Dans une équation de type $ax \equiv b \mod c$

1) Si a n'est pas premier avec c :

→ Si le pgcd(a, c) ne divise pas b, alors il n'y a pas de solution

→ Si le pgcd(a, c) divise b, alors l'équation est équivalente à :

$$a'x \equiv b' \mod c'$$

où $a = \text{pgcd}(a,b) \times a'$

$b = \text{pgcd}(a,b) \times b'$

Dans ce cas, a' est alors premier avec c'

2) Si a est premier avec c, on cherche d'abord à inverser a modulo c.
Pour se ramener à un équation de type

$$x \equiv d \mod c$$

3) On exprime sous la forme

$$S = \{ck + d \mid k \in \mathbb{Z}\}$$

$2x \equiv 1 \mod 7$

$ax \equiv b \mod c$

$pgcd(2,7) = 1$ On remarque 2 et 7 sont premier entre eux

$7 = 3 \times 2 + 1$

$2 = 2 \times 1 + 0$

On constate que $1 \mid 1$ donc cet équation admet des solutions

x est l'inverse de 2 mod 7 si

$2x \equiv 1 [7]$

On cherche l'inverse de 2 mod 7, on a :

$x [7]$	0	1	2	3	4
$2x [7]$	0	2	4	6	8

$2x \equiv 1 \mod 7$

$\Leftrightarrow 4 \times 2x \equiv 1 \times 4 \mod 7$

$\Leftrightarrow x \equiv 4 \mod 7$

b) $4x \equiv 6 \mod 18$

$pgcd(4,18) = 2$

l'équation est équivalente à

$2x \equiv 3 \mod 9$

On cherche l'inverse de 2 mod 9. On a

$2 \times 5 \equiv 1 \mod 9$

Donc :

$$2x \equiv 3 \mod 9$$
$$\Leftrightarrow 5 \times 2x \equiv 5 \times 3 \mod 9$$
$$\Leftrightarrow x \equiv 15 \mod 9$$
$$\Leftrightarrow x \equiv 6 \mod 9$$

$$S = \{ 9k + 6 \mid k \in \mathbb{Z} \}$$

d) $23x \equiv 41 \mod 52$

$\mathrm{pgcd}(23, 52) = 1$

$$52 = 2 \times 23 + 6$$
$$23 = 3 \times 6 + 5$$
$$6 = 1 \times 5 + 1$$
$$5 = 5 \times 1 + 0$$

$$1 = 6 - 1 \times 5$$
$$1 = 6 - 1(23 - 3 \times 6)$$
$$1 = 6 - 1 \times 23 + 3 \times 6$$
$$1 = -1 \times 23 + 4 \times 6$$
$$1 = -1 \times 23 + 4(52 - 2 \times 23)$$
$$1 = -1 \times 23 + 4 \times 52 - 8 \times 23$$
$$1 = 4 \times 52 - 9 \times 23$$

Donc $23 \times (-9) \equiv 1 \mod 52$

Donc $23x \equiv 41 \mod 52$
$$\Leftrightarrow (-9) \times 23x \equiv 41 \times (-9) \mod 52$$
$$\Leftrightarrow x \equiv -369 \mod 52$$