

**TD 4**

THÉORÈME CHINOIS DES RESTES

**Esercice 1.** Le grand-père Mario a trois petits-fils, Alice, Bob et Charlie, âgées 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 ?

**Esercice 2.** 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  $a_1 \equiv a_2 \pmod{d}$ .

**Esercice 3.** Soient  $n_1, \dots, n_k$  des entiers positifs premiers deux-à-deux, et  $N = \prod_{i=1}^k n_i$ . On définit

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

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

- a) Montrer que  $\theta$  est bien définie.
- b) Montrer que  $\theta$  est une bijection.
- c) Montrer que  $\theta(\alpha + \beta) = (\alpha_1 + \beta_1, \dots, \alpha_k + \beta_k)$  et  $\theta(\alpha\beta) = (\alpha_1\beta_1, \dots, \alpha_k\beta_k)$ .
- d) Montrer que pour tout  $m \geq 0$ ,  $\theta(\alpha^m) = (\alpha_1^m, \dots, \alpha_k^m)$ .
- e) 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  $(\frac{\mathbb{Z}}{n_1\mathbb{Z}})^\times \times \dots \times (\frac{\mathbb{Z}}{n_k\mathbb{Z}})^\times$ .

**Esercice 4.** 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 :

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

- a) Montrer que si  $p$  est premier alors  $\varphi(p) = p - 1$ .
- b) Montrer que si  $p$  est premier et  $s \in \mathbb{Z}_{>0}$ , alors  $\varphi(p^s) = p^s - p^{s-1}$ .
- c) 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.
- d) Déduire des points précédents la formule (1).