A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 6EC

Bookmark

Show all steps: ON

Problem

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

If $a^2 \equiv b^2 \pmod{p}$, where *p* is a prime, then $a \equiv \pm b \pmod{p}$.

Step-by-step solution

Step 1 of 2

Consider the congruence equation

$a^2 \equiv b^2 \pmod{p}$, where p is a prime

The object of the problem is to prove that if $a^2 \equiv b^2 \pmod{p}$, where p is a prime then $a \equiv \pm b \pmod{p}$.

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

By the definition, p divides $a^2 - b^2$

This implies that p divides $(a-b)(a+b)$

Comment

Step 2 of 2

Here p is a prime and the result, if $p \mid cd$, where p is prime then $p \mid c$ or $p \mid d$

Thus, p divides $a-b$ or p divides $a+b$.

Again by the definition of congruence equation,

$$a-b \equiv 0 \pmod{p} \text{ or } a+b \equiv 0 \pmod{p}$$
$$a \equiv b \pmod{p} \text{ or } a \equiv -b \pmod{p}$$

Therefore, if $a^2 \equiv b^2 \pmod{p}$, where p is a prime then $a \equiv \pm b \pmod{p}$

Comment