A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 4EI

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 a is a primitive root of m. Prove: If b is any integer which is relatively prime to m, then $b \equiv a^k \pmod{m}$ for some $k \geq 1$.

Step-by-step solution

Step 1 of 3

Here, objective is to prove that, b is relatively prime to m such that $b = a^k \pmod{m}$ for $k \geq 1$

Comment

Step 2 of 3

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*.

Relatively prime:

If (a,b) are relatively prime, then $\gcd(a,b) = 1$

Comment

Step 3 of 3

Let $a = 2$ is a primitive root $m = 5$

Then,

$$2^1 \bmod 5 = 2$$
$$2^2 \bmod 5 = 4$$
$$2^3 \bmod 5 = 3$$

By observing, $b = 2^k \bmod 5$ is relatively prime to $\bmod 5$ for any integer *k*.

Therefore,

If a is a primitive root of m, then b is relatively prime to m such that $b = a^k (\bmod m)$ for $k \geq 1$

Hence, proved

Comment