A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 9EF

Bookmark

Show all steps: ON

Problem

If l, m, n are relatively prime in pairs, prove that $(mn)^{\phi(l)} + (ln)^{\phi(m)} + (lm)^{\phi(n)} \equiv 1 \pmod{lmn}$.

Step-by-step solution

Step 1 of 5

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

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

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 5

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

$$(mn)^{\phi(l)} \equiv 1(\bmod l).$$

Since $ln \equiv 0(\bmod l)$, so

$$(ln)^{\phi(l)} \equiv 0(\bmod l).$$

Similarly, $lm \equiv 0(\bmod l)$, so

$$(lm)^{\phi(l)} \equiv 0(\bmod l).$$

Comment

Step 3 of 5

Now similarly, under modulo *m* and *n*:

$$(ln)^{\phi(m)} \equiv 1(\text{mod}\, m)$$
$$(mn)^{\phi(m)} \equiv 0(\text{mod}\, m)$$
$$(lm)^{\phi(m)} \equiv 0(\text{mod}\, m)$$

and

$$(lm)^{\phi(n)} \equiv 1(\text{mod}\, n)$$
$$(mn)^{\phi(n)} \equiv 0(\text{mod}\, n)$$
$$(ln)^{\phi(n)} \equiv 0(\text{mod}\, n).$$

Comment

Step 4 of 5

Now the following sum $(mn)^{\phi(l)} + (ln)^{\phi(m)} + (lm)^{\phi(n)}$ under $(\text{mod}\, l)$ will be:

$$(mn)^{\phi(l)} + (ln)^{\phi(m)} + (lm)^{\phi(n)} = 1 + 0 + 0 \equiv 1(\text{mod}\, l).$$

Also,

$$(mn)^{\phi(l)} + (ln)^{\phi(m)} + (lm)^{\phi(n)} \equiv 1(\text{mod}\, m),$$
$$(mn)^{\phi(l)} + (ln)^{\phi(m)} + (lm)^{\phi(n)} \equiv 1(\text{mod}\, n).$$

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

Comment

Step 5 of 5

Hence, if $\gcd(l, m, n) = 1$ then $(mn)^{\phi(l)} + (ln)^{\phi(m)} + (lm)^{\phi(n)} \equiv 1(\text{mod}\, lmn)$.

Comment