THE SET \( \{a \leq n \mid (a,n)=1 \} \) WOULD BE AN EXAMPLE OF A REDUCED SET OF RESIDUES, SO WE SEE THERE ARE \( \phi(n) \) SUCH RESIDUES.

**Alternate Proof That \( \phi(n) \) is Multiplicative:**

Let \( S_n \) and \( S_m \) be a reduced set of residues \( (\mod n) \) and \( (\mod m) \) respectively. We see \( |S_n| = \phi(n) \) and \( |S_m| = \phi(m) \). If \( (m,n)=1 \), we will show \( S_{mn} = \{am+bn \mid a \in S_n, b \in S_m\} \) is a reduced set of residues and all elements are distinct. This would mean \( |S_{mn}| = \phi(mn) \) and counting elements in \( S_{mn} \) we see \( |S_{mn}| = \phi(m)\phi(n) \), giving the proof.

So, first, if \( a \in S_n \) and \( b \in S_m \) then \( (am+bn, nm) = 1 \) since \( (a, am) = 1 \) and \( (m, bn) = 1 \). So \( am+bn \) is invertible \( (\mod nm) \).

Also if \( a, a' \in S_n \) and \( b, b' \in S_m \) and \( am+bn \equiv a'm+b'n \ (\mod mn) \) then \( (a-a')m \equiv (b'-b)n \ (\mod mn) \). So \( n | (a-a') \) and \( m | (b'-b) \) so \( a \equiv a' \ (\mod n) \) and \( b \equiv b' \ (\mod m) \). So each element of \( S_{mn} \) is distinct since every element of \( S_n \) and \( S_m \) are distinct.
It remains to show that if \((c, mn) = 1\)
then \(c \equiv a^m b^n \pmod{mn}\) for \(a \equiv s_m\) and \(b \equiv s_n\).

Let \(a \equiv c^{-1} \pmod{n}\) and \(b \equiv c^{-1} \pmod{m}\), we see \(a \equiv s_m\) and \(b \equiv s_n\) as the product of invertible elements. So \(am \equiv c \pmod{n}\) and \(bn \equiv c \pmod{m}\) so \(n | (am - c)\) and \(m | (bn - c)\) so \(m, n | (am + bn - c)\) and \((m, n) = 1\) so \(mn | (am + bn - c)\) and so \(am + bn \equiv c \pmod{mn}\).

So we're done.

Fermat's Little Theorem: \(a^{p-1} \equiv 1 \pmod{p}\) if \((a, p) = 1\).

Fermat didn't prove it.

Euler's Theorem: If \((a, n) = 1\), \(a^\phi(n) \equiv 1 \pmod{n}\).
Euler proved it, and FLT above is a corollary when \(n = p\).

Proof of Euler's Theorem: Let \(x_1, x_2, ..., x_{\phi(n)}\) be a reduced set of residues \(\pmod{n}\), then for \((a, n) = 1\), \(ax_1, ax_2, ..., ax_{\phi(n)}\) is another reduced set of residues so \(\prod_{j=1}^{\phi(n)} x_j \equiv \prod_{j=1}^{\phi(n)} ax_j \equiv a^{\phi(n)} \prod_{j=1}^{\phi(n)} x_j \pmod{n}\), and cancelling the product gets the result.

§3.4 Wilson's Theorem

Wilson's Theorem: \((p-1)! \equiv -1 \pmod{p}\) for all prime \(p\).
\textbf{Proof:} \((p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1), \text{ every element}, a\) 

This product has a unique inverse, \(a^{-1} \pmod{p}\) also on that list. If \(a \neq a^{-1}\), they cancel out \((\text{mod} \ p)\).

Otherwise \((a^2 = 1 \pmod{p}) \Rightarrow a^2 - 1 = 0 \pmod{p}\)

\[\Rightarrow (a-1)(a+1) = 0 \pmod{p}\]

so \(a = 1 \pmod{p}\) or \(\Rightarrow (p-1) \pmod{p}\), so \((p-1)! = 1 \cdot (p-1) = -1 \pmod{p}\).

\textbf{Wilson's Theorem}

With converse: For \(n \in \mathbb{N}\), \((n-1)! \equiv -1 \pmod{n}\) IFF \(n\) is prime.

\textbf{Proof:} If \(n\) is not prime then \(n=ab\) for \(n > a, b > 1\), indeed \(a \leq \left\lfloor \frac{n}{2} \right\rfloor < n - 1\), so \(a \mid (n-1)\).

If \((n-1)! \equiv -1 \pmod{n}\) then \((n-1)! \equiv 1 \pmod{a}\), but \((n-1)! \equiv 0 \pmod{a}\) so \((n-1)! \not\equiv -1 \pmod{n}\).

\textbf{Proposition:} If \(p\) is an odd prime, \(x^2 \equiv -1 \pmod{p}\) has a solution in \(x \in \mathbb{Z}\) IFF \(p \equiv 1 \pmod{4}\).

\textbf{Proof:} If \(p \equiv 1 \pmod{4}\), let \(x = \pm (\gamma!)\) where

\[\Gamma = \frac{1}{2}(p-1)\], indeed, consider

\[(p-1)! = 1 \cdot 2 \cdots (p-1) \gamma (p+1) \gamma + 2 \cdots (p+\gamma) \pmod{p}\]

\[\equiv 1 \cdot 2 \cdots (p-1) \gamma (-\gamma)(1-\gamma)(2-\gamma) \cdots (-1) \pmod{p}\] since \(\gamma = -1 \pmod{p}\)

\[\equiv (\gamma!)^2 \equiv -1 \pmod{p}\) by Wilson's Theorem