

(Working Notes) - Patrick Asaba  
(Presenter) - Jamie Brigitte  
(Rough Draft) - Lauren Remmes  
(Working Notes) - Tate Shippen  
(Final Draft) - Wayne Youngfano

Section 8  
Problem 8.2

Problem 8.2: Suppose that  
 $ac \equiv bc \pmod{m}$   
and also assume  $\gcd(c, m) = 1$ . Prove that  $a \equiv b \pmod{m}$ .

Proof: Linear Congruence Theorem States:  
When  $\gcd(a, m) = 1$  and the congruence statement  
is:

$$ax \equiv c \pmod{m}$$

this has only one solution:

$$x \equiv \frac{c}{a} \pmod{m}$$

Since we know  $\gcd(c, m) = 1$ , then:  
 $ac \equiv bc \pmod{m}$   
can be written as:

$$a \equiv \frac{bc}{c} \pmod{m}$$

$$\therefore a \equiv b \pmod{m}$$

Extension: Two Examples

(a)  $a=47, c=107, b=35, m=6$

$$47(107) \equiv 35(107) \pmod{6}$$

$$47 \equiv \frac{35(107)}{107} \pmod{6}$$

$$47 \equiv 35 \pmod{6}$$

$$\therefore 6 \mid 47 - 35 \Rightarrow 6 \mid 12 \checkmark$$

What is " $\frac{1}{107}$ " mod 6?

i.e. find  $x$  such that  $0 \leq x < 6$   
so that  $x \cdot 107 \equiv 1 \pmod{6}$

$$\Rightarrow x=5 \rightarrow 535 \equiv 1 \pmod{6}$$

(b)  $a=26, c=53, b=16, m=5$

$$26(53) \equiv 16(53) \pmod{5}$$

$$26 \equiv \frac{16(53)}{53} \pmod{5}$$

$$26 \equiv 16 \pmod{5}$$

$$\therefore 5 \mid 26 - 16$$

$$\Rightarrow 5 \mid 10 \checkmark$$