A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 7EH

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

$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$ (HINT: Use Exercises G6 and 7.)

The most important rule for computing

$$\left(\frac{a}{p}\right)$$

is the *law of quadratic reciprocity*, which asserts that for distinct primes p, $q > 2$,

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \text{if } p, q \text{ are both} \equiv 3 \pmod 4 \\ \left(\frac{q}{p}\right) & \text{otherwise} \end{cases}$$

(The proof may be found in any textbook on number theory, for example, *Fundamentals of Number Theory* by W. J. LeVeque.)

Step-by-step solution

Step 1 of 4

Here, objective is to prove that $\left(\frac{-1}{P}\right)=\begin{cases}1 & \text{if } p=1(\text{mod }4)\\ -1 & \text{if } \quad p=3(\text{mod }4)\end{cases}$.

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

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

$$\begin{aligned}&\text{if}\, p=1+4k,\\ &(-1)^{(p-1)/2}=(-1)^{2k}\\ &\qquad\qquad=1\\ &\text{if }\ p=3+4k,\\ &(-1)^{(p-1)/2}=(-1)^{2k+1}\\ &\qquad\qquad=-1\end{aligned}$$

Comment

Step 4 of 4

Then, from the above simplifications

$$\left(\frac{-1}{P}\right)=\begin{cases} 1 & \text{if } p=1+4k \\ -1 & \text{if } \quad p=3+4k \end{cases}$$

$$\left(\frac{-1}{P}\right)=\begin{cases} 1 & \text{if } p=1(\bmod 4) \\ -1 & \text{if } \quad p=3(\bmod 4) \end{cases}$$

Hence, proved

Comment