A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 3EF

Bookmark

Show all steps: ON

Problem

Prove part:

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

Step-by-step solution

Step 1 of 3

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

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

Suppose that $\gcd(a, mn) = 1$. Objective is to prove that

$a^{\phi(m)\phi(n)} \equiv 1 (\bmod mn)$.

Consider the following result:

If $a \equiv 1(\bmod m)$ and $a \equiv 1(\bmod n)$ where $\gcd(m, n) = 1$, then $a \equiv 1(\bmod mn)$.

Comment

Step 2 of 3

By using the greatest common divisor's property, if $\gcd(a, mn) = 1$ then

$\gcd(a, m) = 1$,

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

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

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

Then raise both the sides of this congruence to the power $\phi(m)$, as:

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

Comment

Step 3 of 3

Similarly, since $\gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod m$. Also,

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

As *m* and *n* are both relatively primes, therefore by the above result

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

Comment