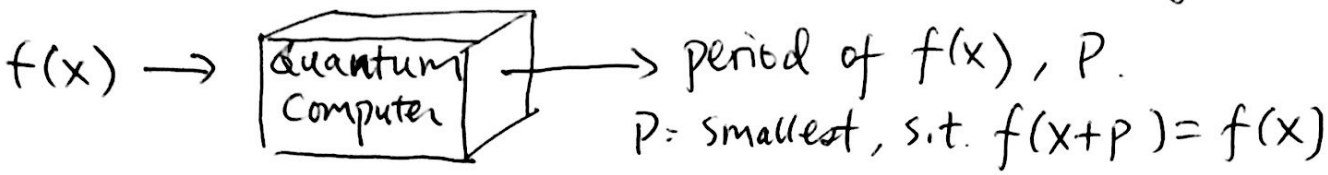
Quantum Factoring: Reduce Factoring to Order Finding



With this, how to factor N?

① generate random num $a < N$

② If $\gcd(a, N) \neq 1$, done. (we've factored N)

③ Define: $f(x) = a^x \bmod N$
then, find period, P, of $f(x)$: $a^{x+P} \pmod N = a^x \pmod N$
$\Rightarrow a^P \equiv 1 \pmod N$

④ If P is odd, go back to Step ①
(meaning re-pick a random "a").
If P is even, but $a^{\frac{P}{2}} = -1 \pmod N$, goto ①
(have to repick rand a)

⑤ $\gcd(a^{\frac{P}{2}}+1, N)$ and $\gcd(a^{\frac{P}{2}}-1, N)$ are factors of N

note: The random number "a" has a high ($\sim \frac{1}{2}$) probability of success.

Proof:

$a^P \equiv 1 \pmod N$

$r \equiv a^{\frac{P}{2}} \pmod N$ is a sqrt of $a \pmod N$

$\exists r$ because P is even

$r \neq 1$ because P is the period. (If r was 1, then $\frac{P}{2}$ would be the period)

$r \neq -1$ by construction

- At the end of the algorithm, we will find an r, s.t. $r \neq 1$ and $r \neq -1$ and $r = a^{\frac{P}{2}} = \sqrt{1} \pmod N$
- There exists such an r by CRT

Claim: $f = \gcd(r-1, N)$ is a factor of N.

That is, $\boxed{f \neq 1}$ and $\boxed{f \neq N}$

$\boxed{f \neq N}$: If $f = N$, then $r-1$ is a multiple of N

$\Rightarrow r-1 \equiv 0 \pmod N \Rightarrow r \equiv 1 \pmod N$, contradiction

---

$\boxed{f \neq 1}$ If $f = 1 = \gcd(r-1, N)$

then $1 = (r-1)u + NV$,

mul both sides by $r+1$, $r+1 = (r^2-1)u + N(r+1)V$

$r^2 \equiv 1 \pmod N$, so $r^2 - 1 \equiv 0 \pmod N$

$\Rightarrow r+1 \equiv 0 \pmod N \Rightarrow r \equiv -1 \pmod N$

contradiction

Factor N $\Leftrightarrow$ Finding non-trivial sqrt of $1 \pmod N$
$\Leftrightarrow$ find u s.t. $u^2 \equiv 1 \pmod N$ and $u \not\equiv \pm 1 \pmod N$

Background:

How many sqrts of 1 are there mod N?

$x^2 \equiv 1 \pmod p$

$\Rightarrow x^2 - 1 \equiv 0 \pmod p \Rightarrow (x+1)(x-1) \equiv 0 \pmod p$

$\Rightarrow x \equiv \pm 1 \pmod p \Rightarrow$ **2 sqrts**

degree n, at most n solutions

How about:

$x^2 \equiv 1 \pmod{pq}$?

Mod p only: $x \equiv \pm 1 \pmod p$, 2 solutions

Mod q " : $x \equiv \pm 1 \pmod q$ 2 solutions

	mod q	mod p	mod pq
$x =$	1	1	root 1
$x =$	1	-1	root 2
$x =$	-1	1	root 3
$x =$	-1	-1	root 4

CRT

$\Rightarrow$ 4 sqrts

If N is a product of n primes, then 2^n sqrts