A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 5EI

Bookmark

Show all steps: ON

Problem

Recall that V_n is the multiplicative group of all the invertible elements in $\mathbb{Z}_n$. If V_n happens to be cyclic, say $V_n = \langle m \rangle$, then any integer $a \equiv m \pmod{n}$ is called a *primitive root* of n.

Suppose m has a primitive root, and let n be relatively prime to $\phi(m)$. (Suppose $n > 0$.) Prove that if a is relatively prime to m, then $x^n \equiv a \pmod{m}$ has a solution.

Step-by-step solution

Step 1 of 4

Here, objective is to prove that $x^n = a(\bmod m)$ has a solution, if a is relatively prime to m.

Comment

Step 2 of 4

V_n is the multiplicative group of all the invertible elements in Z_n. If V_n happens to be cyclic $V_n = m\rangle$.Then any integer g is called a primitive root of n.

Comment

Step 3 of 4

The congruence $x^a = b(\bmod n)$ has a solution, if $\gcd(a, n-1) = 1$.

Comment

Step 4 of 4

Consider m has a primitive root and

n is relatively prime $\phi(m)$

$\phi(m)$ is the order m in V_n

$$\phi(m) = m - 1$$
$$\gcd(n, \phi(m)) = 1$$
$$\gcd(n, m - 1) = 1$$

Since,

n is relatively prime $\phi(m)$.

Therefore,

$x^n = a(\text{mod}\, m)$ has a solution.

Hence, proved

Comment