A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 1EH | 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 $h(\bar{a}) = \bar{a}^2$.

Prove *h* is a homomorphism. Its kernel is $\{\pm\bar{1}\}$.

Step-by-step solution

Step 1 of 4

The objective is to prove that h is a homomorphism and its kernel is $\{\pm\bar{1}\}$.

Comment

Step 2 of 4

Definition 1: If $f : G_1 \to G_2$ is a function such that for any two elements a and b in G_1, $f(ab) = f(a)f(b)$, then f is a homomorphism.

Definition 2: Let $f : G_1 \to G_2$ be a homomorphism. The kernel of f is the set K of all the elements of G_1 which are carried by f onto the neutral element of G_2.

In other words, $K = \{x \in G_1 \mid f(x) = e\}$.

Comment

Step 3 of 4

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

Let a_1 and a_2 be any two elements of $\mathbb{Z}_p^*$.

Then there exist x_1 and x_2 such that $x_1^2 \equiv a_1 \pmod{p}$ and $x_2^2 \equiv a_2 \pmod{p}$.

Therefore, $x_1^2 x_2^2 \equiv a_1 a_2 \pmod{p}$, that is, $(x_1 x_2)^2 \equiv a_1 a_2 \pmod{p}$.

This shows that $h(\overline{a_1 a_2}) = \overline{a_1 a_2}^2$.

Therefore, h is a homomorphism.

Comment

Step 4 of 4

To find kernel, let $h(\overline{k}) = 1$ for some $k \in \mathbb{Z}_p^*$.

Then $k^2 \equiv 1 \pmod{p}$.

This implies $p \mid (k-1)(k+1)$.

Therefore, $k = 1$ or $k = -1$.

Hence, $K = \{\pm \overline{1}\}$.

Comment