A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 5EG

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:

$[(p - l)/2]!^2 \equiv (-1)^{(p+1)/2} \pmod{p}$, for any prime $p > 2$. (HINT: Use Wilson's theorem.)

Step-by-step solution

Step 1 of 4

Here, objective is to prove that $[(p-1)/2]!^2 \equiv (-1)^{(p+1)/2} (\bmod\, p)$ for any prime $p > 2$.

Comment

Step 2 of 4

Wilson's theorem:

A positive integer $p>1$ is a prime if and only if $(p-1)!=-1(\bmod p)$.

And

$$(p-1)!=1\cdot 2\cdots\frac{p-1}{2}\cdot\frac{p+1}{2}\cdots\cdot(p-2)(p-1)$$

Comment

Step 3 of 4

Consider the congruence

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

Comment

Step 4 of 4

Consider

$$(p-1)!\equiv 1\cdot(-1).2\cdot(-2)\cdots\frac{p-1}{2}\cdot\left(-\frac{p-1}{2}\right)\cdots(\bmod p)$$

Rearrange the factors, then

$$(p-1)!(-1)^{(p-1)/2}((p-1)!\equiv\left(1\cdot 2\cdots\frac{p-1}{2}\right)^2(\bmod p)$$

$$-1\equiv(-1)^{(p-1)/2}\left[\left(\frac{(p-1)}{2}\right)!\right]^2(\bmod p)\qquad(\because(p-1)!=-1(\bmod p))$$

$$\left[\left(\frac{(p-1)}{2}\right)!\right]^2\equiv(-1)^{(p+1)/2}(\bmod p)$$

Hence, proved

Comment