A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 1EC

Bookmark

Show all steps: ON

Problem

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

If $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$.

Step-by-step solution

Step 1 of 3

Consider the congruence equation

$$a \equiv b(\text{mod}\, n)$$
$$b \equiv c(\text{mod}\, n)$$

Object of the problem is to prove that if $a \equiv b(\text{mod}\, n)$ and $b \equiv c(\text{mod}\, n)$then $a \equiv c(\text{mod}\, n)$.

Comment

Step 2 of 3

Use the definition, $a \equiv b(\text{mod}\, n)$ iff n divides $a-b$ to prove the result.

By the definition of congruence equation,

$$n \text{ divides } a-b$$
$$n \text{ divides } c-c$$

There are integers p and q such that

$$a-b=np$$
$$a=np+b$$
$$b-c=nq$$
$$b=nq+c$$

Comment

Step 3 of 3

Substitute $b=nq+c$ in $a=np+b$.

$$a=np+(nq+c)$$
$$a=n(p+q)+c$$
$$a-c=n(p+q)$$

Thus, n divides $a-c$

Again by the definition, $a \equiv c(\bmod n)$.

Therefore, if $a \equiv b(\bmod n)$ and $b \equiv c(\bmod n)$ then $a \equiv c(\bmod n)$.

Comment