

## One more example

$$\text{Solve } x \equiv 9 \pmod{37}, x \equiv 7 \pmod{23}$$

Note Since  $37 \cdot 23 = 851$ , there is exactly one solution  $x$  between 0 and 850.

FIRST Find  $a, b$  so  $37a + 23b = 1$

Euclidean algorithm	Expression as an integral linear combination of 37 & 23
$37 - 23 = 14$	$37 - 23$
$23 - 14 = 9$	$23 - (37 - 23) = 2 \cdot 23 - 37$
$14 - 9 = 5$	$(37 - 23) - (2 \cdot 23 - 37) = 2 \cdot 37 - 3 \cdot 23$
$9 - 5 = 4$	$(2 \cdot 23 - 37) - (2 \cdot 37 - 3 \cdot 23) = 5 \cdot 23 - 3 \cdot 37$
$5 - 4 = 1$	$(2 \cdot 37 - 3 \cdot 23) - (5 \cdot 23 - 3 \cdot 37) = 5 \cdot 37 - 8 \cdot 23$

Bottom line  $5 \cdot 37 \equiv 1 \pmod{23}$   
 $(-8) \cdot 23 \equiv 1 \pmod{37}$

DO ALGEBRA NOW. Write  $x = 23k + 7$

Want  $23k + 7 \equiv 9 \pmod{37}$ , or  $23k \equiv 2 \pmod{37}$

Apply  $(-8) \cdot 23 \equiv 1 \pmod{37}$ . Get  $k \equiv -16 \pmod{37}$   
or  $21 \equiv -16$

Hence  $k = 37m + 21$ , so  $x = 23(37m + 21) + 7$   
which simplifies to ~~851m + 490~~.  $490 + 851m$ .

Check

$$\left. \begin{aligned} 490 &= 13 \cdot 37 + 9 \\ 490 &= 23 \cdot 21 + 7 \end{aligned} \right\}$$