A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 2ED

1 Bookmark

Show all steps: ON

Problem

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

If $a \equiv b \pmod{n}$, then $\gcd(a, n) = \gcd(b, n)$.

Step-by-step solution

Step 1 of 4

Here, objective is to prove that $\gcd(a,n) = \gcd(b,n)$

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

Properties:

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

Comment

Step 3 of 4

Consider

$$a = b(\bmod n)$$
$$a = b + rn............(1)$$
$$b = a(\bmod n)$$
$$b = a + np..............(2)$$
$$\text{let } \gcd(a,n) = d, \gcd(b,n) = e$$

Comment

Step 4 of 4

Consider $\gcd(a,n) = d$

$$d \mid a \text{ and } d \mid n$$
$$d \mid a - nr$$
$$d \mid b \text{ and } d \mid n$$
$$d \mid e$$

Consider $\gcd(b,n) = e$

$$e \mid b \text{ and } e \mid n$$
$$e \mid b - np$$
$$e \mid a \text{ and } e \mid n$$
$$e \mid d$$

That is *d* Is divisible by *e* and *e* is divisible by *d*

Therefore,

$$d = e$$
$$\gcd(a,n) = \gcd(b,n)$$

Hence, proved

Comment