A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 5EE

Bookmark

Show all steps: ON

Problem

Prove part:

Let *p* be a prime.

(*a*) If, $(p - 1) \mid m$, then $a^m \equiv 1 \pmod{p}$ provided that $p \nmid a$.

(*b*) If, $(p - 1) \mid m$, then $a^{m+1} \equiv a \pmod{pq}$ for all integers *a*.

Step-by-step solution

Step 1 of 4

(a)

Consider any arbitrary prime number *p*. Suppose $(p-1) \mid m$. Then objective is to prove that $a^m \equiv 1 (\bmod p)$, where $p \nmid a$.

Since $p \nmid a$, therefore both are relatively primes, or $\gcd(p, a) = 1$. Also $(p-1) \mid m$, for some integer *x*

$m = (p-1)x$.

Comment

Step 2 of 4

By Euler's theorem,

$a^{\phi(p)} \equiv 1 (\bmod p)$, or

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

Then

$$\begin{aligned} a^m &= a^{(p-1)x} \\ &= \left(a^{p-1}\right)^x \\ &\equiv 1^x \pmod{p} \\ &\equiv 1 \pmod{p} \end{aligned}$$

Thus, $a^m \equiv 1 \pmod{p}$.

Comment

Step 3 of 4

(b)

If $(p-1) \mid m$, then show that $a^{m+1} \equiv a \pmod{p}$ for all integers *a*.

From above part, if $p \nmid a$ then $a^m \equiv 1 \pmod{p}$. Then multiply by *a* both the side yields,

$$a^{m+1} \equiv a \pmod{p}.$$

If $p \mid a$ then $a \equiv 0 \pmod{p}$. Then

$$\begin{aligned} a^{m+1} &\equiv 0 \\ &\equiv a \pmod{p}. \end{aligned}$$

Comment

Step 4 of 4

Hence, if $(p-1) \mid m$ then $a^{m+1} \equiv a \pmod{p}$ for all integers *a*.

Comment