A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 9EG

Bookmark

Show all steps: ON

Problem

In any integral domain, if $x^2 = 1$, then $x^2 - 1 = (x + 1)(x - 1) = 0$; hence $x = \pm 1$. Thus, an element $x \neq \pm 1$ cannot be its own multiplicative inverse. As a consequence, $\mathbb{Z}_p$ in p the integers $\overline{2}, \overline{3}, \ldots, \overline{p-2}$ may be arranged in pairs, each one being paired off with its multiplicative inverse.

Prove the following:

For any prime $p > 2$, $x^2 \equiv -1 \pmod{p}$ has a solution iff $p \neq 3 \pmod{4}$. (HINT: Use part 8 and Exercise E3.)

Step-by-step solution

Step 1 of 3

The objective is to prove that for any prime $p > 2$, the congruence $x^2 \equiv -1 \pmod{p}$ has a solution iff $p \neq 3 \pmod{4}$.

Comment

Step 2 of 3

Let for any prime $p > 2$.

Then, either $p = 4k + 1$ or $p = 4k + 3$ for some $k \in \mathbb{Z}^+$.

Let $p \neq 3 \pmod{4}$. Then, $p = 4k + 1$ for some $k \in \mathbb{Z}^+$.

By “part G8 of chapter 23”, the congruence $x^2 \equiv -1 \pmod{p}$ has a solution.

Comment

Step 3 of 3

Conversely, let for any prime $p > 2$, the congruence $x^2 \equiv -1 \pmod{p}$ has a solution, say a.

Then $a^2 \equiv -1 \pmod{p}$.

Since $a \not\equiv 0 \pmod{p}$, therefore, by Fermat's Theorem, $a^{p-1} \equiv 1 \pmod{p}$.

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

$$\left(a^2\right)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

If $p = 4k+3$, then $(-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1$.

This implies that $-1 \equiv 1 \pmod{p}$, that is, $p \mid 2$. This is a contradiction because p is prime.

Therefore, $p = 4k+1$ for some $k \in \mathbb{Z}^+$.

Hence, it is proved that for any prime $p > 2$, the congruence $x^2 \equiv -1 \pmod{p}$ has a solution iff $p \not\equiv 3 \pmod{4}$.

Comment