

# 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:

$$x^2 - 9 = (x-3)(x+3) \equiv 0 \pmod{p}$$

$$\Leftrightarrow p \mid (x-3)(x+3)$$

$$\Leftrightarrow p \mid (x-3) \text{ or } p \mid (x+3)$$

$$\Leftrightarrow x-3 \equiv 0 \text{ or } x+3 \equiv 0 \pmod{p}$$

$$\Leftrightarrow x \equiv \pm 3 \pmod{p}$$

$$\left[ p=2,3: \begin{array}{l} \pm 3 \equiv 0 \pmod{3} \\ \pm 3 \equiv 1 \pmod{2} \end{array} \text{ only 1 instead of 2 solutions} \right]$$

EG  $x^2 \equiv 9 \pmod{35}$  5·7

CRT

$$\Leftrightarrow x^2 \equiv 9 \pmod{5} \text{ and } x^2 \equiv 9 \pmod{7}$$

$$\Leftrightarrow x \equiv \pm 3 \pmod{5} \text{ and } x \equiv \pm 3 \pmod{7}$$

	mod 5	mod 7	CRT mod 35
x	3	3	3
	-3	-3	-3
	3	-3	-17
	-3	3	17

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

$$\begin{aligned} &x \equiv 3 \pmod{5} \quad x \equiv -3 \pmod{7} \\ \Rightarrow &x \equiv 3 \cdot 7 \cdot 7^{-1} \pmod{5} - 3 \cdot 5 \cdot 5^{-1} \pmod{7} \\ &\quad \quad \quad 2^{-1} \pmod{5} \equiv 3 \quad \quad \quad 5^{-1} \pmod{7} \equiv 3 \\ &\equiv 63 - 45 = 18 \equiv -17 \pmod{35} \end{aligned}$$