A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 6EH

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 $h(\bar{a}) = \bar{a}^2$.

Prove: (a) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ (b) $\left(\frac{a^2}{p}\right) =$ if $p \nmid a$

Step-by-step solution

Step 1 of 4

Here, objective is to prove that $\left(\frac{a}{P}\right)\left(\frac{b}{P}\right) = \left(\frac{ab}{P}\right)$ and $\left(\frac{a^2}{P}\right) = 1$.

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

(a)

Consider

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

$$\left(\frac{b}{P}\right) = b^{(p-1)/2} (\text{mod } p)$$

Then,

$$\begin{aligned}\left(\frac{a}{P}\right)\left(\frac{b}{P}\right) &= a^{(p-1)/2} (\text{mod } p) b^{(p-1)/2} (\text{mod } p) \\ &= a^{(p-1)/2} b^{(p-1)/2} (\text{mod } p) \\ &= (ab)^{(p-1)/2} (\text{mod } p) \\ &= \left(\frac{ab}{P}\right)\end{aligned}$$

Hence, proved

Comment

Step 4 of 4

(b)

Consider

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

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

$$=(\pm 1)^2 \qquad (\because (a/p)=\pm 1; p \dagger a)$$

$$=1$$

$$\left(\frac{a^2}{P}\right)=1$$

Hence, proved

Comment