III. Congruences et équations modulo n

a. Spécificité des équations modulo n

Solution générale

$x \equiv a\ [n]$ Cela veut dire que x s'écrit sous la forme $\boldsymbol{x = a + kn}$ avec $k \in \mathbb{Z}$
Il y a une solution pour chaque valeur de k, donc une **infinité de solutions**
On note l'ensemble de toutes les solutions : $\boldsymbol{S = \{a + kn, k \in \mathbb{Z}\}}$

Exemple : $x \equiv 2\ [6]$ Les solutions sont de la forme : $x = 2 + 6k$ *on a* $\boldsymbol{S = \{2 + 6k, k \in \mathbb{Z}\}}$

Solutions particulières

$\begin{cases} x \equiv a\ [n] \\ m \leq x \leq p \end{cases}$ Parmi toutes les solutions de la forme $\boldsymbol{x = a + kn}$, on ne prend que celles qui appartiennent à l'intervalle des entiers $[m; p]$

Exemple : $\begin{cases} x \equiv 5\ [8] \\ -10 \leq x \leq 20 \end{cases}$ Les solutions sont de la forme : $x = 5 + 8k.$ Dans $[-10; 20]$ on a $\boldsymbol{S = \{-3; 5; 13\}}$

Simplifier une équation au modulo n

• On peut additionner ou multiplier une équation modulo n :

si $\boldsymbol{a \equiv b\ [n]}$ **alors** $\boldsymbol{a + c \equiv b + c\ [n]}$ **ou** $\boldsymbol{ac \equiv bc\ [n]}$

• On peut remplacer chaque terme par un nombre qui lui est congru :

si $\begin{cases} \boldsymbol{a \equiv r\ [n]} \\ \boldsymbol{b \equiv p\ [n]} \\ \boldsymbol{a \equiv b\ [n]} \end{cases}$ **alors** $\boldsymbol{r \equiv p\ [n]}$

Exemple : $54x \equiv 27\ [5] \Rightarrow \begin{cases} 54 \equiv 4\ [5] \\ 27 \equiv 2\ [5] \\ 54x \equiv 27\ [5] \end{cases}$ donc $\boldsymbol{4x \equiv 2\ [5]}$

b. Résoudre des équations modulo n

Résolution directe (sommes)

Exemple : $x - 12 \equiv 24\ [7] \Rightarrow x \equiv 36\ [7] \Rightarrow \boldsymbol{x \equiv 1\ [7]}$ **Les solutions sont de la forme** $\boldsymbol{1 + 7k,\ k \in \mathbb{Z}}$

Résolution à l'aide d'un tableau de reste

On cherche à résoudre $f(x) \equiv r[n]$. On fait le tableau de reste de l'expression $f(x)$ modulo n et on regarde quels nombres correspondent.

Remarque : Pour être rigoureux.euse, il s'agit d'implications (on perd de l'information). Pour être sûr.e que les nombres de la forme trouvée sont bien solutions, il faut les tester.

Exemple : • $11x \equiv 1\ [7]$ On fait le tableau de restes de $11x$:

$x \equiv \cdots [7]$	0	1	2	3	4	5	6
$11x$	0	11	22	33	44	55	66
$11x \equiv \cdots [7]$	0	4	1	5	2	6	3

$\Rightarrow$ $\boldsymbol{x \equiv 2\ [7]}$ **Les solutions sont de la forme** $\boldsymbol{2 + 7k,\ k \in \mathbb{Z}}$

(Test : $\boldsymbol{11 \times (2 + 7k) = 22 + 77k}$ **et** $\begin{cases} \boldsymbol{22 \equiv 1\ [7]} \\ \boldsymbol{77 \equiv 0\ [7]} \end{cases}$ **donc** $\boldsymbol{11 \times (2 + 7) \equiv 1\ [7]}$ c'est bon)

• $9x^2 - 25 \equiv 1\ [3]$ On fait le tableau de restes de $2x^2 - 25$:

$x \equiv \cdots [3]$	0	1	2
$9x^2 - 25$	-25	-16	11
$9x^2 - 25 \equiv \cdots [3]$	2	2	2

D'après le tableau de reste, il n'y a pas de solution $\Rightarrow S = \emptyset$

Résolution à l'aide d'un inverse modulo n (produit)

On cherche à résoudre $ax \equiv b\ [n]$. On cherche un entier k tel que $ak \equiv 1\ [n]$. On multiplie toute l'équation par k, puis on la « passe » au modulo n

