Last time

\( \varphi(p^k) = p^k - p^{k-1} \) if \( p \) is prime

Truth:

\( \varphi(mn) = \varphi(m) \varphi(n) \)

if \( \gcd(m,n) = 1 \)
1st do Chinese Remainder Theorem

if \( \gcd(m, n) = 1 \), \( b, c \in \mathbb{Z} \).

Then

\[ x \equiv b \mod m \quad \text{and} \quad x \equiv c \mod n \]

has exactly one solution

with \( 0 \leq x < mn \).
e.g. \( m = 8 \), \( n = 9 \) \( b = 7 \), \( c = 4 \)

I want \( x \) so that

\[ x \equiv 7 \mod 8 \text{ and } x \equiv 4 \mod 9 \]

with \( 0 \leq x < 8 \cdot 9 = 72 \)

(peek in back of book: \( x = 31 \))
Hummm... I need \( x = 8q + 7 \).

Also need:
\[
\begin{align*}
8q &\equiv -3 \pmod{9} \\
8q &\equiv 6 \pmod{9}. 
\end{align*}
\]

Since \( \gcd(8, 9) = 1 \) this has exactly one solution.

\[
8 \cdot 8q = 8 \cdot 6 \pmod{9}
\]

Thus \( x = 8 \cdot 3 + 7 = 31 \) \( \checkmark \).
Now we can show that $\mathcal{O}(mn) = \mathcal{O}(m) \mathcal{O}(n)$

Let show

\[
\# \{ a \mid \gcd(a, mn) = 1 \} \leq \frac{\# \{ c \mid \gcd(c, n) = 1 \} \cdot \# \{ b \mid \gcd(b, m) = 1 \}}{\# \{ (b, c) \mid \gcd(b, m) = 1 \text{ and } \gcd(c, n) = 1 \}}
\]
we need to show that the map
\[ f(a) = (a \mod m, a \mod n) \]
is 1-to-1 and onto, i.e.

1-to-1: \[ f(a) = f(b) \Rightarrow a = b \]

onto: if (c, d) is in our set
then \( \exists a \) st. \( f(a) = (c, d) \)
Suppose \( f(a_1) = f(a_2) \)

\[
\Rightarrow (a_1 \mod m, a_1 \mod n) = (a_2 \mod m, a_2 \mod n)
\]

\[
\Rightarrow a_1 \mod m = a_2 \mod m \quad \text{and} \quad a_1 \mod n = a_2 \mod n
\]

\[
\Rightarrow m \mid a_2 - a_1 \quad \text{and} \quad n \mid a_2 - a_1
\]

but \( \gcd(m, n) = 1 \), so

\[
\Rightarrow mn \mid a_2 - a_1 \quad \text{but} \quad 0 \leq a_1, a_2 < mn
\]

\[
\Rightarrow mn - mn < a_2 - a_1 < mn
\]

\[
\Rightarrow a_2 - a_1 = 0, \quad \text{so} \quad a_1 = a_2 \quad \checkmark
\]
onto. need to know that if
(b, c) is in \( \equiv (b, c) | \gcd(b, m) = 1 \) \( \gcd(c, n) = 1 \)
then \( \exists a \in \equiv a | \gcd(a, mn) = 1 \)
so that
\[ f(a) = (b, c) \]
This is true by the Chinese remainder theorem.