Quantum Computation

Lectures 15-16

Applications of the quantum Fourier transform
Order-finding quantum subroutine

Modular arithmetic:

Let $x, N$ be positive integers.

$x$ has a (unique) multiplicative inverse modulo $N$ if and only if $x$ and $N$ have no common factor (except 1).

\[
\begin{array}{c|cccc}
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 \\
2 & 0 & 2 & 4 & 1 \\
3 & 0 & 3 & 1 & 4 \\
4 & 0 & 4 & 3 & 2
\end{array}
\]

For $x$ and $N$ co-prime, the order of $x \mod N$ is the smallest positive integer $r$ such that $x^r \equiv 1 \pmod{N}$.

\[
\begin{array}{c|cccc}
x & 0 & 1 & 2 & 3 \\
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 \\
2 & 0 & 2 & 4 & 0 \\
3 & 0 & 3 & 0 & 3 \\
4 & 0 & 4 & 2 & 0 \\
5 & 0 & 5 & 4 & 3 \\
\end{array}
\]

\[
\begin{array}{c|cccc}
x & 1 & 2 & 3 & 4 \\
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 \\
2 & 0 & 2 & 4 & 0 \\
3 & 0 & 3 & 0 & 3 \\
4 & 0 & 4 & 2 & 0 \\
5 & 0 & 5 & 4 & 3 \\
\end{array}
\]

$x = 1; r = 1$

$x = 2; r = 4$

$x = 3; r = 4$

$x = 4; r = 2$

$x = 5; r = 2$

$1 \equiv 1 \pmod{6}$

$5 \equiv 1 \pmod{6}$
$\mathbb{Z}_N = \{1, 2, \ldots, N-1\} \quad \text{positive integers modulo } N$

$\mathbb{Z}_N^+ = \{0, 1, 2, \ldots, N-1\} \quad \text{integers modulo } N$

$\mathbb{Z}_N^+$ is a group under addition modulo $N$. Any element of $\mathbb{Z}_N^+$ generates a subgroup.

$x, 2x, 3x, \ldots, nx = 0 \pmod{N} \implies nx = kN$

↑

Smallest positive $n$ such that

$nx = 0 \pmod{N}$

$(N-1)x + x = 0 \pmod{N}$

additive inverse of $x$

$m x = 0 \pmod{N} \iff m$ is a multiple of $n$.

$N$ is a multiple of $m$.

$\gcd(x, N) = \frac{N}{N} = \frac{x}{k}$

$\frac{x}{k}$

prime factorization

1. If $\gcd(x, N) = 1$, then $x$ generates $\mathbb{Z}_N^+$ there exists a (unique) $n$ such that $nx = 1 \pmod{N}$, i.e., $x$ has a (unique) multiplicative inverse modulo $N$.

2. If $x$ has a multiplicative inverse $m$ modulo $N$, i.e., $mx = 1 \pmod{N}$, then the subgroup generated by $x$ contains $1$. The subgroup generated by $1$ is the whole of $\mathbb{Z}_N^+$, which means the subgroup generated by $x$ is $\mathbb{Z}_N^+$, so $\gcd(x, N) = 1$. 
The integers \( x \), \( 1 \leq x \leq N-1 \), such that \( x \) is co-prime to \( N \), are a group \( \mathbb{Z}_N^* \) under multiplication modulo \( N \). The order of the group is denoted \( |\mathbb{Z}_N^*| = \varphi(N) \).

1. \( N = p \): All \( x = 1, \ldots, p-1 \) are co-prime to \( p \) \( (\mathbb{Z}_p^* = \mathbb{Z}_p^0) \);
   \( \varphi(p) = p - 1 \).

2. \( N = p^d \): All \( x = 1, \ldots, p^d - 1 \) are co-prime to \( p^d \), except multiples of \( p \), i.e., \( p, 2p, \ldots, (p^{d-1} - 1)p \);
   \( \varphi(p^d) = p^{d-1}(p - 1) = p^{d-1}(p - 1) \).

