4.1

$$210 = 2.3.5.7$$

$$48 = 2^4.3$$

Donc $d = pgcd(210, 48) = 6$.

Pour résoudre

$$210u + 48v = 6,\ u, v \in \mathbb{Z}$$

On cherche d'abord une solution particulière (a) puis on cherchera toutes les solutions (b).

$$210u + 48v = 6 \Leftrightarrow 35u + 8v = 1\ .$$

a)

$$35 = 8.4 + 3$$

$$8 = 3.2 + 2$$

$$3 = 2 + 1$$

Donc

$$1 = 3 - 2 = 3 - (8 - 3.2) = 3.3 - 8 = (35 - 8.4).3 - 8 = 35.3 - 8.13\ .$$

b)

$$35u + 8v = 1 \Leftrightarrow 35u + 8v = 35.3 - 8.13$$

$$35(u - 3) + 8(v + 13) = 0 \Leftrightarrow 35(u - 3) = -8(v + 13)\ (*)$$

$$\Rightarrow 35|8(v + 13) \Rightarrow 35|v + 13$$

d'après le lemme de Gauss (car $35 \wedge 8 = 1$). De même, $8|u - 3$.

Donc $v + 13 = 35k$ et $u - 3 = 8l$, $k, l \in \mathbb{Z}$.

On reporte dans $(*)$:

$$(*) \Leftrightarrow 35.8l = -8.35k \Leftrightarrow l = -k\ .$$

Conclusion, $210u + 48v = 6 \Leftrightarrow u = 3 - 8k$, $v = -13 + 35k$, $k \in \mathbb{Z}$.

4.5

(ii)

$$\begin{cases} x &= 3[17] \\ x &= 4[11] \\ x &= 5[6] \end{cases} \Leftrightarrow x = 3 + 17k,\ k \in \mathbb{Z},\ 3 + 17k = 4[11],\ 3 + 17k = 5[6]\ .$$

Or $3 + 17k = 4[11] \Leftrightarrow 6k = 1[11] \Leftrightarrow k = 2[11]$ (en multipliant par 2 mod 11).

Donc

$$x = 3 + 17(2 + 11l) = 5[6],\ l \in \mathbb{Z} \Leftrightarrow 34 + 187l = 2[6] \Leftrightarrow l = -2[6]$$

d'où,

$$x = 3 + 17(2 + 11(-2 + 6n)),\ n \in \mathbb{Z} \Leftrightarrow x = 37 - 374 + 1122n,\ n \in \mathbb{Z}$$

$$\Leftrightarrow x = -337 + 1122n\, n \in \mathbb{Z}\ .$$

(iii)

$$(*)\begin{cases} 4x &= 6[14] \\ 3x &= 1[5] \\ 5x &= 11[3] \end{cases}$$

$$4x = 6[14] \Leftrightarrow 2x = 3[7] \Leftrightarrow x = -9[7] = -2[7] \ .$$

On remplace dans la deuxième équation x par $-2 + 7k$, $k \in \mathbb{Z}$.

$$3x = 1 \bmod 5 \Leftrightarrow 3(-2 + 7k) = 1 \bmod 5 \Leftrightarrow 21k = 7 \bmod 5 \Leftrightarrow k = 2 \bmod 5 \ .$$

On remplace donc dans la dernière équation x par $-2 + 7(2 + 5l) = 12 + 35l$, $l \in \mathbb{Z}$. Donc $5x = 11[3] \Leftrightarrow 5(12 + 35l) = 11[3] \Leftrightarrow 175l = 11[3] \Leftrightarrow l = 2[3]$.
Donc $(*) \Leftrightarrow x = 12 + 35(2 + 3n) = 82 + 105n$, $n \in \mathbb{Z}$.

5.1 petit théorème de Fermat

1) Pour tout $a \in \mathbb{Z}$, soit $\phi_a : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $n \bmod p \mapsto an \bmod p$.
On a $\forall\, a, b \in \mathbb{Z}$, $\circ\phi_b = \phi_{ab}$.
Si p est premier et si p ne divise pas a, alors $p \wedge a = 1$. Donc il existe $b, c \in \mathbb{Z}$ tels que

$$ab + pc = 1$$

$$\Rightarrow ab = 1 \bmod p$$

Donc $\phi_a \circ \phi_b = \phi_b \circ \phi_a = \phi_{ab} = \phi_1 = \mathrm{Id}_{\mathbb{Z}/p\mathbb{Z}}$.
Donc ϕ_a est bijective de réciproqie $\phi_a^{-1} = \phi_b$.

