A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 5EH

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: if $a \equiv b$ (mod p), then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. In particular, $\left(\frac{a+kp}{p}\right) = \left(\frac{a}{p}\right)$

Step-by-step solution

Step 1 of 4

Here, objective is to prove that $\left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$, if $a = b \pmod p$ and $\left(\frac{a+kp}{P}\right) = \left(\frac{a}{P}\right)$.

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

Comment

Step 3 of 4

If $a = b \pmod p$, then $x^2 = a \pmod p$ if and only if $x^2 = b \pmod p$

That means one of the above equations is not solvable or solvable if and only if same is true for the other.

For $x^2 = a \pmod p$

The Legendre symbol is $\left(\frac{a}{P}\right)$

For $x^2 = b \pmod p$

The Legendre symbol is $\left(\frac{b}{P}\right)$

Therefore, the above equations are solvable or not solvable if and only if $\left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$

Comment

Step 4 of 4

$$x^2 = a \pmod{p},$$
$$x^2 = b \pmod{p}.$$

Then, we can write as

$$b = a \ (\text{mod } p)$$
$$b = a + pk; k \text{ is an integer}$$
$$\left(\frac{b}{P}\right) = \left(\frac{a}{P}\right)$$
$$\left(\frac{a+kp}{P}\right) = \left(\frac{a}{P}\right)$$

Therefore,

$\left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$, if $a = b \pmod{p}$, and also $\left(\frac{a+kp}{P}\right) = \left(\frac{a}{P}\right)$.

Hence, proved

Comment