3. Arbitrary \( N = p_1^{d_1} \cdots p_M^{d_M} \); \( \varphi(N) = \prod_{j=1}^{M} \varphi(p_j^{d_j}) = \prod_{j=1}^{M} p_j^{d_j - 1}(p_j - 1) \).

   \[ \text{[Use: } a, b \text{ co-prime } \Rightarrow \varphi(ab) = \varphi(a)\varphi(b) \]\n
Any element of \( \mathbb{Z}_N^* \) generates a subgroup

\[
x, x^2, \ldots, x^r = 1 \pmod{N}
\]

order of \( x \): Smallest positive \( r \)

such that \( x^r = 1 \pmod{N} \)

\( x^{r-1} = x^{-1} \pmod{N} \)

\( x^8 = 1 \pmod{N} \iff S \) is a multiple of \( r \)

\( \left[ x^S \pmod{N} \text{ is a periodic function with period } r \right] \)

modular exponentiation

\( r \) \( \equiv \) \( \text{order of subgroup \pmod{N}} \Rightarrow r \mid \varphi(N) \leq N - 1 \)

\( x \) \( \equiv \) \( \text{generated by \pmod{N}} \Rightarrow x^{\varphi(N)} = 1 \pmod{N} \)
In the subgroup $x, x^2, \ldots, x^r = 1 \pmod{N}$, the arithmetic in the exponent of the modular exponentiation is mod-$\tau$ addition.

Order of $x^n$: smallest positive integer $s$ such that $(x^n)^s = 1 \pmod{N}$. ($s \leq r$, $ns$ is a multiple of $r$); i.e., $s$ is the smallest positive integer such that $ns = 0 \pmod{r} \Rightarrow s = \frac{r}{\gcd(nr)}$.

$N = p^i$:

$x^{p^i-1} = 1 \pmod{p}$ for any $x$ not a multiple of $p$.

$N = p^q$:

$x^{p^q-1(p-1)} = 1 \pmod{p}$ for any $x$ not a multiple of $p$.

Fact: $\mathbb{Z}_{p^q}$ is a cyclic group; i.e., there exists a generator $x$ that generates the entire group $[\mathbb{Z}_{p^q} = x^{\phi(p^q)}]$.
we want to find the order of $x$.

For any $x \in Z_N^*$, $Z_N^* = \{0, 1, \ldots, N-1\}$ divides up into disjoint equivalence classes \{\(x^ky \mod N\), \(k = 0, \ldots, r\}\}.

If $y \in Z_N^*$, you get a coset of the subgroup generated by $x$, containing $r$ members; if $y \not\in Z_N^*$, you get a class whose number of members, $\bar{r}$, divides $r$.

Put this in Hilbert space:

$U_x |y\rangle \equiv \left\{ \begin{array}{ll} |xy \mod N\rangle, & y = 0, \ldots, N-1, \\ |y\rangle, & y = N, \ldots, 2L-1. \end{array} \right.$

$L = \lceil \log N \rceil$ (size of)

$U_x$ unitary: $xy = x'y' \mod N \Rightarrow y'y' \mod N$ (x has an inverse)

Each equivalence class forms a cycle under $U_x$.

Eigenstates of $U_x$:

$|u_\phi\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi ik\phi/r} |x^k y \mod N\rangle, \quad s=0, \ldots, r-1$

$U_x |u_\phi\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi ik\phi/r} |x^{k+1} y \mod N\rangle$

$= e^{2\pi is\phi/r} |u_\phi\rangle$
\( N = 15: \mathbb{Z}_n \) contains 1, 2, 4, 7, 8, 11, 13, 14

**x = 2**

\[
\begin{array}{cccc}
1 & 2 & 4 & 8 \\
7 & 14 & 13 & 11 & 7 \\
0 & 0 & 0 & 0 \\
3 & 6 & 12 & 9 & 3 \\
5 & 10 & 5 & 10 & 5 \\
\end{array}
\]

**x = 8 gives same classes**

\[
\begin{array}{cccc}
k = 1 & 2 & 3 & 4 \\
1 & 2 & 3 & 4 \\
7 & 14 & 13 & 11 & 7 \\
0 & 0 & 0 & 0 \\
3 & 6 & 12 & 9 & 3 \\
5 & 10 & 5 & 10 & 5 \\
\end{array}
\]

