Simon '94 (p.56), $f(x) = f(x \oplus a)$, measured $y$ has $a \cdot y = 0$ (equivalently $\sum_i a_i y_i = 0 \bmod 2$), exponential speedup ($2^{n/2} \rightarrow O(n)$) to determine $a$

Shor '94 (p.70), $f(x) = f(x + r)$, resulting $y$ is measured with probability $p(y) = \frac{1}{2^n m} \left| \sum_{k=0}^{m-1} e^{2\pi i k y/2^n} \right|^2$, gives $|y - 2^n / r| < 1/2$ with $p > .4$, sufficient to determine period $r$ via partial fraction expansion, exponential speedup ($n2^n, \exp(n^{1/3}) \rightarrow O(n^3)$).

(Note: replaces $H^\otimes n |x\rangle = \frac{1}{2^{n/2}} \sum_{0 \leq y < 2^n} e^{i\pi x \cdot y} |y\rangle$ with $U_{FT} |x\rangle = \frac{1}{2^{n/2}} \sum_{0 \leq y < 2^n} e^{2\pi i x y/2^n} |y\rangle$.)

Practical application is $f(x) \equiv b^x \bmod N$, where $b \equiv a^c \bmod N$ is an encrypted message, from which $d'$, satisfying $cd' \equiv 1 \bmod r$, can be calculated, and $d'$ recovers unencrypted message $a \equiv b'^c \bmod N$ (in contrast to using $d$, with $cd \equiv 1 \bmod (p-1)(q-1)$, where $N = pq$ and $r$ divides $(p-1)(q-1) = |G_{pq}|$).

$H^\otimes n |x\rangle_n = \frac{1}{2^{n/2}} \sum_{0 \leq y < 2^n} e^{i \pi x y / 2^n} |y\rangle_n$

$U_{FT} |x\rangle_n = \frac{1}{2^{n/2}} \sum_{0 \leq y < 2^n} e^{2\pi i x y / 2^n} |y\rangle_n$
What about $U_f$ for the function $f(x) = b^x \mod N$?

$x = \sum_{i=0}^{l} x_i 2^i = \overline{1011}_2$  

$b^{11} = b^8 \cdot b^2 \cdot b$, so calculate

$b, b^2, b^4, b^8, b^{16}, b^{32}, b^{64} \mod N$

$X = X_{n-1} X_{n-2} \ldots X_1 X_0$

$b^x = b^{X_{n-1} 2^{n-1} + X_{n-2} 2^{n-2} + \ldots + X_1 \cdot 2 + X_0}$

$= \prod_j \left(b^{2^j}\right)^{x_j}$

Number of powers to calculate only grows logarithmically in $x$.

Calculate by successive squares.
\[ U_f = O(n^4) \]

\[ n_0 = \lceil \log_2 N \rceil \] output bits

\[ (+) = H |0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \]

U implements multiplication by \( b \mod N \) and

\[ U_f \left| x \right\>_n n_0 \rangle = \left| x \right\>_n \left| b^x \mod N \right\>_n \] with "recycling"

\[ \text{total qubits} \sim 2-3 n_0 \]
\[ U_f |x\rangle_n |0\rangle_{n_0} = |x\rangle_n |f(x)\rangle_{n_0} \]

\[ U_f \frac{1}{2^{n/2}} \sum_{0 \leq x < 2^n} |x\rangle_n |0\rangle_{n_0} = U_f \frac{1}{\sqrt{n}} \sum_{k=0}^{\Theta n} |0\rangle_{n_0} \]

\[ = \frac{1}{2^{n/2}} \sum_{x} |x\rangle_n |f(x)\rangle_{n_0} \]

\[ \rightarrow \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle_n |f(x_0)\rangle_{n_0} \]

- **What is \( m \)?**

\[ m = \left \lfloor \frac{2^n}{r} \right \rfloor \text{ if } x_0 > 2^n \mod r \]

\[ m = \left \lfloor \frac{2^n}{r} \right \rfloor + 1 \text{ if } x_0 < 2^n \mod r \]
\[
|\psi\rangle_n = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle |f(x_0)\rangle
\]

(from Lec 16)

\[
U_{FT} |\psi\rangle_n = \frac{1}{2^{n/2}} \sum_{k=0}^{m-1} \frac{e^{2\pi i (x_0 + kr) y/2^n}}{\sqrt{m}} y
\]

\[
p(y) = \frac{1}{2^n} \left| \sum_{k=0}^{m-1} e^{2\pi i kr/2^n} \right|^2 \text{ peaked at } y = \frac{2^n}{r}
\]

\[
p(y) = \frac{1}{2^n m} \left| 1 - \frac{e^{2\pi i (myr/2^n)}}{1 - e^{2\pi i y/2^n}} \right|^2
\]

\[
\sin^2 \pi m y r / 2^n
\]

