# A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 7ED

Bookmark

Show all steps: ON

## Problem

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

If $a^2 \equiv 1 \pmod 2$, then $a^2 \equiv 1 \pmod 4$.

## Step-by-step solution

**Step 1** of 3

For some integer *a*, consider the following congruence:

$a^2 \equiv 1(\text{mod}\, 2)$.

Objective is to show that $a^2 \equiv 1(\text{mod}\, 4)$.

Since $a^2 \equiv 1(\text{mod}\, 2)$, therefore by the definition of congruence, one have

$2 \mid (a^2 - 1)$.

Factor $a^2 - 1$ as $(a+1)(a-1)$. Since 2 is prime, it must divide either $(a+1)$ or $(a-1)$. This shows that one of the factor is even.

But if $(a+1)$ is even, then so is $(a-1)$, because $a+1$ is even implies that *a* is odd so $a-1$ will be even.

Comment

**Step 2** of 3

Since *a* is odd then *a* will be of the form $2k+1$ for some integer *k*. So

$$\begin{aligned} a^2-1 &= (a+1)(a-1) \\ &= (2k+2)(2k) \\ &= 4k(k+1), \end{aligned}$$

where $k(k+1)$ is some integer value. Thus, $4 \mid (a^2-1)$ and by the definition of congruence it conclude that $a^2 \equiv 1 (\bmod 4)$.

Comment

**Step 3** of 3

Hence, if $a^2 \equiv 1 (\bmod 2)$, then $a^2 \equiv 1 (\bmod 4)$.

Comment