Exemple : • $11x \equiv 1\ [7]$ Cette fois, on cherche k tel que $11k \equiv 1\ [7]$.
On cherche dans la liste des multiples de 11 celui qui est de la forme $1 + 7n$
(un multiple de 7 +1) : C'est $22 = 21 + 1$. On va donc multiplier l'équation par 2
$11x \equiv 1\ [7] \overset{\times 2}{\Rightarrow} 22x \equiv 2\ [7]$
et comme $22 \equiv 1\ [7]$ (c'est comme ça qu'on l'a voulu), on a $\mathbf{1}x \equiv \mathbf{2}\ [\mathbf{7}]$

Table de 11	Table de 7
11	7
22	14
33	21
44	28
55	35

c. Équations à 2 inconnues modulo n

Exprimer une inconnue en fonction de l'autre

On a $ax + by \equiv c\ [n]$.

• Si on veut exprimer y en fonction de x, on cherche un entier k tel que $bk \equiv 1\ [n]$. On multiplie toute l'équation par k, puis on isole y

• Si on veut exprimer x en fonction de y, on cherche un entier p tel que $ap \equiv 1\ [n]$…

Exemple : • $5x - 3y \equiv 11\ [4]$ On veut exprimer x en fonction de y : on cherche k tel que $5k \equiv 1\ [4]$.
Pour $k = 5$ on a $25 \equiv 1\ [4]$ donc $5x - 3y \equiv 11\ [4] \overset{\times 5}{\Rightarrow} 25x - 15y \equiv 55\ [4]$
On a $\begin{cases} 25 \equiv 1\ [4] \\ -15 \equiv 1\ [4] \\ 55 \equiv 3\ [4] \end{cases}$ donc $x + y \equiv 3\ [4] \Leftrightarrow \mathbf{x \equiv 3 - y\ [4]}$

Résoudre un système d'équations modulo n

• On utilise les mêmes méthodes que pour résoudre un système classique, soit en exprimant une inconnue en fonction de l'autre et en la remplaçant dans la 2ème équation, soit en fonctionnant par combinaison pour faire « disparaître » une des inconnues.

• Dans les 2 méthodes, quand on en arrive à $ax \equiv b\ [n]$, on utilise un tableau de reste ou on trouve l'entier k tel que $ak \equiv 1\ [n]$

Exemple : On veut résoudre $\begin{cases} 2x - 3y \equiv 3\ [5] \\ x + 4y \equiv 2\ [5] \end{cases}$

Méthode 1 : Substitution : $\begin{cases} 2(2 - 4y) - 3y \equiv 3\ [5] \\ x \equiv 2 - 4y\ [5] \end{cases} \Rightarrow \begin{cases} 4 - 8y - 3y \equiv 3\ [5] \\ x \equiv 2 - 4y\ [5] \end{cases} \Rightarrow \begin{cases} -11y \equiv -1\ [5] \\ x \equiv 2 - 4y\ [5] \end{cases} \Rightarrow$
$\begin{cases} 4y \equiv 4\ [5] \\ x \equiv 2 - 4y\ [5] \end{cases} \Rightarrow \overset{\times 4}{} \begin{cases} 16y \equiv 16\ [5] \\ x \equiv 2 - 4y\ [5] \end{cases} \Rightarrow \begin{cases} y \equiv 1\ [5] \\ x \equiv 2 - 4\ [5] \end{cases} \Rightarrow \begin{cases} y \equiv 1\ [5] \\ x \equiv 3\ [5] \end{cases}$
Les solutions sont de la forme $\boldsymbol{S = \{(3 + 5k; 1 + 5p), k \in \mathbb{Z}, p \in \mathbb{Z}\}}$

Méthode 2 : Combinaison
$\begin{cases} 2x - 3y \equiv 3\ [5] \\ x + 4y \equiv 2\ [5] \end{cases} \Rightarrow \overset{\times -2}{} \begin{cases} 2x - 3y \equiv 3\ [5] \\ -2x - 8y \equiv -4\ [5] \end{cases} \Rightarrow -11y \equiv -1\ [5] \Leftrightarrow 4y \equiv 4\ [5] \overset{\times 4}{\Rightarrow} 16y \equiv 16\ [5] \Rightarrow \mathbf{y \equiv 1\ [5]}$
$\begin{cases} 2x - 3y \equiv 3\ [5] \\ x + 4y \equiv 2\ [5] \end{cases} \Rightarrow \begin{matrix} \times 4 \\ \times 3 \end{matrix} \begin{cases} 8x - 12y \equiv 12\ [5] \\ 3x + 12y \equiv 6\ [5] \end{cases} \Rightarrow 11x \equiv 18\ [5] \Rightarrow \mathbf{x \equiv 3\ [5]}$