Now only appreciable near
\[
y = \frac{j \cdot 2^n}{r}
\]

needs classical work to extract \( r \) from (nearest integer to \( j \cdot 2^n / r \))
Output bits \( n_0 = \left\lceil \log_2 N \right\rceil \) (round up)

\( n = 2n_0 \) input bits to ensure many periods: i.e., \( m \) large

e.g. \( N \) with 500 digits, \( n_0 \approx 1700 \)

Input bits \( n = 2n_0 \approx 3400 \) will want \( y = y_j = j^{2n} \frac{1}{r} + \delta_j \) \( \delta_j \leq \frac{1}{2} \)

\[
p(y_j) = \frac{1}{2^{nm}} \frac{\sin^2(\pi \delta_j \frac{m^2}{2^n})}{\sin^2(\pi \delta_j \frac{r}{2n})} \approx \frac{1}{r} \sin^2(\pi \delta_j)^2
\]

Use \( \sin(x) > x/\pi/2 \) for \( x < \pi/2 \)

\[
\geq \frac{1}{r} \frac{4}{\pi^2} \quad \text{(using } m \sim 2^n/r \gg 1)\]

\( r \) different values of \( j \), so total prob of measuring \( y \) within \( \frac{1}{2} \) of \( 2^n/r \) is \( > \frac{4}{\pi^2} \approx 0.405 \)

[more refined estimate \( \Rightarrow > 90\% \)]
To extract $j/r$ reliably from $y = 2^n r$, we need $2^n \gg 2^n 0 = N$. Why?

We have $|y - j \frac{2^n}{r}| < \frac{1}{2}$ with high prob and want $\frac{1}{2N^2}$

$\Rightarrow \left| \frac{y}{2^n} - j \frac{1}{r} \right| < \frac{1}{2^{n+1}}$ 

If there were some other $j'/r'$, then $\left| j/r - j'/r' \right| > \frac{1}{N^2}$, since $r, r' < N$ and $\left| \frac{a}{b} - \frac{c}{d} \right| > \frac{1}{bd}$ for integers.

So picture looks like this:

Any other $j'/r'$ is far enough away that $j/r$ is uniquely specified by $y/2^n$ (up to common factors in $j, r$).
Continued fraction, write any number as \( a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \ddots}}} \)

\[ \pi = 3.\overline{1415926536} = 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1 + \frac{1}{292 + \ddots}}}} \]

\[ \frac{1}{.14159...} = 7.06251330542... \]

\[ \frac{1}{.0625...} = 15.9965945... \]

\[ \frac{1}{.9965...} = 1.003417099... \]

\[ \frac{1}{.003...} = 292.64... \]

\[ \pi = (3; 7, 15, 1, 292, \ldots) \]

Partial sums =

\[
3, \frac{22}{7}, \frac{333}{106}, \frac{355}{113}, \ldots
\]

\[
\frac{355}{113} = 3.14159292... \]

Known in 5th c. AD to Chinese (Tsu)
Some continued fractions

Golden mean:

\[ \varphi = \frac{1 + \sqrt{5}}{2} = 1.618\ldots = [1; \overline{1}] \]

\[ \sqrt{2} = [1; \overline{2}] \]

\[ \sqrt{3} = [1; \overline{1, 2}] \]

\[ e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots] \]

\[ \overline{\varphi} \text{ satisfies } \varphi - 1 = \frac{1}{\varphi} \]

\[ \sqrt{2} \text{ satisfies } x - 1 = \frac{1}{1 + x} \]
Euclidean Algorithm

\[ \text{GCD} (60, 40) = \text{GCD}(40, 20) = 20 \]

\[ \text{GCD}(200, 60) = \text{GCD}(60, 20) = 20 \]

Ex: 
\[ (62, 92) \rightarrow (42, 20) \rightarrow \]
\[ (f, c) \rightarrow (c, f \mod c) \]

\[ (60, 7) \rightarrow (7, 4) \rightarrow (4, 3) \rightarrow (3, 1) \]

No divisor
How do we use this to calculate inverse $7^{-1} \mod 60$?

$1 = 4 - 3 = 4 - (7 - 4)$

$= 2 \cdot 4 - 7$

$= 2(60 - 8 - 7) - 7$

$= 2 \cdot 60 - 17 \cdot 7$

$7^{-1} \mod 60 = -17 = 43$

$43 \cdot 7 = 301 \mod 60 = 1$