2) Comme $\phi_a : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ est une bijection et comme $\phi_a(\overline{0}) = \overline{0}$, ϕ_a est une bijection de l'ensemble

$$\{\overline{1}, \overline{2}, ..., \overline{p-1}\}$$

dans lui-même.
Donc

$$\phi_a(\overline{1})...\phi_a(\overline{p-1}) = \overline{1}...\overline{p-1}$$

(c'est le produit de la même liste d'éléments, seul l'ordre change !) Or, on a :

$$\phi_a(\overline{1})...\phi_a(\overline{p-1}) = \overline{1}...\overline{p-1} = \overline{a}\overline{1}\overline{a}\overline{2}...\overline{a}\overline{p-1}$$

$$= \overline{a}^{p-1}\overline{1}...\overline{p-1} \ .$$

Donc

$$\overline{a}^{p-1}\overline{1}...\overline{p-1} = \overline{1}...\overline{p-1} \ .$$

On peut simplfier par $\overline{p-1}$, ..., $\overline{1}$ qui sont inversibles dans $\mathbb{Z}/pZ$ car $1, ..., p-1$ sont premiers à p.
Donc $\overline{a}^{p-1} = \overline{1} \Leftrightarrow a^{p-1} = 1 \bmod p$.

5.2 théorème de Wilson

1) D'après le petit théorème de Fermat, $\forall\, 1 \leqslant i \leqslant p-1$, $\overline{i}^{p-1} - \overline{1} = 0$. Donc

$$(X - \overline{1})...(X - \overline{p-1}) | X^{p-1} - \overline{1}$$

dans $\mathbb{Z}/p\mathbb{Z}[X]$. Or, ces deux polynômes sont unitaires et de meme degré. Donc

$$(X - \overline{1})...(X - \overline{p-1}) | X^{p-1} - \overline{1} \ .$$

2) Si on compare les termes constants, on trouve :

$$(-\overline{1})...(-\overline{p-1}) = -\overline{1}$$

$$\Leftrightarrow (p-1)! = -1 \bmod p$$

si p est un nombre premier impair. C'est encore vrai si $p = 2$.

3) Si $n \geqslant 2$ n'est pas premier, il existe $2 \leqslant a \leqslant n-1$ tel que $a|n$.
Alors $2 \leqslant a \leqslant n-1 \Rightarrow a|(n-1)!$. Si $(n-1)! = -1 \bmod n$, alors $n|(n-1)!+1 \Rightarrow a|(n-1)!+1$.
Mais alors $a|(n-1)! + 1 - (n-1)! = 1$ *absurde !*

5.3

Si n est un entier non divisible par 11, alors $11|n^{10} - 1$ d'après le petit théorème de Fermat. Si $11|n$, alors $n = 0 \bmod 11 \Rightarrow n^{10} - 1 = -1 \bmod 11$ n'est pas divisible par 11.

Si n est un entier non divisible par 13, alors $13|n^{12} - 1 = (n^6 - 1)(n^6 + 1)$ d'après le petit théorème de Fermat. Comme 13 est premier, $13|(n^6 - 1)(n^6 + 1) \Rightarrow 13|n^6 - 1$ ou $13|n^6 + 1$. Si $13|n$, alors $n = 0 \bmod 13 \Rightarrow (n^6 - 1)(n^6 + 1) = n^{12} - 1 = -1 \bmod 13$ donc $n^6 - 1 \neq 0 \bmod 13$ et $n^6 + 1 \neq 0 \bmod 13$.

5.4 D'après le petit théorème de Fermat, $2^{12} = 1 \bmod 13$.
Or $1137 = 12.94 + 9$. Donc

$$2^{1137} = 2^{12.94+9} = (2^{12})^{94}.2^9 = 2^9 \bmod 13$$

$$= (2^3)^3 \bmod 13 = (-5)^3 \bmod 13 = -5.25 \bmod 13 = -5.12 \bmod 13 = (-5)(-1) = 5 \bmod 13 \ .$$

Comme $0 \leqslant 5 < 13$, 5 est le reste de la division euclidienne de 2^{1137} par 13.
De même, $2^{16} = 1 \bmod 17$.

$$1137 = 16.71 + 1 \Rightarrow 2^{1137} = (2^{16})^{71}.2 = 2 \bmod 17 \ .$$

Comme $0 \leqslant 2 < 17$, 2 est le reste de la division euclidienne de 2^{1137} par 17.
Posons $x = 2^{1137}$. On a

$$x = 5 \bmod 13 \text{ et } x = 2 \bmod 17 \ .$$

On pose $x = 5 + 13k$, $k \in \mathbb{Z}$. Donc $x = 2 \bmod 17 \Leftrightarrow 5 + 13k = 2 \bmod 17$

$$\Leftrightarrow -4k = -3 \bmod 17$$

on muliplie par $4 \bmod 17$

$$\Leftrightarrow k = -12 \bmod 17$$

$$\Leftrightarrow k = 5 \bmod 17 \ .$$

Par conséquent, $x = 2^{1137} = 5 + 13(5 + 17l) = 70 + 221l$, $l \in \mathbb{Z}$. En particulier, $2^{1137} = 70 \bmod 221$. Comme $0 \leqslant 70 < 221$, 70 est le reste de la division euclidienne de 2^{1137} par 221.