A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 6EF Bookmark Show all steps: ON

Problem

Prove part:

Under the conditions of part 3, if t is a common multiple of $\phi(m)$ and $\phi(n)$, then $a^t \equiv 1 \pmod{mn}$. Generalize to three integers l, m, and n.

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 $\gcd(a, mn) = 1$. Then

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

If t is a common multiple of $\phi(m), \phi(n)$, then objective is to prove that

$$a^t \equiv 1 \pmod{mn}.$$

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 3

Since t is a common multiple of $\phi(m), \phi(n)$, so for some integers x and y one have,

$$t = x \cdot \phi(m),$$
$$t = y \cdot \phi(n).$$

Then

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

Similarly,

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

Comment

Step 3 of 3

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

$$a^y \equiv 1 \pmod{mn}.$$

Comment