

# A Book of Abstract Algebra | (2nd Edition)

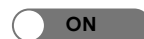


Chapter 23, Problem 2EI



Bookmark

Show all steps:



## 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 every prime number  $p$  has a primitive root. (HINT: For every prime  $p$ ,  $\mathbb{Z}_p^*$  is a cyclic group.

The simple proof of this fact is given as Theorem 1 in Chapter 33.)

## Step-by-step solution

### Step 1 of 3

Here, objective is to prove that, every prime number  $p$  has a primitive root.

[Comment](#)

### Step 2 of 3

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

[Comment](#)

### Step 3 of 3

If  $p = 2$ , then  $g = 1$  is a primitive root

Consider

$P$  is a prime and  $P > 2$ ,  $n$  is the least universal exponent for  $P$ .

That means  $n$  is the smallest positive integer

$$x_n \equiv 1 \pmod{p}; \forall x \in \mathbb{Z} / p\mathbb{Z}.$$

And we have the multiplicative order of  $g$  is  $n$ .

By using Fermat's little theorem,

$$n \leq p - 1$$

$f(x) = x_n - 1$  has at most  $n$  roots over the field  $\mathbb{Z} / p\mathbb{Z}$  and

$f(x) \equiv 0 \pmod{p}$  for all non zero  $x \pmod{p}$

Then,

$$n \geq p - 1$$

$$n = p - 1$$

And  $g$  is exact order of  $P - 1$

Hence,  $g$  is a primitive root.

---

[Comment](#)