A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 4EE

1 Bookmark

Show all steps: ON

Problem

Prove part:

Let p and q be distinct primes. Then $p^{q-1} + q^{p-1} \equiv 1 (\text{mod } pq)$.

Step-by-step solution

Step 1 of 3

Consider any two distinct prime numbers p and q. Objective is to prove that

$p^{q-1} + q^{p-1} \equiv 1(\text{mod } pq)$.

Since p and q are distinct prime numbers, therefore both are relatively primes, or

$\gcd(p, q) = 1$.

Consider the following result:

If $a \equiv 1(\text{mod } m)$ and $a \equiv 1(\text{mod } n)$ where $\gcd(m, n) = 1$, then $a \equiv 1(\text{mod } mn)$.

Comment

Step 2 of 3

By Fermat's theorem,

$p^{q-1} \equiv 1(\text{mod } q)$.

Also, $q^{p-1} \equiv 0(\text{mod } q)$.

On adding both the congruences, one get

$p^{q-1} + q^{p-1} \equiv 1(\text{mod } q)$.

Similarly, again by Fermat's theorem, $q^{p-1} \equiv 1(\mathrm{mod}\ p)$. Also, $p^{q-1} \equiv 0(\mathrm{mod}\ p)$.

On adding both the congruences, one get

$$p^{q-1} + q^{p-1} \equiv 1(\mathrm{mod}\ p).$$

Thus, by using the above result it implies that $p^{q-1} + q^{p-1} \equiv 1(\mathrm{mod}\ pq)$.

Comment

Step 3 of 3

Hence, for distinct primes *p* and *q*, $p^{q-1} + q^{p-1} \equiv 1(\mathrm{mod}\ pq)$.

Comment