Université de Versailles – Saint-Quentin-en-Yvelines
Université Paris Saclay

le _ _ / _ _ / 2024
Groupe de TD __

Master 1 Informatique 2024–2025
Compléments de maths

NOM : _____	Prénom : _____	Num. Étu. : 2☐☐☐☐☐☐☐☐

Questions :

1. On appelle ordre d'un élément a d'un groupe $(G, *)$ le plus petit entier $n \geq 1$ tel que $a^n = e$. On rappelle aussi le théorème de Lagrange : "tout sous-groupe a un ordre qui divise l'ordre du groupe". Sachant de plus que pour tout $a \in G$, $\{a^i, i \in \mathbb{N}\}$ est un sous-groupe, donner tous les ordres possibles pour les éléments dans $(\mathbb{Z}/140\mathbb{Z}, +)$.
2. Donner deux systèmes d'équations de congruence avec des modulos compris entre 6 et 13, avec au moins deux équations chacun, l'un n'ayant aucune solution et l'autre ayant une solution. Justifier pourquoi le premier n'a pas de solution et résoudre entièrement le deuxième.

Réponse :

Soit $a \in G$. On note $A = \{a^i, i \in \mathbb{N}\}$. Soit maintenant $n \in \mathbb{N}$ le plus petit entier non nul tel que $a^n = e = a^0$. On montre d'abord que pour tout $i, j < n$ et différents, $a^i \neq a^j$. En effet sans perdre de généralités, on peut supposer $i < j$. Ainsi $a^i = a^j$ est équivalent à $a^{j-i} = e$. Comme $j - i$ est nécessairement inférieur à n. on en déduit que nécessairement $j = i$. Par conséquent on a toujours $a^i \neq a^j$ quand $i < j < n$. Donc on en déduit que le cardinal de l'ensemble A est n : tous les éléments $e, a, a^2, \ldots, a^{n-1}$ sont différents, puis a^k pour $k \geq n$ est dans cet ensemble (d'ailleurs c'est un groupe cyclique). Ainsi, $A = \{e, a, a^2, \ldots, a^{n-1}\}$. D'après l'énoncé c'est un sous-groupe, il est de taille n qui est l'ordre de a et encore d'après l'énoncé tout ordre de sous-groupe divise l'ordre du groupe, donc l'ordre de chaque élément d'un groupe divise l'ordre du groupe.

On applique donc maintenant cela à $\mathbb{Z}/140\mathbb{Z}$ muni de l'addition. Ce groupe est d'ordre 140, donc tous les ordres possibles pour les éléments de ce groupe sont les diviseurs de 140. Comme $140 = 14 \times 10 = 2^2 \times 5 \times 7$, les diviseurs de 140 sont tous les $2^i \times 5^j \times 7^k$ pour $i = 0, 1, 2$, $j = 0, 1$ et $k = 0, 1$, il y en a donc $3 \times 2 \times 2 = 12$ et ce sont : $1, 2, 4, 5, 7, 10, 14, 20, 28, 35, 70, 140$.

Pour la deuxième question, il suffit de donner, pour ne pas avoir de solution des équations qui sont incompatibles, donc il faut au moins des modulos non premiers entre eux, et faire attention à la valeur à satisfaire. On peut par exemple choisir

$$\begin{cases} x = 3 & \mod 9 \\ x = 2 & \mod 6 \end{cases}$$

Le PGCD de 9 et 6 est 3, donc pour justifier que cette équation n'a pas de solution, il faut regarder les équations modulo 3. Ici cela donne $0 \mod 3$ en haut et $2 \mod 3$ en bas, ce qui est donc incompatible.

Pour un système qui se résout facilement, on peut prendre des modulos premiers entre eux et cela permet de s'assurer qu'il y aura toujours une solution, par contre on peut vouloir se simplifier les calculs en prenant un système vraiment facile à résoudre. Par exemple

$$\begin{cases} x = 2 & \mod 9 \\ x = 2 & \mod 6 \end{cases}$$

On remarque que $x = 2 \mod 6$ est équivalent au système

$$\begin{cases} x = 2 & \mod 3 \\ x = 0 & \mod 2 \end{cases}$$

La première équation est nécessairement satisfaite par l'équation $x = 2 \mod 9$ et la deuxième signifie que x est pair. Par conséquent le système initial est équivalent à

$$\begin{cases} x = 2 & \mod 9 \\ x = 0 & \mod 2 \end{cases}$$

La solution est unique modulo 18 et on constate que $2 \mod 18$ convient.