A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 2EH

Bookmark

Show all steps: ON

Problem

An integer *a* is called a *quadratic residue* modulo *m* if there is an integer *x* such that $x^2 \equiv a \pmod m$. 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 $h(\bar{a}) = \bar{a}^2$.

The range of *h* has $(p - 1)/2$ elements. Prove: If ran $h = R$, R is a subgroup of $\mathbb{Z}_p^*$ having two cosets.

One contains all the residues, the other all the nonresidues.

The *Legendre symbol* is defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } p \nmid a \text{ and } a \text{ is a residue mod } p. \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is a nonresidue mod } p. \\ 0 & \text{if } p \mid a. \end{cases}$$

Step-by-step solution

Step 1 of 2

The objective is to prove that if $\operatorname{ran} h = R$, then R is a subgroup of $\mathbb{Z}_p^*$ having two cosets.

Comment

Step 2 of 2

Since $h:\mathbb{Z}_p^* \to \mathbb{Z}_p^*$ is a homomorphism, therefore, by Theorem 2 of Chapter 14, $\operatorname{ran} h = R$ is a subgroup of $\mathbb{Z}_p^*$.

By Lagrange's Theorem (Theorem 3, Chapter 13), number of distinct cosets of R is equal to the number of elements in G divided by the number of elements in R, that is, $p-1$ divided by $(p-1)/2$.

$$(p-1)\div\left(\frac{p-1}{2}\right)=2.$$

Therefore, it is proved that if $\operatorname{ran} h = R$, then R is a subgroup of $\mathbb{Z}_p^*$ having two cosets.

Comment