A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 3EG

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:

$(p - 1)! + 1 \equiv 0 \pmod p$ for any prime number p This is known as *Wilson's theorem*.

Step-by-step solution

Step 1 of 3

Consider the group Z_p, for some prime number p. Objective is to prove the following statement of Wilson's theorem:

$(p-1)!+1 \equiv 0 \pmod p$.

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,

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

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 $ab = 1 \pmod p$, 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, $\overline{2} \cdot \overline{3} \cdots \overline{p-2} = \overline{1}$. Or

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

Now, multiply both the sides of this equality by $p-1$ and get,

$$\begin{aligned} (p-1)(p-2)! &\equiv (p-1) \pmod{p} \\ (p-1)! &\equiv (0-1) \pmod{p} \\ (p-1)! &\equiv -1 \pmod{p} \\ (p-1)! + 1 &\equiv 0 \pmod{p}. \end{aligned}$$

Comment

Step 3 of 3

Hence, $(p-1)! + 1 \equiv 0 \pmod{p}$.

Comment