A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 2EF

Bookmark

Show all steps: ON

Problem

Prove part:

If gcd (a, n) = 1, then $a^{m\phi(n)} \equiv 1 \pmod{n}$ for all values of m.

Step-by-step solution

Step 1 of 2

Consider any two relatively prime numbers a and n, that is,

$$\gcd(a, n) = 1.$$

Objective is to prove that

$$a^{m\phi(n)} \equiv 1 \pmod{n}$$

for all values of m.

Since $\gcd(a, n) = 1$, then by Euler's theorem,

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Comment

Step 2 of 2

Then raise both the sides of this congruence to the power m, as:

$$\begin{aligned} \left(a^{\phi(n)}\right)^m &\equiv 1^m \pmod{n} \\ a^{m\phi(n)} &\equiv 1^m \pmod{n} \\ &\equiv 1 \pmod{n}. \end{aligned}$$

(note that this m was arbitrary).

Thus, $a^{m\phi(n)} \equiv 1 \pmod{n}$ for all values of m.

Comment