Ex: $4^5 \equiv 4^2 \pmod 7$

$4^2 \equiv 16 \pmod 7$
$\equiv 2 \pmod 7$

$\to 4^2 \cdot 4^3 \equiv 4^2 \pmod 7$

$4^5 \equiv 4^2 \cdot 4^2 \cdot 4 \pmod 7$
$\equiv 2 \cdot 2 \cdot 4 \pmod 7$
$\equiv 2 \pmod 7$

$(4,7)=1 \overset{}{\underset{4.2}{\Longrightarrow}} (4^2,7)=1$

$\underset{1.45}{\Longrightarrow}$ cancel common factor of 4^2 from both sides

$\to 4^3 \equiv 1 \pmod 7$

Non-Ex: $4^5 \equiv 4^3 \pmod 6$

Check
$4^3 \equiv 64 \pmod 6$
$\equiv 4 \pmod 6$

$\cancel{4^3} \cdot 4^2 \equiv \cancel{4^3} \pmod 6$

$4^5 \equiv 4^3 \cdot 4^2 \pmod 6$
$\equiv 4 \cdot 4^2 \pmod 6$
$\equiv 4 \pmod 6$

$\Longrightarrow 4^2 \equiv 1 \pmod 6$

FALSE $4^2 \equiv 16 \pmod 6$
$\equiv 4 \pmod 6$

What went wrong: $(4,6)=2 \neq 1$ so 1.45 doesn't work.

Actually, $4^i \equiv 4 \pmod 6$ for all $i>0$.

Corollary of Thm 4.6 = Thm 4.36

If p is prime and $1 \le a < p$,

a is in CCRS, $a \neq 0$

then there is a unique b in CCRS such that

$$ab \equiv 1 \pmod{p}.$$

The number b is the "multiplicative inverse of a modulo a."

Proof: $(a, p) = 1$, so by 4.6

$$a^k \equiv 1 \pmod{p}$$

for some $k \geq 1$. Then $b \equiv a^{k-1} \pmod{p}$. ∎

Ex: $4^3 \equiv 1 \pmod{7}$

$\Rightarrow 4 \cdot 4^2 \equiv 1 \pmod{7}$

$\Rightarrow 4 \cdot 2 \equiv 1 \pmod{7}$

"The multiplicative inverse of 4 modulo 7 is 2."

"Dividing" by 4, mod 7, is the same as mult by 2.

Ex: Solve $4x \equiv 3 \pmod 7$.

Approach #1: Use 3.24

Approach #2: Mult both sides by 2 = inverse of 4, mod 7.

$$\Rightarrow \quad \overset{\equiv 1}{2 \cdot 4}\, x \equiv 2 \cdot 3 \pmod 7$$

$$x \equiv 6 \pmod 7$$

Next HW: 4.8 – 4.11

By Thm 4.6, if $(a,n) = 1$, then

$$a^k \equiv 1 \pmod n$$

for some $k \geq 1$.

The smallest such k is called the order of a modulo n, denoted $\mathrm{ord}_n(a)$

Ex: $\mathrm{ord}_7(4) = 3$

<u>Next week</u>: We'll see that if p is prime and $(a,p)=1$, then

$$\mathrm{ord}_p(a) \text{ divides } p-1.$$