A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 8ED

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 $a^2 + b^2 \equiv 2ab \pmod{n^2}$, and conversely.

Step-by-step solution

Step 1 of 4

Firstly consider that $a \equiv b(\bmod n)$. Objective is to prove that

$a^2 + b^2 \equiv 2ab(\bmod n^2)$.

By using the definition of congruence if $a \equiv b(\bmod n)$ then $n \mid (a-b)$. So for some integer *k* one have,

$(a-b) = nk$.

Take the square of both the sides and get:

$$(a-b)^2 = (nk)^2$$
$$a^2 - 2ab + b^2 = n^2k^2.$$

Comment

Step 2 of 4

Since *k* is an integer, so k^2 will also be an integer. By the definition of divisibility it implies that

$n^2 \mid (a^2 - 2ab + b^2)$.

And hence in the form of congruence one can write it as

$n^2 \mid (a^2+b^2)-2ab$.

Or equivalently,

$(a^2+b^2) \equiv 2ab (\mathrm{mod}\, n^2)$.

Comment

Step 3 of 4

Conversely, let $a^2+b^2 \equiv 2ab(\mathrm{mod}\, n^2)$. Task to show that

$a \equiv b(\mathrm{mod}\, n)$.

By using the given condition, (a^2+b^2-2ab) is divisible by n^2, so there exist some integer *k* such that

$(a^2+b^2-2ab) = n^2 k$, or $(a-b)^2 = n^2 k$.

On taking the positive square root both the sides, one get

$(a-b) = nk'$,

where k' is some integer. This will imply that $n \mid (a-b)$ and hence $a \equiv b(\mathrm{mod}\, n)$.

Comment

Step 4 of 4

Hence, $a \equiv b(\mathrm{mod}\, n)$ if and only if $a^2+b^2 \equiv 2ab(\mathrm{mod}\, n^2)$.

Comment