Université de Versailles – Saint-Quentin-en-Yvelines
Université Paris Saclay le 26 / 09 / 2023

Master 1 Informatique 2023–2024
Compléments de maths

Corrigé CC3 - TD3

Questions :

1. Donner les éléments inversibles pour la multiplication dans $\mathbb{Z}/8\mathbb{Z}$
2. Résoudre le système d'équations suivant dans l'ensemble des entiers ($\mathbb{Z}$). Donner toutes les solutions possibles s'il y en a.

$$\begin{cases} x = 7 & \mod 9 \\ x = 9 & \mod 17 \end{cases}$$

1.

D'après le cours, les éléments inversibles pour la multiplication dans $\mathbb{Z}/8\mathbb{Z}$ sont les (classes des) éléments $a \in \{0, \cdots, 7\}$ qui vérifient $\mathrm{pgcd}(a, 8) = 1$, autrement dit les éléments premiers avec 8.

8 est premier avec 1, 3, 5, 7 mais pas avec 2, 4, 6 (qui partagent avec 8 au moins le diviseur 2) et ni avec 0 (avec qui 8 partage 8 comme diviseur). Les inversibles pour la multiplication dans $\mathbb{Z}/8\mathbb{Z}$ sont donc 1, 3, 5, 7.

2.

On observe tout d'abord que 9 et 17 sont premiers entre eux (car 17 est un nombre premier et 17 ne divise pas 9). Ainsi, d'après le théorème des restes chinois, le système admet une infinité de solution entière (mais une unique solution modulo $9 \times 17 = 153$). Cherchons donc une solution entière particulière $x_0 \in \mathbb{Z}$, l'ensemble S des solutions sera alors de la forme :

$$S = \{x_0 + 153k, k \in \mathbb{Z}\}.$$

Commençons par trouver un couple $(u, v) \in \mathbb{Z}^2$ vérifiant $17u + 9v = 1$ grâce à l'algorithme d'Euclide étendu.

$$\begin{aligned} 17 &= 17 \times 1 + 9 \times 0 & \\ 9 &= 17 \times 0 + 9 \times 1 & \\ 8 &= 17 \times 1 + 9 \times (-1) & L_3 = L_1 - L_2 \\ 1 &= 17 \times (-1) + 9 \times 2 & L_4 = L_2 - L_3 \end{aligned}$$

Ainsi $(u, v) = (-1, 2)$ convient.

> **Remarque.** Si une solution particulière nous "saute rapidement aux yeux", on peut tout à fait éviter l'utilisation de l'algorithme d'Euclide étendu (AEE) et l'introduire directement. l'AEE reste néanmoins la méthode qui fonctionne **toujours**, contrairement aux solutions "évidentes".

Ainsi $17u + 9v = 1$. En réduisant cette égalité modulo 17, on déduit que $9v \equiv 1 \mod 17$ et en la réduisant modulo 9, on déduit que $17u \equiv 1 \mod 9$. En notant que $17u = -17$ et $9v = 18$, on a donc :

$$\begin{cases} -17 \equiv 1 & \mod 9 \\ -17 \equiv 0 & \mod 17 \end{cases} \quad \text{et} \quad \begin{cases} 18 \equiv 0 & \mod 9 \\ 18 \equiv 1 & \mod 17 \end{cases}$$

Ainsi, en multipliant -17 par 7 et -18 par 9, on obtient :

$$\begin{cases} 7 \times -17 \equiv 7 \times 1 \equiv 7 & \mod 9 \\ 7 \times -17 \equiv 7 \times 0 \equiv 0 & \mod 17 \end{cases} \quad \text{et} \quad \begin{cases} 9 \times 18 \equiv 9 \times 0 \equiv 0 & \mod 9 \\ 9 \times 18 \equiv 9 \times 1 \equiv 9 & \mod 17 \end{cases}$$

Enfin en additionnant les équations ci-dessus, on obtient alors :

$$\begin{cases} 7 \times (-17) + 9 \times 18 \equiv 7 + 0 \equiv 7 & \mod 9 \\ 7 \times (-17) + 9 \times 18 \equiv 0 + 9 \equiv 9 & \mod 17 \end{cases}.$$

Ainsi $7 \times (-17) + 9 \times 18 = -119 + 162 = 43$ est une solution du système.

On en déduit finalement $S = \{43 + 153k, k \in \mathbb{Z}\}$ (ou de manière équivalente 43 est l'unique solution modulo 153).