Eigenstates:
\[
\begin{align*}
(\psi_1) &= \frac{1}{2} (11) + 12 + 14 + 18 \\
(\psi_2) &= \frac{1}{2} (11) - (12) - 14 + 18 \\
(\psi_3) &= \frac{1}{2} (11) - (12) + 14 - 18 \\
(\psi_4) &= \frac{1}{2} (11) + (12) - 14 - 18
\end{align*}
\]

\[ u_{2,15} = |110\rangle \]

\[ u_{2,110} = |15\rangle \]

Eigenstates:
\[
\begin{align*}
\frac{1}{i} (u_{2,15} + 110) = +1 \\
\frac{1}{i} (u_{2,15} - 110) = -1
\end{align*}
\]

\( u_4 \) does 2-eyes

\( u_8 \) does 1-cycles

**x = 7**

\[
\begin{array}{cccc}
1 & 2 & 4 & 8 \\
7 & 14 & 13 & 11 & 7 \\
0 & 0 & 0 & 0 \\
3 & 6 & 12 & 9 & 3 \\
5 & 10 & 5 & 10 & 5 \\
\end{array}
\]

\[ (r = 4) \]

**x = 13 gives same classes**

\[
\begin{array}{cccc}
1 & 2 & 4 & 8 \\
7 & 14 & 13 & 11 & 7 \\
0 & 0 & 0 & 0 \\
3 & 6 & 12 & 9 & 3 \\
5 & 10 & 5 & 10 & 5 \\
\end{array}
\]

\[ (r = 4) \]

\[ (r = 4) \]
<table>
<thead>
<tr>
<th>$x = 11$</th>
<th>$4x^k$</th>
<th>$11$</th>
<th>$1$</th>
<th>($x = 2$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2x^k$</td>
<td>$7$</td>
<td>$2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$4x^k$</td>
<td>$14$</td>
<td>$4$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$8x^k$</td>
<td>$13$</td>
<td>$8$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$0x^k$</td>
<td>$0$</td>
<td>$0$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$3x^k$</td>
<td>$3$</td>
<td>$3$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$6x^k$</td>
<td>$10$</td>
<td>$6$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$6x^k$</td>
<td>$6$</td>
<td>$9$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$9x^k$</td>
<td>$9$</td>
<td>$9$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$12x^k$</td>
<td>$12$</td>
<td>$12$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$x = 124$</th>
<th>$4x^k$</th>
<th>$124$</th>
<th>$1$</th>
<th>($x = 2$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2x^k$</td>
<td>$13$</td>
<td>$2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$4x^k$</td>
<td>$11$</td>
<td>$4$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$7x^k$</td>
<td>$8$</td>
<td>$7$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$0x^k$</td>
<td>$0$</td>
<td>$0$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$3x^k$</td>
<td>$12$</td>
<td>$3$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$5x^k$</td>
<td>$10$</td>
<td>$5$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$9x^k$</td>
<td>$6$</td>
<td>$9$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
We are interested in the $\gamma = 1$ equivalence class:

$$1|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i ks}{r}} |x^k \text{ (mod } N)\rangle$$

$$U_x 1|u_s\rangle = e^{2\pi i \frac{s}{r}} 1|u_s\rangle$$

Phase $\phi$ we want to estimate; periodicity $r/s$

$$|x^k \text{ (mod } N)\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-\frac{2\pi i ks}{r}} 1|u_s\rangle, \text{ } k = 0, \ldots, r-1$$

---

This transformation:

$$|z\rangle|\psi\rangle \rightarrow |z\rangle|z_2\rangle \cdots |z_{t}\rangle \big(U_x^{t-1}z_1, U_x^{t-2}z_2 \cdots U_x^{0}z_{t-1}, U_x^{z_{t}} \big) |\psi\rangle$$

$$|z\rangle|\psi\rangle \rightarrow |z\rangle |U^z_x|\psi\rangle$$

Including the Hadamards: $10^{\otimes t}|\psi\rangle \rightarrow \frac{1}{2^{t/2}} \sum_{z=0}^{2^t-1} |z\rangle U^z_x |\psi\rangle$  

quantum parallelism
If \( |\psi\rangle \rightarrow |u_0\rangle \), \( 10^{8t} |\psi\rangle \rightarrow \left( \frac{1}{2^{t/2}} \sum_{z=1}^{2^t} e^{2\pi i z^8/8} |z\rangle \right) \otimes |u_0\rangle \)

\( U_{x^8}^{y} |y\rangle = |x^8 y \pmod{N}\rangle \)

(a) We can't put in \( |u_0\rangle \) without knowing \( v \)

Phase kickback

(b) How do we do this?

