A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 9EH

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

Which of the following congruences is solvable?

(a) $x^2 = 30 \pmod{101}$

(b) $x^2 \equiv 6 \pmod{103}$

(c) $2x^2 \equiv 70 \pmod{106}$

NOTE: $x^2 \equiv a \pmod{p}$ is solvable iff *a* is a quadratic residue modulo *p* iff

$$\left(\frac{a}{p}\right) = 1$$

Step-by-step solution

Step 1 of 5

Here, objective is to find which of the given congruence’s are solvable.

Comment

Step 2 of 5

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

Rules to find Legendre symbol:

$$
\begin{aligned}
&1.(a/n) = (b/n),\ \text{if}\ \ a = b \bmod n \\
&2.(1/n) = 1\ \ \text{and}\ \ (0/n) = 0 \\
&3.(2m/n) = (m/n)\ \ \text{if}\ \ n = \pm 1 \bmod 8. \\
&\text{otherwise}(2m/n) = -(m/n)
\end{aligned}
$$

Comment

Step 3 of 5

(a)

Consider the congruence

$$x^2 = 30 \pmod{101}$$

$$a = 30, p = 101.$$

Find Legendre symbol

$$
\begin{aligned}
\frac{30}{101} &= -\frac{15}{101} \\
&= -\frac{11}{15} \\
&= \frac{4}{11} \\
&= -\frac{2}{11} \\
&= \frac{1}{11} \\
&= 1
\end{aligned}
$$

$$\frac{30}{101} = 1$$

Hence, the congruence is solvable.

Comment

Step 4 of 5

(b)

Consider the congruence

$x^2 = 6 \pmod{103}$

$a = 6, p = 103.$

Find Legendre symbol

$$\frac{6}{103} = \frac{3}{103}$$
$$= \frac{3}{103}$$
$$= -\frac{1}{3}$$
$$= -1$$

$$\frac{6}{103} = -1$$

Hence, the congruence is not solvable.

Comment

Step 5 of 5

(C)

Consider the congruence

$$2x^2 = 70 \pmod{106}$$
$$2x^2 = 70 + 106k$$
$$x^2 = 35 + 53k$$
$$x^2 = 35 \pmod{53}$$
$$a = 35 p = 53.$$

Find Legendre symbol

$$\frac{35}{53} = \frac{18}{35}$$
$$= -\frac{9}{35}$$
$$= -\frac{8}{9}$$
$$= -\frac{4}{9}$$
$$= -\frac{2}{9}$$
$$= -\frac{1}{9}$$
$$= -1$$
$$\frac{35}{53} = -1$$

Hence, the congruence is not solvable.

Comment