Recall \( \phi(N) = \# \) of integers \( \leq N \) that are relatively prime (or coprime) to \( N \).

(i) \( N = \text{prime } p \Rightarrow \phi(N) = p-1 \)

(ii) \( N = p_1 p_2 \ldots p_k \), \( p_i \text{ primes } \Rightarrow \phi(p_1 p_2 \ldots p_k) = (p_1-1)(p_2-1)\ldots(p_k-1) \).

Fermat's little theorem: \( a^{p-1} \equiv 1 \pmod{p} \)

when \( 1 \leq a \leq p-1 \).

The key to the proof was in observing that the two sets of integers below are in fact equal:

\( \{1, 2, \ldots, p-1\} \) and \( \{a, 2a, 3a, \ldots, (p-1)a\} \)

each taken \( \pmod{p} \).

Qn. Can we generalize this to general \( N \)?

Ans. Yes, if we restrict the sets to those \( m \) such that \( \text{GCD}(m,N)=1 \).
Euler's Theorem.

Let \( N \geq 1 \) arbitrary integer.
Let \( a \) be such that \( 1 \leq a \leq N \) and \( \gcd(a, N) = 1 \). Then \( a^\phi(N) \equiv 1 \pmod{N} \).

Proof. Let \( \{ b_1, b_2, \ldots, b_{\phi(N)} \} \) be the set of integers coprime to \( N \).
So \( \gcd(b_i, N) = 1 \), for all \( i = 1, \ldots, \phi(N) \).

Consider the set
\[
\{ a b_1 \pmod{N}, a b_2 \pmod{N}, \ldots, a b_{\phi(N)} \pmod{N} \}.
\]

Claim: The above set is in 1-1 correspondence with \( \{ b_1, b_2, \ldots, b_{\phi(N)} \} \).
Proof: Suppose for some \( i, j \) and \( i \neq j \), we have \( a b_i \equiv a b_j \pmod{N} \).
Since \( \gcd(a, N) = 1 \), \( a^{-1} \) exists.
So \( a^{-1} \cdot a b_i \equiv a^{-1} \cdot a b_j \pmod{N} \)
\[
\Rightarrow b_i \equiv b_j \pmod{N}, \text{ which is a contradiction!}
\]
Hence the claim is true!

Now as before, we may complete the proof of the theorem:

\[
\frac{\phi(N)}{\prod_{i=1}^{\phi(N)} (a \cdot b_i)} \equiv \frac{\phi(N)}{\prod_{i=1}^{\phi(N)} (a \cdot b_i)} \pmod{N}
\]

Cancelling the \(b_i\)'s on both sides, which is OK since \(\gcd(\phi_i, N) = 1, \forall i\), we get

\[
1 \equiv a \pmod{N}.
\]

\[\square\]

\(\exists \) RETURN TO JUSTIFYING RSA

Need to show \(M^e \equiv M \pmod{N}\)

When \(N = pq\) ; \((p, q : \text{primes})\) and

\[
ed \equiv 1 \pmod{\phi(N)} \rightarrow \star
\]

Note \(\star \Rightarrow ed - 1 = k \cdot \phi(N), \text{ for some integer } k.\)
Let us assume that the message $M$ is such that $\gcd(M, N) = 1$.

Note that otherwise, we're in big trouble. See why? If the $\gcd(M, N) \neq 1$, then since $N = pq$, the $\gcd$ is either $p$, $q$ or $pq$.

If it is $p$ or $q$, then "Eve" can factor $N$. If it is $pq$ then $M^{ed} \equiv M \equiv 0 \pmod{N}$.

So assuming $\gcd(M, N) = 1$,

$$M^{ed} = M^{k \phi(N) + 1} = \left[M^{\phi(N)}\right]^k \cdot M \equiv \left[1^k \cdot M \pmod{N}\right],$$

by Euler's theorem

$$\equiv M \pmod{N}.$$

\[ \square \]
Remarks on the Security of RSA:

1. Factoring $N=pq$ is so far hard, when $p$ and $q$ are large primes. If $N$ is factored by someone then $\phi(N) = (p-1)(q-1)$ is known and $d$ can be found, knowing $e$: solve for the inverse of $e$ in $ed \equiv 1 \pmod{\phi(N)}$.

2. If $\phi(N)$ is known, for general $N$, then it is not clear how to factor $N$, although there are randomized algorithms that might succeed.

But when $N=pq$, if $\phi(pq)$ is known then we can figure out $p$ & $q$:

Note: $\phi(pq) = pq - p - q + 1$. So we can figure out $(p+q) = pq + 1 - \phi(pq)$. Knowing $p+q$ and $pq$, we can first find $(p-q)$ and then $p$ and $q$. 

Remarks (Continued.)

Problem (1.43)

Suppose "Eve" finds out $d$, then knowing $e$ and $N = pq$, can she figure out the factors $p$ and $q$?

If $e$ is small like 3 (say), then Yes!

Solution. Recall $ed \equiv 1 \pmod{\varphi(N)}$

$\Rightarrow ed - 1 = k \varphi(N)$ for some $k \geq 1$.

If $d$ is known and $e = 3$, then $\varphi(N) = \frac{3d - 1}{k}$ for some $k \geq 1$.

Note that $12 \leq \varphi(N)$

so $3d - 1 < 3 \varphi(N) - 1$, so $k = 1$ or 2!!

We can simply try each choice (if we have to) and see that choice of $\varphi(N)$ and $N$ and figure out $p$ and $q$ as in Remark (2) above.
§ FINDING AN INVERSE MOD N:

First recall that an integer $a$ has an inverse mod $N$, only if $\gcd(a, N) = 1$. The so-called extended GCD algorithm is really a way to write the GCD of $m$ and $n$ (more generally) as an integer multiple combination of $m$ and $n$:

$$\text{GCD}(m, n) = mx + ny.$$ 

Necessarily, $x$ or $y$ will be negative, but by adding and subtracting $mn$ to the final solution, one can get $x$ or $y$ to be $> 0$, as one wishes!

Quick Example Next.
Example: Find the inverse of 25 mod 561.

(Answer comes out to be 202.)

First check that \( \text{GCD}(561, 25) = 1 \).

Then starting at the bottom, with 1, systematically replace each remainder (circled below) in terms of the other numbers in each equation:

\[
\text{GCD} \\
561 = (22)25 + (11) \\
25 = (2)11 + (3) \\
11 = (3)3 + (2) \\
3 = (1)2 + (1) \\
2 = (2)1 + 0
\]

Starting with

the \( \text{GCD}(561, 25) = 1 \) \( = 3 - (1)2 \)

(replace 2) \( = 3 - (1)[11 - (3)3] \)

(-regroup) \( = (-1)11 + (4)3 \)

(replace 3) \( = (-1)11 + (4)[25 - (2)11] \)

regroup \( = (4)25 - (9)11 \)

(replace 11) \( = (4)25 - (9)[561 - (22)25] \)

\( = (-9)561 + (202)25 \).

\( \Rightarrow (202) \times 25 \equiv 1 \pmod{561} \).

Answer.