A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 7EG

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:

If $p \equiv 3 \pmod 4$, then $(p + 1)/2$ is even. (Why?) Conclude that

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

Step-by-step solution

Step 1 of 4

The objective is to prove that if $p \equiv 3(\bmod 4)$, then $\left(\frac{p-1}{2}\right)!^2 \equiv 1(\bmod p)$.

Comment

Step 2 of 4

Let $p \equiv 3(\bmod 4)$.

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

$$\frac{p+1}{2}=\frac{4k+3+1}{2}$$
$$=2k+2, \text{is even.}$$

Therefore, if $p \equiv 3 \pmod 4$, then $\frac{p+1}{2}$ is even.

Comment

Step 3 of 4

By Wilson's theorem, $(p-1)! \equiv -1 \pmod p$.

$$1\cdot 2\cdot \ldots \cdot \frac{p-1}{2}\cdot \frac{p+1}{2}\cdot \ldots \cdot (p-1) \equiv -1 \pmod p$$

Now,

$$\frac{p+1}{2} \equiv -\frac{p-1}{2} \pmod p$$
$$\frac{p+3}{2} \equiv -\frac{p-3}{2} \pmod p$$
$$\vdots$$
$$(p-1) \equiv -1 \pmod p$$

Using this,

$$1\cdot 2\cdot \ldots \cdot \frac{p-1}{2}\cdot \frac{p+1}{2}\cdot \ldots \cdot (p-1) \equiv -1 \pmod p$$
$$1\cdot 2\cdot \ldots \cdot \frac{p-1}{2}\cdot (-1)^{\frac{p-1}{2}}\cdot 1\cdot 2\cdot \ldots \cdot \frac{p-1}{2} \equiv -1 \pmod p$$
$$(-1)^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!^2 \equiv -1 \pmod p$$

Multiply both sides by $(-1)^{\frac{p-1}{2}}$.

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

As $\frac{p+1}{2}$ is even, $\left(\frac{p-1}{2}\right)!^2 \equiv 1 \pmod p$.

Comment

Step 4 of 4

Therefore, it is proved that if $p \equiv 3 \pmod{4}$, then $\left(\frac{p-1}{2}\right)!^2 \equiv 1 \pmod{p}$.

Comment