

## TD 5

### CONGRUENCES LINÉAIRES ET THÉORÈME DES RESTES CHINOIS

**Exercice 1.** Soient  $n \geq 1$  et  $a$  deux entiers, et  $d = \text{pgcd}(a, n)$ .

a) Montrer que si  $d = 1$ , alors pour tout  $z, z' \in \mathbb{Z}$ ,

$$az \equiv az' \pmod{n} \iff z \equiv z' \pmod{n}.$$

b) Montrer que, pour tout  $z, z' \in \mathbb{Z}$ ,

$$az \equiv az' \pmod{n} \iff z \equiv z' \pmod{n/d}.$$

c) On suppose que la congruence  $az \equiv b \pmod{n}$  admet une solution  $z_0$ . Montrer que ses solutions sont exactement les entiers  $z_0 + k \frac{n}{d}$ , avec  $k \in \mathbb{Z}$ , et qu'elle a exactement  $d$  solutions distinctes modulo  $n$ .

**Exercice 2.**

(a) Résoudre dans  $\mathbb{Z}$  les congruences suivantes :

- $21z \equiv 12 \pmod{30}$ ,
- $14z \equiv 5 \pmod{21}$ ,
- $15z \equiv 9 \pmod{25}$ ,
- $z + 4 \equiv 16z + 13 \pmod{18}$ .

(b) Résoudre dans  $\mathbb{Z}$  les systèmes suivants :

$$\begin{cases} 5z \equiv 2 \pmod{3} \\ 3z \equiv 4 \pmod{7} \\ 3z \equiv 7 \pmod{8} \end{cases}, \quad \begin{cases} 6z \equiv 9 \pmod{15} \\ 22z \equiv 55 \pmod{77} \\ 3z \equiv 2 \pmod{13} \\ 27z \equiv 9 \pmod{36} \end{cases}.$$

**Exercice 3.** (du CC du 23/10/24) Le théorème chinois des restes est ainsi nommé parce que sa première formulation remonte à un texte du III ou IV siècle après J.-C. du mathématicien et astronome chinois Sun Zi. La première preuve générale et constructive de ce théorème est apparu beaucoup plus tard, dans l'ouvrage *Shùshū Jiǔzhāng* (« Traité mathématique en neuf chapitres ») du mathématicien chinois Qin Jiushao. On sait que ce livre a été publié dans le XIIIe siècle et que l'année de publication  $n$  satisfait les conditions suivantes :

- $n$  est impair.
- le reste de la division de  $n$  par 9 est 5 ;
- $11 \mid (2n + 3)$  ;

Dans quelle année le livre *Shùshū Jiǔzhāng* a-t-il été publié ?

**Exercice 4.** Déterminer un couple d'entiers  $a, b$  tels que la congruence linéaire

$$az \equiv b \pmod{319}$$

a exactement 11 solutions distinctes modulo 319.

**Exercice 5.** Le grand-père Mario a trois petits-enfants, Alice, Bob et Charlie, âgés respectivement de 17, 16 et 4 ans. Le grand-père dit à Alice : « Pour obtenir mon âge, il faut un multiple du tien, plus celui de Bob. » Puis, s'adressant à Bob, il ajoute : « Pour obtenir mon âge, il faut un multiple du tien, plus celui de Charlie. » Enfin, il dit à Charlie : « Sais-tu que mon âge est exactement un multiple du tien ? » Quel est l'âge de grand-père Mario ?

**Exercice 6.** Soient  $n_1, \dots, n_k$  des entiers positifs premiers deux-à-deux, et  $N = \prod_{i=1}^k n_i$ . On définit

$$\begin{aligned} \theta : \frac{\mathbb{Z}}{N\mathbb{Z}} &\rightarrow \frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{n_k\mathbb{Z}} \\ [a]_N &\mapsto ([a]_{n_1}, \dots, [a]_{n_k}). \end{aligned}$$

Pour  $\alpha, \beta \in \mathbb{Z}/N\mathbb{Z}$ , on note  $\theta(\alpha) = (\alpha_1, \dots, \alpha_k)$  et  $\theta(\beta) = (\beta_1, \dots, \beta_k)$ .

- Montrer que  $\theta$  est bien définie.
- Montrer que  $\theta$  est une bijection.
- Montrer que  $\theta(\alpha + \beta) = (\alpha_1 + \beta_1, \dots, \alpha_k + \beta_k)$  et  $\theta(\alpha\beta) = (\alpha_1\beta_1, \dots, \alpha_k\beta_k)$ .
- Montrer que pour tout  $m \geq 0$ ,  $\theta(\alpha^m) = (\alpha_1^m, \dots, \alpha_k^m)$ .
- Montrer que  $\alpha$  est inversible si et seulement si  $\alpha_i$  est inversible pour tout  $i$ , et que le cas échéant,  $\theta(\alpha^{-1}) = (\alpha_1^{-1}, \dots, \alpha_k^{-1})$ . En déduire qu'il existe une bijection entre  $(\frac{\mathbb{Z}}{N\mathbb{Z}})^\times$  et  $(\frac{\mathbb{Z}}{n_1\mathbb{Z}})^\times \times \dots \times (\frac{\mathbb{Z}}{n_k\mathbb{Z}})^\times$ .

**Exercice 7.** On rappelle que pour tout  $n \in \mathbb{Z}_{>0}$  la fonction  $\varphi$  d'Euler (ou l'indicatrice d'Euler) est définie de la façon suivante :

$$\varphi(n) = \#\{a \in \mathbb{Z} : 1 \leq a \leq n, \text{pgcd}(a, n) = 1\}.$$

Dans cet exercice on veut démontrer que si  $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ , où les  $p_i$  sont des premiers distincts et  $e_i > 0$  pour tout  $i$ , alors :

$$\varphi(n) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \dots (p_r^{e_r} - p_r^{e_r-1}). \quad (1)$$

- Montrer que si  $p$  est premier alors  $\varphi(p) = p - 1$ .
- Montrer que si  $p$  est premier et  $s \in \mathbb{Z}_{>0}$ , alors  $\varphi(p^s) = p^s - p^{s-1}$ .
- Montrer que  $\varphi$  est une fonction *multiplicative*, c'est à dire que  $\varphi(nm) = \varphi(n)\varphi(m)$  chaque fois que  $n$  et  $m$  sont deux entiers premiers entre eux.
- Déduire des points précédents la formule (1).

**Exercice 8.** Soient  $n_1, n_2 \in \mathbb{Z}_{>0}$  et soit  $d = \text{pgcd}(n_1, n_2)$ . Soient  $a_1, a_2 \in \mathbb{Z}$ . Montrer qu'il existe un entier  $z$  tel que  $z \equiv a_1 \pmod{n_1}$  et  $z \equiv a_2 \pmod{n_2}$  si et seulement si  $a_1 \equiv a_2 \pmod{d}$ .