# A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 5EF

Bookmark

Show all steps: ON

## Problem

Prove part:

For every $a \neq$ (mod $p$), $a^{p^n(p-1)}$, where $p$ is a prime.

## Step-by-step solution

**Step 1** of 3

Consider any arbitrary prime number $p$. Suppose that $a \neq 0(\bmod p)$.

Objective is to prove that

$$a^{p^n(p-1)} \equiv 1(\bmod p^{n+1}).$$

Prove this statement by using the Principle of mathematical induction.

If $n$ is zero, then $a^{p^0(p-1)} = a^{p-1}$. Since $a \neq 0(\bmod p)$, so there is no common factor between $a$ and $p$. That is, $\gcd(a, p) = 1$. By Fermat's theorem,

$$a^{p-1} \equiv 1(\bmod p).$$

Thus, result is true for zero value of $n$.

Comment

**Step 2** of 3

Suppose that above result holds for $n = k$, that is,

$$a^{p^k(p-1)} \equiv 1(\bmod p^{k+1}).$$

Or, for some integer $q$,

$a^{p^k(p-1)} = 1 + qp^{k+1}$.

Now, task is to show that result holds for $n = k+1$ as well.

Note that,

$$p^{k+1}(p-1) = p\left(p^k(p-1)\right).$$

Therefore,

$$\begin{aligned} a^{p^{k+1}(p-1)} &= a^{p\left(p^k(p-1)\right)} \\ &= \left(a^{p^k(p-1)}\right)^p \\ &= \left(1 + qp^{k+1}\right)^p \\ &= 1 + p_{C_1}\left(qp^{k+1}\right) + \cdots + \left(qp^{k+1}\right)^p \end{aligned}$$

The last step is obtained by the expansion of binomial theorem. Since $p \mid p_{C_1}$, so $p \mid p_{C_1}\left(qp^{k+1} + \cdots + \left(qp^{k+1}\right)^p\right)$. Therefore, for some integer $q'$,

$$a^{p^{k+1}(p-1)} = 1 + q'p^{k+2}.$$

Thus, $a^{p^{k+1}(p-1)} \equiv 1\left(\operatorname{mod} p^{k+2}\right)$.

Comment

**Step 3** of 3

Hence, by induction it conclude that $a^{p^n(p-1)} \equiv 1\left(\operatorname{mod} p^{n+1}\right)$, for every *n*.

Comment