Solving quadratic equations

EG Solve $x^2 \equiv 9 \pmod p$ if $p > 3$ is a prime.

Obvious two solutions: $x \equiv \pm 3 \pmod p$

There are no other solutions because:

$$x^2 - 9 = (x-3)(x+3) \equiv 0 \pmod p$$
$$\iff p \mid (x-3)(x+3)$$
$$\iff p \mid (x-3) \text{ or } p \mid (x+3)$$
$$\iff x - 3 \equiv 0 \text{ or } x + 3 \equiv 0 \pmod p$$
$$\impliedby x \equiv \pm 3 \pmod p$$

[$p = 2, 3$: $\pm 3 \equiv 0 \pmod 3$, $\pm 3 \equiv 1 \pmod 2$ — only 1 instead of 2 solutions]

EG $x^2 \equiv 9 \pmod{35}$, $35 = 5 \cdot 7$

CRT

$$\iff x^2 \equiv 9 \pmod 5 \text{ and } x^2 \equiv 9 \pmod 7$$
$$\impliedby x \equiv \pm 3 \pmod 5 \text{ and } x \equiv \pm 3 \pmod 7$$

	mod 5	mod 7	CRT → mod 35
x	3	3	3
	−3	−3	−3
	3	−3	−17
	−3	3	17

4 solutions: $\pm 3, \pm 17$

$x \equiv 3 \pmod 5$, $x \equiv -3 \pmod 7$

$$\implies x \equiv 3 \cdot 7 \cdot 7^{-1}_{\bmod 5} - 3 \cdot 5 \cdot 5^{-1}_{\bmod 7}$$

$7^{-1}_{\bmod 5} \equiv 2^{-1} \bmod 5 \equiv 3$, $5^{-1}_{\bmod 7} = 3$

$$\equiv 63 - 45 = 18 \equiv -17 \pmod{35}$$