A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 4EA

Bookmark

Show all steps: ON

Problem

Solve the following quadratic congruences. (If there is no solution, write "none.")

(a) $6x^2 \equiv 9 \pmod{15}$

(b) $60x^2 \equiv 18 \pmod{24}$

(c) $30x^2 \equiv 18 \pmod{24}$

(d) $4(x+1)^2 \equiv 14 \pmod{10}$

(e) $4x^2 - 2x + 2 \equiv 0 \pmod{6}$

(f) $3x^2 - 6x + 6 \equiv 0 \pmod{15}$

Step-by-step solution

Step 1 of 6

(a)

Consider the congruence equation

$6x^2 \equiv 9 \pmod{15}$

Take $x^2 = y$ then $6y \equiv 9 \pmod{15}$

Use the result, the congruence $ax \equiv b \pmod{n}$ has a solution if and only if $\gcd(a,n) \mid b$ to solve the given equation.

The congruence equation $6y \equiv 9 \pmod{15}$ has a solution modulo 15 because

$\gcd(6,15) = 3$ and $3 \mid 9$.

The solution of congruence equation $6y \equiv 9 \pmod{15}$ is same as the solution of

$2y \equiv 3 \pmod{5} \left(\text{since } \frac{6}{3}y \equiv \frac{9}{3}\left(\text{mod } \frac{15}{3}\right)\right)$.

Comment

Step 2 of 6

The congruence equation $2y \equiv 3 \pmod{5}$ is equivalent to $\overline{2}\overline{y} = \overline{3}$ in Z_5.

$\overline{y} = \left(\overline{2}\right)^{-1}\overline{3}$ in Z_5

$\overline{y} = \overline{3}\overline{3}$ in Z_5

$\overline{y} = \overline{4}$ in Z_5

The solution of the congruence equation $6y \equiv 9 \pmod{15}$ is $\boxed{y \equiv 4 \pmod{5}}$.

Therefore, the solution of congruence equation $6x^2 \equiv 9 \pmod{15}$ is same as the solution of

$x^2 \equiv 4 \pmod{5}$

Comment

Step 3 of 6

The congruence equation $x^2 \equiv 4 \pmod{5}$ is equivalent to $\left(\overline{x}\right)^2 = \overline{4}$ in Z_5.

Need to find the values for x in Z_5 such that $\left(\overline{x}\right)^2 = 4$ in Z_5

So the solutions are $\overline{x} = \overline{2}$ and $\overline{x} = \overline{3}$.

Verify that

$$\left(\bar{2}\right)^2 = \left(\bar{2}\right)\left(\bar{2}\right)$$
$$= \bar{4} \text{ in } Z_5$$
$$\left(\bar{3}\right)^2 = \left(\bar{3}\right)\left(\bar{3}\right)$$
$$= \bar{9}$$
$$= \bar{4} \quad \text{in } Z_5$$

Therefore, the solutions of the congruence equation $6x^2 \equiv 9 \pmod{15}$ are

$\boxed{x \equiv 2 \pmod 5 \text{ and } x \equiv 3 \pmod 5}$.

Comment

Step 4 of 6

(b)

Consider the congruence equation

$60x^2 \equiv 18 \pmod{24}$

Take $x^2 = y$ then $60y \equiv 18 \pmod{24}$

Use the result, the congruence $ax \equiv b \pmod n$ has a solution if and only if $\gcd(a,n) \mid b$ to solve the equation.

By the result the congruence equation $60y \equiv 18 \pmod{24}$ has no solution since

$\gcd(60,24) = 12 \text{ and } 12 \nmid 18$.

Therefore, the congruence equation $60x^2 \equiv 18 \pmod{24}$ has the solution.

Hence, the solution is none.

Comment

Step 5 of 6

(c)

Consider the congruence equation

$30x^2 \equiv 18 \pmod{24}$

Take $x^2 = y$ then $30y \equiv 18 \pmod{24}$

Use the result, the congruence $ax \equiv b \pmod n$ has a solution if and only if $\gcd(a,n) \mid b$ to solve the equation.

The congruence equation $30x^2 \equiv 18 \pmod{24}$ has a solution modulo 24 because

$\gcd(30,24) = 6 \text{ and } 6 \mid 18$.

The solution of congruence equation $30y \equiv 18 \pmod{24}$ is same as the solution of

$$5y \equiv 3 \pmod 4 \left(\text{since } \frac{30}{6} y \equiv \frac{18}{6} \left(\bmod \frac{24}{6} \right) \right).$$

Comment

Step 6 of 6

The congruence equation $y \equiv 3 \pmod 4$ is equivalent to $\overline{5}\overline{y} = \overline{3} \text{ in } Z_4$ or $\overline{1}\overline{y} = \overline{3} \text{ in } Z_4$.

$$\overline{y} = \left(\overline{1}\right)^{-1} \overline{3} \text{ in } Z_4$$
$$\overline{y} = \overline{1}\overline{3} \text{ in } Z_4$$
$$\overline{y} = \overline{3} \text{ in } Z_4$$

The solution of the congruence equation $y \equiv 3 \pmod 4$ is $\boxed{y \equiv 3 \pmod 4}$.

The solution of congruence equation $30x^2 \equiv 18 \pmod{24}$ is same as the solution of $x^2 \equiv 3 \pmod 4$

There is no $x \in Z_4 = \{1, 2, 3\}$ such that $\overline{x}^2 \equiv 3 \text{ in } Z_4$

Hence, the quadratic equation $30x^2 \equiv 18 \pmod{24}$ has no solution modulo 24.

Comment