A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 3EI

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*.

Find primitive roots of the following integers (if there are none, say so): 6, 10, 12, 14, 15.

Step-by-step solution

Step 1 of 7

Here, objective is to find the primitive roots of given integers.

Comment

Step 2 of 7

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 7

To find primitive root of 6:

Consider $a = 5$

$$\gcd(a,10) = 1,$$
$$\phi(n) = 2$$

$$5^2 = 1$$

By observing, 5 having order $2 \pmod 6$

Therefore, the primitive root for 6 is 5

Comment

Step 4 of 7

To find primitive root of 10:

Consider $a = 3,7,9$:

$$\gcd(a,10) = 1$$
$$\phi(n) = 4$$

$$3^4 = 1, 3^2 = 9, 7^2 = 9, 7^4 = 1$$

By observing, $3,7$ having order $4 \pmod{10}$

Therefore, the primitive roots for 10 are $3,7$

Comment

Step 5 of 7

To find primitive root of 12:

Consider $a = 5,7,11$:

$$\gcd(a,15) = 1$$

Then,

There is no integer *a* having order $4 \pmod{12}$

Therefore, there are no primitive roots for 12.

Comment

Step 6 of 7

To find primitive root of 14:

Consider $a = 3,5,9,11,13$:

$$\gcd(a,14) = 1$$

$$\phi(n) = 6$$

By observing, $3,5$ having order $6 \pmod{14}$

Therefore, the primitive roots for 14 are $3,5$.

Comment

Step 7 of 7

To find primitive root of 15:

Consider $a = 2,4,7,8,11,13,14$:

$\gcd(a,15) = 1$

$\phi(n) = 8$

$2^4 = 1, 4^2 = 1, 7^2 = 1, 8^2 = 1, 11^2 = 1, 13^2 = 1, 14^2 = 1$

By observing, there are no integers having order $8 \pmod{15}$

Therefore, there are no primitive roots for 15.

Comment