Suppose you run algorithm twice and get c, c' both good, and get approximations $\frac{a}{b}$, $\frac{a}{b'}$ then prob. $LCM(b, b') = r$ is $\frac{1}{2}$.

## Time Complexity of factoring
## Comparison to Classical

N is size of domain of f
$\Longleftrightarrow$ N is # to factor

- $QFT_N$: $O((\log_2 N)^2)$ single + 2 qubit gates
- $U_f$: For factoring application: $O(\log_2 N)$ gates

$\Rightarrow$ $O((\log_2 N)^2)$ time for Quantum

$\Rightarrow$ $e^{O((\log_2 N)^{1/3})}$ for classical

"number field sieve"

↓

sub-exponential in $\log_2 N$ (almost exponential)

↓ polynomial in $\log_2 N$