A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 6EI

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.

Let $p > 2$ be a prime. Prove that every primitive root of p is a quadratic nonresidue, modulo p. (HINT: Suppose a primitive root α is a residue; then every power of a is a residue.)

Step-by-step solution

Step 1 of 3

Here, objective is to prove that, every primitive root of p is a quadratic non residue modulo p

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.*

Comment

Step 3 of 3

Consider $p > 2$ and p be a prime.

Then, $p-1 > \frac{(p-1)}{2}; \forall \text{primes } p$

Consider a is a primitive root and quadratic residue modulo p

Then,

$$\text{ord}_p a = p-1$$

Euler's criterion states that,

$$a^{(p-1)/2} = 1 \bmod p$$

But the above condition is impossible. Since

$$p-1 > \frac{(p-1)}{2}; \forall \text{primes } p$$

Therefore,

Every quadratic non residue mod p is a primitive root of p for $p > 2$ and p be a prime.

Hence, proved

Comment