1. Let \( |z_i\rangle \rightarrow |z_i x^8 y \pmod{N}\rangle \)
2. Design a reversible classical circuit to calculate the function \( x^8 y \pmod{N} \), then do it in quantum parallel.

Modular exponentiation: Divide the \( z \) back into its bitwise components

\[
X^x \pmod{N} = X_0 x^{2^1} z_1 x^{2^2} z_2 \cdots = (x_0 x^{2^1} x^{2^2} x^{2^3} x^{2^4} x^{2^5} x^{2^6} x^{2^7} x^{2^8}) \pmod{N}
\]

Compute \( x_0, x_1, x_2, \ldots, x_{2^t-1} \) - 1 squaring operations, each using \( O(2^t) \) elementary multiplications.

Further \( t \) multiplications, each using \( O(2^t) \) multiplications.

\( O(2^t) \) operations

k=0, \( x^k = 1 \)

Input \( |\psi\rangle = |1\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} |u_s\rangle \sum_{i=0}^{t-1} \left( \frac{1}{2^{t/2}} \sum_{z=0}^{2^t-1} e^{2\pi i z s \pmod{N}} |z\rangle \right) \otimes |u_0\rangle \)

\( 1|\psi\rangle = s^t |\rangle \rangle \)

Near-eigenstate. \( F^t \) gives near position eigenstate (period -1) in \( z \); read out one of these periods.

The modular exponentiation can be done efficiently. Making it reversible does not change the \( O(2^t) \) operations.

Quantum parallelism calculates \( x^2 \pmod{N} \) in superposition and extracts the period \( r \)'s through the inverse FT.

Classically, one would need to compute \( r \approx O(\phi(N)) \approx O(N) \approx O(2^t) \)

Values of \( x^2 \pmod{N} \) to extract \( r \).
Measurement yields \( M \)-bit approximation to one of
the \( \frac{S}{\sqrt{r}}, \frac{S}{\sqrt{r^2}}, \ldots, \frac{S}{r^{L-1}} \) with probability \( 1 - e \), provided
\[ t \geq M + 1 + \log(1 + 1/2e). \]
A continued-fraction procedure extracts the fraction \( S/r \) exactly, provided \( M \geq 2L+1 \).
\[ \Rightarrow t \geq 2L + 2 + \log(1 + 1/2e). \]

Failure modes:

1. Poor approximation to \( S/r \), run with \( e \) small to make this probability negligible.
2. Get \( S/r \) or ambiguity because \( S/r \) can be reduced. Run several times.

Resources:

1. Hadamard: \( O(t) = O(L) \)
2. FT: \( O(t^2) = O(L^2) \)
3. Modular exponentiation: \( O(tL^2) = O(L^3) \)

Note quantum parallelism and phase kickback.
Success probability $p$

Probability of first success on $N$th trial: $Q_N = (1-p)^{N-1} \cdot p$

Probability of success by $N$th trial: $Q_N = \sum_{n=1}^{N} (1-p)^{n-1} \cdot p = \frac{p(1-(1-p)^N)}{1-(1-p)} = 1-(1-p)^N$

To have $Q_N \geq 1-\epsilon$, we need $(1-p)^N \leq \epsilon$, i.e.,

$N \geq \frac{-\log \epsilon}{-\log(1-p)} = \frac{\log(1/\epsilon)}{\log(1/(1-p))}$
Factoring:

Input: \( \text{l-bit composite number } N, \text{ not even or a prime power, } \)

Output: A nontrivial factor of \( N \) (easily checked)

Randomly choose \( x, 1 < x < N-1 \), and calculate \( \gcd(x, N) \) by Euclid's algorithm. \( O(L^3) \)

\[
\text{if } \gcd(x, N) = 1,
\text{ find and save } r \text{ of } x \quad \text{ (crucial quantum step)}
\]

\[
\text{if } x \text{ is even and } y = x^{r/2} \neq \pm 1 \pmod{N}
\]

\[
y^2 = x^r \equiv 1 \pmod{N}
\]

\[
y = 2, \ldots, N-2 \pmod{N}
\]

\[
y^2 - 1 = (y-1)(y+1) = 0 \pmod{N} \quad \text{So } N \text{ divides } (y-1)(y+1) = x^r-1
\]

\( \Rightarrow N \text{ has a common factor with } y-1 \text{ or } y+1 \)

This common factor cannot be \( N \), so \( N \) has a nontrivial common factor with both \( y-1 \) and \( y+1 \).

