need $2^{m_0} > N^2$: $m_0 = 16$ works. → $m_0 > 2\log_2(N)$ poly many

Let's try with $m_0 = 8$. $2^8 = 256$ (might work?)

Take $\alpha = 27$ ($f(x) = \alpha^x \bmod N$)

Shor

$y = 42$

Ctd frac. exp. of $\frac{y}{m} = \frac{42}{256}$

$\frac{42}{256} = \frac{21}{128} = 0 + \frac{21}{128} = 0 + \frac{1}{(128/21)}$

$= 0 + \frac{1}{6 + 2/21} = 0 + \frac{1}{6 + \frac{1}{(21/2)}}$

$= 0 + \frac{1}{6 + \frac{1}{10 + 1/2}}$

Approximations

0

$\frac{1}{6}$

$\frac{10}{61}$

$\frac{21}{128}$

possible r's

$\gcd(a^{r/2}-1, N)$

try $r=6$ $\quad a^{r/2} \equiv 27^3 \equiv 170 \pmod{247}$

so $\gcd(\underset{169}{170-1}, 247)$

$$247 = 1\cdot 169 + 78$$
$$169 = 2\cdot 78 + \boxed{13} \leftarrow \gcd$$
$$78 = 6\cdot 13 + 0$$

So 13 divides $N=247$. In fact, $247 = 13\cdot 19$.

Discrete Log (both for mod p & elliptic curves) can also be reduced to period finding.

$\Rightarrow$ "all" public-key cryptography is "broken"!

quantum computer can break it in poly time.

Post-Quantum Cryptography = cryptography that is secure against a quantum computers.