A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 3EH

Bookmark

Show all steps: ON

Problem

An integer *a* is called a *quadratic residue* modulo *m* if there is an integer *x* such that $x^2 \equiv a$ (mod *m*). This is the same as saying that $\bar{a}$ is a square in $\mathbb{Z}_m$. If *a* is not a quadratic residue modulo *m*, then *a* is called a *quadratic nonresidue* modulo *m*. Quadratic residues are important for solving quadratic congruences, for studying sums of squares, etc. Here, we will examine quadratic residues modulo an arbitrary prime $p > 2$.

Let $h : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ be defined by $h(\bar{a}) = \bar{a}^2$.

Referring to part 2, let the two cosets of *R* be called 1 and -1. Then $\mathbb{Z}_p^*/R = \{1, -1\}$.

Explain why

$$\left(\frac{a}{p}\right) = h(\bar{a})$$

for every integer *α* which is not a multiple of *p*.

Step-by-step solution

Step 1 of 4

Here, objective is to explain why $\left(\frac{a}{P}\right) = h(\bar{a})$ for every integer *a* which is not a multiple of *p*.

Comment

Step 2 of 4

Consider the congruence $x^2 = a \pmod{p}$ where *p* is odd prime, is solvable, if and only if the

Legendre symbol $\left(\frac{a}{P}\right)=1$ .Where, $\left(\frac{a}{P}\right)=a^{(p-1)/2}(\text{mod } p)$

Comment

Step 3 of 4

Consider

$Z_p / R=\{1,-1\}$

$\text{if } a^2=b^2$

$a=\pm b$

$x \neq \pm a$

$x=a$

Comment

Step 4 of 4

Consider $(1,-1)$, have the same square.

$(1)^2=(-1)^2$

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

Then, , $\left(\frac{a}{P}\right)=a^2$

$$\left(\frac{a}{P}\right)=h(\bar{a})$$

Therefore,

$\left(\frac{a}{P}\right)=h(\bar{a})$ for every integer *a* which is not a multiple of *p.*

Hence, proved.

Comment