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

Chapter 23, Problem 3EE

Bookmark

Show all steps: ON

## Problem

Prove part:

($a$) Let $p$ a prime > 2. If $p \equiv 3 \pmod 4$, then $(p - 1)/2$ is odd.

($b$) Let $p > 2$ be a prime such that $p \equiv 3 \pmod 4$. Then there is *no* solution to the congruence $x^2 + 1 \equiv 0 \pmod p$. [HINT: Raise both sides of $x^2 \equiv -1 \pmod p$ to the power $(p - 1)/^2$, and use Fermat's little theorem.]

## Step-by-step solution

**Step 1** of 4

Consider any arbitrary odd prime number $p$, that is, $p > 2$. Suppose that $p \equiv 3(\bmod 4)$.

(a)

Objective is to prove that $(p-1)/2$ is odd.

If $p \equiv 3(\bmod 4)$then $p$ will be of the form

$p = 3 + 4n$,

for some integer $n$. Then

$$\begin{aligned}\frac{(p-1)}{2} &= \frac{(3+4n)-1}{2}\\ &= \frac{2+4n}{2}\\ &= 1+2n.\end{aligned}$$

Comment

**Step 2** of 4

Hence, if $p \equiv 3 \pmod 4$, then $(p-1)/2$ will be odd.

Comment

**Step 3** of 4

(b)

Objective is to show that there is no solution to the congruence $x^2+1 \equiv 0 \pmod p$.

Since $p \equiv 3 \pmod 4$, so $p = 3+4n$ for some integer *n*. Let, if possible, *a* be the solution of $x^2+1 \equiv 0 \pmod p$. Then

$a^2+1 \equiv 0 \pmod p$.

Or, $a^2 \equiv -1 \pmod p$. By Fermat's theorem,

$a^{p-1} \equiv 1 \pmod p$.

Also,

$(a^2)^{(p-1)/2} \equiv 1 \pmod p$, or $(-1)^{(p-1)/2} \equiv 1 \pmod p$.

Since $(p-1)/2$ is odd, so $(-1)^{(p-1)/2} \equiv -1 \pmod p$, a contradiction.

Comment

**Step 4** of 4

Hence, if $p \equiv 3 \pmod 4$ then there is no solution to the congruence $x^2+1 \equiv 0 \pmod p$.

Comment