A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 6EE

Bookmark

Show all steps: ON

Problem

Prove part:

Let *p* and *q* be distinct primes.

(*a*) If $(p - 1) \mid m$ and $(q - 1) \mid m$, then $am \equiv 1 \pmod{pq}$ for any *a* such that $p \nmid a$ and $q \nmid a$.

(*b*) If $(p - 1) \mid m$ and $(q - 1) \mid m$, then $a^{m+1} \equiv a \pmod{pq}$ for integers *a*.

Step-by-step solution

Step 1 of 4

(a)

Consider any two distinct prime numbers *p* and *q*. Suppose $(p-1) \mid m$ and $(q-1) \mid m$. Then objective is to prove that $a^m \equiv 1 \pmod{pq}$, where $p \nmid a$ and $q \nmid a$.

Consider the following result:

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

Comment

Step 2 of 4

Since $p \nmid a$, therefore both are relatively primes, or $\gcd(p,a) = 1$. Similarly, from $q \nmid a$ one have $\gcd(q,a) = 1$.

Some result says that, if $(p-1) \mid m$ and $p \nmid a$, then

$a^m \equiv 1 \pmod{p}$.

Similarly, if $(q-1)|m$ and $q \nmid a$, then

$$a^m \equiv 1 \pmod{q}.$$

As *p* and *q* are both distinct, from the above result it implies that

$$a^m \equiv 1 \pmod{pq}.$$

Comment

Step 3 of 4

(b)

If $(p-1)|m$ and $(q-1)|m$. Then show that $a^{m+1} \equiv a \pmod{pq}$ for integers *a*.

From above part, if $p, q \nmid a$ then $a^m \equiv 1 \pmod{pq}$. Then multiply by *a* both the side yields,

$$a^{m+1} \equiv a \pmod{pq}.$$

If $p, q | a$ then $a \equiv 0 \pmod{pq}$. Then

$$\begin{aligned} a^{m+1} &\equiv 0 \\ &\equiv a \pmod{pq} \end{aligned}$$

Comment

Step 4 of 4

Hence, if $(p-1)|m$ and $(q-1)|m$ then $a^{m+1} \equiv a \pmod{pq}$ for integers *a*.

Comment