

A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 2EG

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 $\overline{2}, \overline{3}, \dots, \overline{p-2}$ may be arranged in pairs, each one being paired off with its multiplicative inverse.

Prove the following:

$(p-2)! \equiv 1 \pmod{p}$ for any prime number p .

Step-by-step solution

Step 1 of 3

Consider the group \mathbb{Z}_p , for some prime number p . Objective is to show that

$$(p-2)! \equiv 1 \pmod{p}.$$

If p is any prime, then the only divisors of p will be 1 and p itself. So, the following numbers, that are less than p ,

$$1, 2, 3, \dots, p-2, p-1$$

will be relatively prime to p .

[Comment](#)

Step 2 of 3

Note that, for each of these integers a there is another b such that $ab \equiv 1 \pmod{p}$, where b is some unique modulo p .

From the question summary, if $x^2 = 1$ then $x = \pm 1$. That is, ± 1 are the only self-inverse elements. Since p is prime and $a = b$ if and only if $a = 1$ or $a = -1 \equiv p-1 \pmod{p}$. Now, if one omit 1 and $p-1$, then the others remaining can be grouped into the pairs such that product of each pair is 1. Therefore, in Z_p ,

$$2 \cdot 3 \cdots \overline{p-2} = 1.$$

Equivalently,

$$\begin{aligned} 1 \cdot 2 \cdot 3 \cdots \overline{p-2} &\equiv 1 \pmod{p} \\ (p-2)! &\equiv 1 \pmod{p}. \end{aligned}$$

[Comment](#)

Step 3 of 3

Hence, $(p-2)! \equiv 1 \pmod{p}$.

[Comment](#)