

# Chinese remainder theorem

EG

$$x \equiv 32 \pmod{35}$$

$$x = 32 + 35m = 32 + 5 \cdot 7m$$



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

and

$$x \equiv 4 \pmod{7}$$

Chinese remainder theorem  
(because 5, 7 are prime)

EG

$$x \equiv 2 \pmod{5} \quad x \equiv 4 \pmod{7}$$

Find such x!

$$x \equiv 2 \cdot 7 \cdot 7_{\text{mod } 5}^{-1} + 4 \cdot 5 \cdot 5_{\text{mod } 7}^{-1}$$

$\equiv 2 \pmod{5}$   
 $\equiv 0 \pmod{7}$

$\equiv 2_{\text{mod } 5}^{-1} \equiv 3$   
 $\equiv 3$

$\equiv 0 \pmod{5}$   
 $\equiv 4 \pmod{7}$

$$\equiv 2 \cdot 7 \cdot 3 + 4 \cdot 5 \cdot 3 = 42 + 60 = 102 \equiv 32 \pmod{35}$$

EG

$$x \equiv 1 \pmod{4} \quad x \equiv 2 \pmod{5}$$

$$x = 1 \cdot 5 \cdot 5_{\text{mod } 4}^{-1} + 2 \cdot 4 \cdot 4_{\text{mod } 5}^{-1}$$

$\equiv 1$   
 $\equiv (-1)^{-1} \equiv -1$

$$\equiv 1 \cdot 5 \cdot 1 + 2 \cdot 4 \cdot (-1) = -3 \pmod{20}$$

4 · 5

EG

$$x \equiv 1 \pmod{4} \quad x \equiv 2 \pmod{5} \quad x \equiv 3 \pmod{7}$$

Option 1:  $x \equiv -3 \pmod{20} \quad x \equiv 3 \pmod{7}$   
 proceed as before

Option 2:

$$x = 1 \cdot 5 \cdot 7 \cdot (5 \cdot 7)_{\text{mod } 4}^{-1} + 2 \cdot 4 \cdot 7 \cdot (4 \cdot 7)_{\text{mod } 5}^{-1} + 3 \cdot 4 \cdot 5 \cdot (4 \cdot 5)_{\text{mod } 7}^{-1}$$

$\equiv (-2)_{\text{mod } 4}^{-1} \equiv -1$   
 $\equiv (-2)_{\text{mod } 5}^{-1} \equiv 2$   
 $\equiv (-1)_{\text{mod } 7}^{-1} \equiv -1$

$$\equiv -35 + 112 - 60 = 17 \pmod{140}$$

4 · 5 · 7