A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 7EI

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.

A prime p of the form $p = 2^m + 1$ is called a *Fermat prime*. Let p be a Fermât prime. Prove that every quadratic nonresidue mod p is a primitive root of p. (HINT: How many primitive roots are there? How many residues? Compare.)

Step-by-step solution

Step 1 of 4

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

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.*

Fermat's little theorem:

$a^{p-1} = 1 \bmod p; p$ is prime

Comment

Step 3 of 4

Consider is *a* primitive root of n.

Consider prime $p = 2^m + 1$

$$a^{p-1} = 1 \bmod p \quad (\because \text{Fermat's little theorem})$$

$$a^{2^m+1-1} = 1 \bmod p$$

$$a^{2^m} = 1 \bmod p$$

By using Lagrange's theorem, *a* must have order

$$2^k; 0 \le k \le m$$

Comment

Step 4 of 4

Consider *a* is quadratic non residue mod *p*

Then, $\left(\frac{a}{P}\right) = -1$

Euler's criterion states that, $\left(\frac{a}{P}\right) = a^{(p-1)/2} \bmod p$

Then *a* cannot have order

$$2^k; 0 \le k \le m$$

But *a* has the order, 2^m

That is *a* is a primitive root of *p.*

Therefore,

Every quadratic non residue mod *p* is a primitive root of *p.*

Hence, proved

Comment