

Last time

$$\phi(p^k) = p^k - p^{k-1} \quad \text{if } p \text{ is prime}$$

Truth:

$$\phi(mn) = \phi(m) \phi(n)$$

$$\text{if } \gcd(m, n) = 1$$

1st do Chinese Remainder theorem

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

Then

$x \equiv b \pmod{m}$ and $x \equiv c \pmod{n}$

has exactly one solution

with $0 \leq x < mn$

eg $m=8$, $n=9$ $b=7$, $c=4$

I want x so that

$$x \equiv 7 \pmod{8} \text{ and } x \equiv 4 \pmod{9}$$

with $0 \leq x < 8 \cdot 9 = 72$

(peek in back of book:
 $x=31$)

Hmm...

need $x = 8q + 7$

also need

$$x = 8q + 7 \equiv 4 \pmod{9}$$

$$8q \equiv -3 \pmod{9}$$

$$8q \equiv 6 \pmod{9}.$$

since $\gcd(8, 9) = 1$

this has exactly one solution.

$$8 \cdot 8q = 8 \cdot 6 \pmod{9}$$

$$1 \cdot q = 48 \pmod{9}$$

$$q = 3 \pmod{9}$$

thus $x = 8 \cdot 3 + 7 = 31$ ✓

Now we can show that $\phi(mn) = \phi(m)\phi(n)$

ie show

$$\# \left\{ a \mid \begin{array}{l} \gcd(a, mn) = 1 \\ 0 < a \leq mn \end{array} \right\}$$

$$= \# \left\{ b \mid \gcd(b, m) = 1 \right\} \cdot \# \left\{ c \mid \gcd(c, n) = 1 \right\}$$

$$= \# \left\{ (b, c) \mid \gcd(b, m) = 1 \text{ and } \gcd(c, n) = 1 \right\}$$

we need to show that the map

$$f(a) = (a \bmod m, a \bmod n)$$

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 $\exists a$ sth $f(a) = (c, d)$

do 1-to-1:

$$\text{Suppose } f(a_1) = f(a_2)$$

$$\Rightarrow (a_1 \bmod m, a_1 \bmod n) = (a_2 \bmod m, a_2 \bmod n)$$

$$\Rightarrow a_1 \bmod m = a_2 \bmod m \text{ and } a_1 \bmod n = a_2 \bmod n$$

$$\Rightarrow m \mid a_2 - a_1 \text{ and } n \mid a_2 - a_1$$

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

$$m \cdot n \mid a_2 - a_1 \text{ but } 0 \leq a_1, a_2 < mn$$
$$\text{so } -mn < a_2 - a_1 < mn$$

$$\Rightarrow a_2 - a_1 = 0, \text{ so } a_1 = a_2 \quad \checkmark$$

onto: need to know that if
 (b, c) is in $\{ (b, c) \mid \begin{array}{l} \cancel{\gcd(b, m) = 1} \\ \gcd(c, n) = 1 \end{array} \}$

then $\exists a \in \{ a \mid \gcd(a, mn) = 1 \}$

sth $f(a) = (b, c)$

ie need a so that

$$a \equiv b \pmod{m} \quad \text{and} \quad a \equiv c \pmod{n}$$

This is true by the Chinese remainder
Theorem! \triangleleft