A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 4EG | 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:

For any composite number $n \neq 4$, $(n - 1)! \equiv 0 \pmod{n}$. [HINT: If p is any prime factor of n, then p is a

factor of $(n - 1)!$ Why?]

Before going on to the remaining exercises, we make the following observations: Let $p > 2$ be a prime. Then

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

Consequently,

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

REASON: $p - 1 \equiv -1 \pmod{p}$, $p - 2 \equiv -2 \pmod{p}$,$\cdots$, $(p + 1)/2 \equiv -(p - 1)/2 \pmod{p}$. With this result, prove the following:

Step-by-step solution

Step 1 of 3

Consider any composite number $n \neq 4$. Objective is to prove that

$(n-1)! \equiv 0 \pmod{n}$.

Since n is composite, so there exist some integer a, b such that

$n = ab$,

where $0 < a, b < n$. There may arise following two cases:

Case 1: if $a = b$, then $n = a^2$. Since a is the factor of n, therefore a will appear in $(n-1)!$. So,

$$\begin{aligned}(n-1)! &= 1 \times 2 \times \cdots \times a \times \cdots \times (n-a) \times \cdots \times (n-1) \\ &\equiv 1 \times 2 \times \cdots \times a \times \cdots \times (-a) \times \cdots \times (-1) \pmod{n} \\ &\equiv 1 \times 2 \times \cdots \times a^2 \times \cdots \times (-1) \pmod{n} \\ &\equiv 0 \pmod{n}.\end{aligned}$$

By using the equation $n = a^2$.

Comment

Step 2 of 3

Case 2: if $a \neq b$, then both *a* and *b* will appear as a separate terms in $(n-1)!$. Then their product will be equal to *n* and under modulo *n*, $(n-1)!$ will get reduced into $0 \pmod{n}$. That is,

$$\begin{aligned}(n-1)! &= 1 \times 2 \times \cdots \times a \times \cdots \times b \times \cdots \times (n-1) \\ &= 1 \times 2 \times \cdots \times ab \times \cdots \times \cdots \times (n-1) \\ &= 1 \times 2 \times \cdots \times n \times \cdots \times (n-1) \\ &\equiv 0 \pmod{n}.\end{aligned}$$

Comment

Step 3 of 3

Hence, for any composite number $n \neq 4$, $(n-1)! \equiv 0 \pmod{n}$.

Comment