Calculate \( \gcd(y-1, N) \) or \( \gcd(y+1, N) \) (Euclid's algorithm, \( O(L^3) \)) and output the \( \gcd \).
\( N = 15 \)

\[\begin{align*}
X = 2: & \quad x = 4, \quad y = 4 \\
X = 4: & \quad x = 2, \quad y = 4 \\
X = 7: & \quad x = 4, \quad y = 49 = 4 \pmod{15} \\
X = 8: & \quad x = 4, \quad y = 64 = 4 \pmod{15} \\
X = 11: & \quad x = 2, \quad y = 11, \quad y = 10, \quad y + 1 = 12 \\
X = 13: & \quad x = 4, \quad y = 169 = 4 \pmod{15} \\
X = 14: & \quad x = 2, \quad y = 14, \quad y = N - 1, \text{ so start over}
\end{align*}\]

\( y \) even in all cases
**Period Finding:**

\[ f : \{0,1\}^L \rightarrow \{0,1\}^L \]  
(Range of \( f \))

\[ f(z+r) = f(z) \quad \forall f(0), \ldots, f(r-1) \]

\[ U_1 f(z) = | f(z+1) \rangle \]

\[ U_1 y = | y \rangle, \quad y \neq f(z) \quad \text{for any } z \]

\[ U_1^z | f(z) \rangle = | f(z) \rangle \]

**Order Finding:**

as Special Case.

\[ f(x)(z) = x^z \pmod N \]

\[ f(x)(z+r) = f(x)(z) \]

\[ U_x y = | x y \pmod{N} \rangle \]

\[ U_x^z | 1 \rangle = | x^z \pmod{N} \rangle \]

---

\[
\begin{align*}
\left| \begin{array}{c}
10 \\
10 \\
\vdots \\
10 \\
10 \\
\end{array} \right> \\
\left| f(0) \right> \\
\end{align*} = U^0 \left| \begin{array}{c}
10 \\
10 \\
\vdots \\
10 \\
10 \\
\end{array} \right> = U^1 \left| \begin{array}{c}
10 \\
10 \\
\vdots \\
10 \\
10 \\
\end{array} \right> = \cdots = U^{x-1} \left| \begin{array}{c}
10 \\
10 \\
\vdots \\
10 \\
10 \\
\end{array} \right> = \frac{1}{\sqrt{x}} \sum_{s=0}^{x-1} e^{2\pi i s z / x} \left| u_s \right> \\
\left| f(0) \right> = \frac{1}{\sqrt{x}} \sum_{s=0}^{x-1} \left| u_s \right>
\end{align*}
\]

Determine one of the phases, \( s/r \); extract the period, \( r \).
What does this part of the circuit do?

\[ |z\rangle |\bar{y}\rangle \rightarrow |z\rangle \left( \frac{z_1^{x_1} z_2^{x_2} \cdots + z_2^{x_2} z_3^{x_3} \cdots + z_n^{x_n} z_1^{x_1}}{\sum_{j=1}^{n} z_j^{x_j} z_j} = z \right) |\bar{y}\rangle = |z\rangle U_z |\bar{y}\rangle \]

\[ |z\rangle |f(0)\rangle \rightarrow |z\rangle U_z |f(0)\rangle = |z\rangle |f(z)\rangle \]

So we could replace this part of the circuit with the standard unitary for reversible function evaluation:

\[ |z\rangle |y\rangle \rightarrow |z\rangle |y \oplus f(z)\rangle \]

Now choose the initial state of the \textit{b} ancilla qubits to be \( |0\rangle \).

\[ |z\rangle |0\rangle \rightarrow |z\rangle |f(z)\rangle . \]

