A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 1EI | 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.

Prove that a is a primitive root of n iff the order of $\bar{a}$ in V_n is $\phi(n)$.

Step-by-step solution

Step 1 of 4

Here, objective is to prove that, *a* is a primitive root of n if and only if the order of $\bar{a}$ in v_n is $\phi(n)$.

Comment

Step 2 of 4

Primitive root of *n:*

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 $a = m \pmod{n}$ is called a primitive root of *n.*

Comment

Step 3 of 4

Consider Euler’s phi function $\phi(n)$.

It measures the positive integers up to *n* and that are relative prime to *n.* It is a multiplicative function. That is $\phi(mn)=\phi(m)\phi(n);\ \text{ if }\ \gcd(m,n)=1$

So this function determines the order of the multiplicative group of integers modulo *n.*

Comment

Step 4 of 4

V_n is also multiplicative group of all the invertible elements in Z_n

Then, the number of elements in Z_n is determined by Euler’s function $\phi(n)$

By using Euler’s theorem

$a^{\phi(n)}=1\bmod n;$

For every *a* co prime to *n.*

Therefore, the order of $\bar{a}$ in v_n is $\phi(n)$.

Hence, proved

Comment