A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 8EC

Bookmark

Show all steps: ON

Problem

Prove the following for all integers *a*, *b*, *c*, *d* and all positive integers *m* and *n:*

If $ac \equiv bc \pmod{n}$ and $\gcd(c, n) \equiv 1$, then $a \equiv b \pmod{n}$.

Step-by-step solution

Step 1 of 2

Consider the congruence equation

$ac \equiv bc \pmod{n}$ and $\gcd(c,n) = 1$

The object of the problem is to prove that if $ac \equiv bc \pmod{n}$ and $\gcd(c,n) = 1$ then $a \equiv b \pmod{n}$.

Use the definition, $a \equiv b \pmod{n}$ iff n divides $a-b$ to prove the given result.

By the definition, n divides $ac - bc$

This implies that n divides $c(a-b)$

Comment

Step 2 of 2

Given that $\gcd(c,n) = 1$ and by the result, if $n' | cd$, and $\gcd(c,n') = 1$ then $n' | d$

Thus, by the result n divides $a-b$.

Again by the definition of congruence equation,

$a-b\equiv 0(\bmod p)$

$a\equiv b(\bmod p)$

Therefore, if $ac\equiv bc(\bmod n)$ and $\gcd(c,n)=1$ then $a\equiv b(\bmod n)$

Comment