Including the Hadamards, the transformation becomes

\[ |0\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} |z\rangle |f(z)\rangle \leftarrow \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} \sum_{s=0}^{2^n-1} e^{2\pi i s z / 2^n} |z\rangle |u_s\rangle \]

\[ = \frac{1}{\sqrt{2^n}} \sum_{s=0}^{2^n-1} \left( \frac{1}{2^n} \sum_{z=0}^{2^n-1} e^{2\pi i s z / 2^n} \right) |z\rangle |u_s\rangle \]

\[ = \frac{1}{\sqrt{2^n}} \sum_{s=0}^{2^n-1} \left( \frac{1}{2^n} \sum_{z=0}^{2^n-1} e^{2\pi i s z / 2^n} \right) |z\rangle |u_s\rangle \]

Near-momentum eigenstate with \( p_0 = s / r \).

Measurement after \( F^+ \) yields one of the \( s / r \) or \( s = 0 \) states. Must repeat algorithm if \( s = 0 \).
RSA cryptosystem

1. Select two large prime numbers, p and q.
2. Compute \( N = pq \).
3. Select a small (odd) integer, \( e \), that is co-prime to \( \phi(N) = (p-1)(q-1) \).
4. Find the multiplicative inverse \( d \) of \( e \) modulo \( \phi(N) \). \( \text{lcm}(m, n) \leq d \times \text{lcm}(m, n) \leq d \times \text{lcm}(m, n) \Rightarrow 1 \leq M \leq N \)

Public key: \((e, N)\)
Secret key: \((d, N)\)

Message \( M \): Encode using public key as \( M' = M^e \pmod{N} \). Decode using secret key as \( M'' = (M')^d \pmod{N} \).

Why does this work? Because \( M^{\phi(N)} = 1 \pmod{N} \) if \( M \) is co-prime to \( N \),

\[ M^{ed} \pmod{N} = M(M^{\phi(N)})^k \pmod{N} \]

\[ ed \equiv 1 \pmod{\phi(N)} \Rightarrow ed = 1 + k \phi(N) \]
\( M \text{ co-prime to } N \Rightarrow M^{\varphi(N)} = 1 \pmod{N} \)
\[ \Rightarrow M^{ed} = M \pmod{N} \]

- \( M \text{ not co-prime to } N \Rightarrow \)
  - \( M \) is a multiple of \( p \) or a multiple of \( q \), but not both, so say it's a multiple of \( p \).

\[ M = \hat{0} \pmod{p} \]
\[ M^{\varphi(N)} = M^{(p-1)(q-1)} = 1 \pmod{q} \]
\[ \text{so } Med = M \pmod{q} \]

\[ Med = M \pmod{N} \text{ is a solution.} \]

By the Chinese remainder theorem, it is the unique solution.

What we have shown is that encoding, \( M^e \pmod{N} \), is a 1-1 function from \( \mathbb{Z}_N \) to itself; decoding, \( M^d \pmod{N} \), is the inverse function.

Messages like this are hazardous, because the encoded message can be used to find the secret key.

\( M \text{ co-prime to } N \Leftrightarrow M^e \text{ is co-prime to } N \).

\( \Rightarrow \) Immediate consequence of the group \( \mathbb{Z}_N^* \).
\[ M^e \text{ has a multiplicative inverse } x. \]

\[ M^e x = 1 \pmod{N} \Rightarrow M \left( M^{e-1} x \right) = 1 \pmod{N} \]

\[ \text{Inverse of } M \]

\[ \Rightarrow M \text{ is co-prime to } N \]

This says that the messages not co-prime to N (multiples of \( p \) or \( q \)) are encoded as numbers not co-prime to N. In this case, Euclid's algorithm applied to \( M^e \pmod{N} \) and N would reveal \( p \) or \( q \), thus allowing the extraction of the secret key.

Can it be done efficiently?

- Generating the prime numbers:
  
  \[ \left( \text{probability that an } L\text{-bit \# is prime} \right) \sim \frac{1}{\log(2^L)} \sim \frac{1}{L} \]

  \( o(L^3) \) operations to test for primality

  \( o(L^4) \) operations to get an \( L \)-bit prime

- Getting \( e \) and \( d \): Euclid's algorithm; \( o(L^3) \) operations

- Encoding and decoding: Modular exponentiation; \( o(L^3) \) operations
ed = d' (mod 26)
Other attacks?