

Clarification about Lemma (b):

If  $\gcd(a, n) = 1$  and  $m|a$  and  $m|b$ , then

$$ax \equiv b \pmod{n} \quad \text{iff} \quad \left(\frac{a}{m}\right)x \equiv \frac{b}{m} \pmod{n}.$$

In the forwards direction:

$$3x \equiv 6 \pmod{7}$$

1. check  $\gcd(3, 7) = 1$ .
2. Note  $3|3$  and  $3|6$ .
3. Instead solve

$$x \equiv 2 \pmod{7}.$$

In the backwards direction  
**INCORRECTLY:**

$$19x \equiv 42 \pmod{50}$$

Multiply by 5:

$$95x \equiv 210 \pmod{50}$$

Here:  $a = 95$ ,  $b = 210$ ,  $n = 50$ ,  
and  $m = 5$ .

Since  $\gcd(95, 50) \neq 1$ , we

cannot say

$$95x \equiv 210 \pmod{50}$$

$$\text{iff } 19x \equiv 42 \pmod{50}$$

In the backwards direction:

$$4x \equiv 13 \pmod{47}$$

1. Multiply both sides by 12

$$48x \equiv 156 \pmod{47}$$

2. Double check that  $\gcd(48, 47) = 1$ .

If so, then

$$4x \equiv 13 \pmod{47}$$

iff

$$48x \equiv 156 \pmod{47}.$$

Here:  $a = 48$ ,  $b = 156$ ,  
 $n = 47$ , and  $m = 12$ .

If not, then return to  
the original congruence.

In order for the backwards  
direction to be a valid move,  
choose  $m$  so that  $\gcd(m, n) = 1$ .

Note: The statement of the  
lemma is correct, but its  
use requires some care.