A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 9ED

Bookmark

Show all steps: ON

Problem

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

If $a \equiv 1 \pmod{m}$, then *a* and *m* are relatively prime.

Step-by-step solution

Step 1 of 3

Consider the congruence relation $a \equiv 1(\bmod m)$. Objective is to prove that *a* and *m* are relatively prime.

By using the definition of congruence, if $a \equiv b(\bmod n)$ then $n \mid (a-b)$. So, if $a \equiv 1(\bmod m)$ then

$m \mid (a-1)$.

Comment

Step 2 of 3

There may arise following two cases:

Case 1: $m = 1$. Since the greatest common divisor of 1 with any positive integer is 1. Therefore, *a* and *m* will be relatively prime.

Case 2: if $m \neq 1$ and $m \mid (a-1)$, then there does not exist any integer that will divide *a* and $(a-1)$ both. So, *m* will not divide *a* and then $\gcd(a, m) = 1$.

Comment

Step 3 of 3

Hence, if $a \equiv 1 \pmod{m}$ then *a* and *m* are relatively prime.

Comment