A Book of Abstract Algebra | (2nd Edition)

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

Prove the following:

In $\mathbb{Z}_p$, $\bar{2} \cdot \bar{3} \cdots \overline{p-2} = \bar{1}$.

Step-by-step solution

Step 1 of 3

Consider the group Z_p, for some prime number p. Objective is to show that in Z_p,

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

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,

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

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 $a = -1 \equiv p-1 (\bmod p)$. 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, the product of $2, 3, \ldots, p-2$ will be equal to 1.

Comment

Step 3 of 3

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

Comment