A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 4ED

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 $a^m \equiv b^m \pmod{n}$ for every positive integer *m*.

Step-by-step solution

Step 1 of 4

Consider the congruence equation

$a \equiv b(\operatorname{mod} n)$

Object of the problem is to prove that if $a \equiv b(\operatorname{mod} n)$ then $a^m \equiv b^m(\operatorname{mod} n)$ for every positive integer m.

Prove the result using mathematical induction on m.

Comment

Step 2 of 4

Let the statement be $p(m): a^m \equiv b^m \pmod n$

For $m = 1$,

$p(1): a \equiv b \pmod n$

By the hypothesis, the statement $p(1)$ is true.

Comment

Step 3 of 4

For $m = 2$, then show that $p(2): a^2 = b^2 \pmod n$

Use the result, $a \equiv b \pmod n$ iff n divides $a - b$ to prove the result.

So there is an integer p such that $a - b = np$

$$\begin{aligned} a^2 - b^2 &= (a-b)(a+b) \\ &= np(a+b) \\ &= ns \qquad \text{put } s = p(a+b) \end{aligned}$$

By the result of congruence equation, $a^2 \equiv b^2 \pmod n$

Comment

Step 4 of 4

Assume that the statement $p(m)$ is true for $m = k > 2$ and show that the statement $p(m+1)$ is true.

$$\begin{aligned} a^{m+1} - b^{m+1} &= a^{m+1} - ab^m + ab^m - b^{m+1} \\ &= a(a^m - b^m) + b^m(a-b) \end{aligned}$$

By the induction hypothesis, $a^m - b^m = np' \text{and } a - b = np$

$$\begin{aligned} a^{m+1} - b^{m+1} &= anp' - npb^m \\ &= n(ap' - pb^m) \\ &= nr' \qquad \text{take } ap' - pb^m = r' \end{aligned}$$

Thus, $a^{m+1} \equiv b^{m+1} \pmod n$

Hence, by the induction, the statement $a^m \equiv b^m \pmod n$ is true for positive integer m

Comment