Exercici 16. Calculeu totes les solucions de les congruències següents:

(a) $30X \equiv 3 \pmod 7$,

(b) $15X \equiv 5 \pmod{26}$,

(c) $1224X \equiv 31 \pmod{335}$,

(d) $1984X \equiv 666 \pmod{2001}$,

(e) $154X \equiv 112 \pmod{280}$,

(f) $525X \equiv 735 \pmod{1000}$,

(g) $55X \equiv 77 \pmod{121}$,

(h) $68X \equiv 153 \pmod{170}$,

(i) $45X \equiv 105 \pmod{120}$,

(j) $45X \equiv 105 \pmod{100}$,

Solució 16. Per resoldre aquest exercici faré ús del següent mètode:
Sigui $aX \equiv b$ (mod m). Aquesta congruència té solució$\Leftrightarrow$mcd(a, m) | b. Suposem que és cert. Hem de reduir a i b a (mod m):

$$a \equiv a^{'} \text{ (mod m)}$$
$$b \equiv b^{'} \text{ (mod m)}$$

Ara ens queda la congruència de la següent forma:

$$a^{'}\ X \equiv b^{'} \text{ (mod m)}$$

(1) Si $a^{'} = 1$, ja hem acabat, ja que tenim el resultat $X \equiv b^{'}$ (mod m).

(2) Si no, busquem l'invers de $a^{'} \in (\dfrac{\mathbb{Z}}{m\mathbb{Z}})^{*}$, al qual anomenarem a^{*}. Ara multipliquem a banda i banda de la congruència i obtenim:

$$X(a^{'} \cdot a^{*} \equiv b^{'} \cdot a^{*} \text{ (mod m)}.$$

Ara bé,

$$a^{'} \cdot a^{*} \equiv 1 \text{ (mod m} \Rightarrow \text{tenim queX} \equiv b^{'} \cdot a^{*} \equiv c \text{ (mod m)}.$$

(a) $30X \equiv 3 \pmod 7$,

$$mcd(30, 7) = 1|3 \Rightarrow \exists \text{ solució}$$
$$30 \equiv 2 \pmod 7$$
$$2X \equiv 3 \pmod 7$$
$$4 = 2^{-1} \in (\frac{\mathbb{Z}}{7\mathbb{Z}})^{*} \Rightarrow X \equiv 4 \cdot 3 \equiv 5 \pmod 7$$

(b) $15X \equiv 5 \pmod{26}$,

$$mcd(15, 26) = 1|5 \Rightarrow \exists \text{ solució}$$
$$7 = 15^{-1} \in (\frac{\mathbb{Z}}{26\mathbb{Z}})^* \Rightarrow X \equiv 5 \cdot 7 \equiv 9 \pmod{26}$$

(c) $1224X \equiv 31 \pmod{335}$,

$$mcd(1224, 335) = 1|31 \Rightarrow \exists \text{ solució}$$
$$1224 \equiv 219 \pmod{335}$$
$$219X \equiv 31 \ (\text{mod} 335)$$
$$309 = 219^{-1} \in (\frac{\mathbb{Z}}{335\mathbb{Z}})^* \Rightarrow X \equiv 219 \cdot 309 \equiv 119 \pmod{335}$$

(d) $1984X \equiv 666 \pmod{2001}$,

$$mcd(1984, 2001) = 1|666 \Rightarrow \exists \text{ solució}$$

Per Bézout tenim que $1984\lambda + 2001\mu = 1$. Si resolem la equació diofantina, trobem que $\lambda = -824$. Aií doncs, tenim que:

$$-824 = 1984^{-1} \in (\frac{\mathbb{Z}}{2001\mathbb{Z}})^* \Rightarrow X \equiv (-824) \cdot 666 \equiv 1491 \pmod{2001}$$

(e) $154X \equiv 112 \pmod{280}$,

$$mcd(154, 280) = 14|112 \Rightarrow \exists \text{ solució}$$

Dividim tota la congruència per $14 \Rightarrow 11X \equiv 8 \pmod{20}$

$$11 = 11^{-1} \in (\frac{\mathbb{Z}}{20\mathbb{Z}})^* \Rightarrow X \equiv 11 \cdot 8 \equiv 8 \pmod{20}$$

(f) $525X \equiv 735 \pmod{1000}$. No té solucions, ja que $mcd(525, 1000) = 25 \nmid 735$.

(g) $55X \equiv 77 \pmod{121}$,

$$mcd(55, 121) = 11|77 \Rightarrow \exists \text{ solució}$$

Dividim tota la congruència per $11 \Rightarrow 5X \equiv 7 \pmod{11}$

$$5 = 5^{-1} \in (\frac{\mathbb{Z}}{11\mathbb{Z}})^* \Rightarrow X \equiv 5 \cdot 7 \equiv 2 \pmod{11}$$

(h) $68X \equiv 153 \pmod{170}$. No té solucions, ja que $mcd(68, 153) = 34 \nmid 153$.

(i) $45X \equiv 105 \pmod{120}$,

$$mcd(45, 120) = 15|105 \Rightarrow \exists \text{ solució}$$

Dividim tota la congruència per $15 \Rightarrow 3X \equiv 7 \pmod{8}$

$$3 = 3^{-1} \in (\frac{\mathbb{Z}}{8\mathbb{Z}})^* \Rightarrow X \equiv 3 \cdot 7 \equiv 5 \pmod 8$$

(j) $45X \equiv 105 \pmod{100}$,

$$mcd(45, 100) = 5|105 \Rightarrow \exists \text{ solució}$$

Dividim tota la congruència per 5 $\Rightarrow 9X \equiv 21 \pmod{50}$

$$9 = 9^{-1} \in (\frac{\mathbb{Z}}{50\mathbb{Z}})^* \Rightarrow X \equiv 39 \cdot 21 \equiv 19 \pmod{50}$$