A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 1ED

Bookmark

Show all steps: ON

Problem

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

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

Step-by-step solution

Step 1 of 4

Here, objective is to prove that $a \equiv b \ (\text{mod } n/d)$

Comment

Step 2 of 4

Consider a, b are integers, *m* is a positive integer.

If *m* divides $a-b$, then *a* is congruent to *b* modulo *m* which is represented by $a = b(\text{mod m})$

$\text{if } a = b(\text{mod m}), \text{ then } b = a(\text{mod m})$

Comment

Step 3 of 4

Consider $ac = bc(\text{mod } n), \gcd(c, n) = d$

$ac = bc(\text{mod } n)$, Can be written as

$a = c \pmod{n}$..(1)

$c = b$ (mod n)...(2)

from eq.(1)

$c = a$ (mod n)........(3)

from eq..(2)

$$\frac{c}{d} = \frac{b}{d} \left(\text{mod } \frac{n}{d}\right)$$

$$\frac{c}{d} = \frac{b}{d} + \text{k } \frac{n}{d} \text{....(4)}$$

Similarly, from eq...(3)

$$\frac{c}{d} = \frac{a}{d} + \text{q } \frac{n}{d} \text{............(5)}$$

Comment

Step 4 of 4

Equate equations...(4) and (5)

$$\frac{b}{d} + \text{k } \frac{n}{d} = \frac{a}{d} + \text{q } \frac{n}{d}$$

$$b + (kd)\frac{n}{d} = a + (qd)\frac{n}{d}$$

$$b - a = (kd - qd)\frac{n}{d}$$

$$b - a = r\frac{n}{d} \qquad (\because r = (kd - qd))$$

$$a \equiv b\left(\text{mod}\frac{n}{d}\right);$$

Hence, proved

Comment