A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 8EF

Bookmark

Show all steps: ON

Problem

If gcd (m, n) = l, prove that $n^{\phi(m)} + m^{\phi(n)} \equiv 1 \pmod{mn}$.

Step-by-step solution

Step 1 of 3

Consider any two relatively prime numbers *m* and *n*, that is, $\gcd(m,n)=1$. Objective is to prove that

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

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

Since $\gcd(m,n)=1$, so one can apply Euler's theorem and get,

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

Also, $n^{\phi(m)} \equiv 0(\bmod n)$.

On adding both the congruences, one get

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

Similarly, again by Euler's theorem, $m^{\phi(n)} \equiv 0(\bmod m)$. Also, $n^{\phi(m)} \equiv 1(\bmod m)$.

On adding both the congruences, one get

$n^{\phi(m)} + m^{\phi(n)} \equiv 1(\mathrm{mod}\, m)$.

Thus, by using the above result it implies that $n^{\phi(m)} + m^{\phi(n)} \equiv 1(\mathrm{mod}\, mn)$.

Comment

Step 3 of 3

Hence, if $\gcd(m, n) = 1$ then $n^{\phi(m)} + m^{\phi(n)} \equiv 1(\mathrm{mod}\, mn)$.

Comment