Université Saclay-Paris-Sud **Feuille de TD 3, détails sur l'exercice 11**
M303

Exercice 1. (**Exercice 11, question 2 détaillée**) Soit n un entier > 1. On fait opérer le groupe $G = (\mathbb{Z}/n\mathbb{Z})^\times$ sur l'ensemble $X = \mathbb{Z}/n\mathbb{Z}$ par $a \cdot x = ax$. Écrire la formule des classes correspondante (on pourra définir une bijection entre l'ensemble des orbites et les diviseurs de n). *Détails et indications :*

1. Si $x \mod n$ et $y \mod n$ sont dans la même orbite alors il existe a dans $\mathbb{Z}$ premier à n (ie tel que $a \mod n$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$) tel que $x = ay \mod n$. On a alors vérifié en TD que ceci implique que (x, n) ont les mêmes diviseurs que (y, n) et donc même pgcd.

   Réciproquement, si $d = x \wedge n = y \wedge n$ alors $\frac{x}{d} \wedge \frac{n}{d} = 1 = \frac{y}{d} \wedge \frac{n}{d}$. En particulier, $\frac{x}{d}$ et $\frac{y}{d}$ sont inversibles $\mod \frac{n}{d}$ donc il existe $\alpha, \beta \in \mathbb{Z}$, tels que
   $$\frac{x}{d}\alpha = 1 = \beta\frac{y}{d} \mod \frac{n}{d}.$$
   Notamment α et β sont inversibles $\mod \frac{n}{d}$ donc on a trouvé ainsi un $\gamma \in \mathbb{Z}$ inversible $\mod \frac{n}{d}$ tel que
   $$\frac{x}{d} = \gamma\frac{y}{d} \mod \frac{n}{d}.$$
   En multipliant cette égalité par d, on trouve que $x = \gamma y \mod n$. L'entier γ est a priori seulement inversible $\mod \frac{n}{d}$ et on aimerait un entier γ' inversible $\mod n$. Finalement la question se ramène donc à prouver la chose suivante :

2. *Montrer que le morphisme*
   $$(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/\frac{n}{d}\mathbb{Z})^\times,\ x \mod n \mapsto x \mod \frac{n}{d}$$
   est surjectif. (En effet, si ceci est vrai alors on relève $\gamma \mod \frac{n}{d}$ en $\gamma' \mod n$ qui répond à notre question : il existe γ' dans $\mathbb{Z}$ premier à n (ie tel que $\gamma' \mod n$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$) tel que $x = \gamma' y \mod n$ autrement dit x et y sont dans la même orbite.

   (a) Pour prouver le point précédent, et en oubliant totalement les notations de l'exercice en cours. Soit n un entier et p un nombre premier. Montrer que le morphisme
   $$(\mathbb{Z}/np\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times,\ x \mod np \mapsto x \mod n$$
   est surjectif (en distinguant selon que p divise ou pas n).

   (b) Déduire de cette sous question la précédente.

3. Vérifier que l'on a une bijection entre les orbites pour l'action considérée et les diviseurs de n (donnée par orbite de $x \mod n \mapsto x \wedge n$; de bijection réciproque d divisant $n \mapsto$ orbite de $d \mod n$).

4. Soit donc d un diviseur de n. Montrer que le stabilisateur de $d \mod n$ est de cardinal $\phi(n)/\phi(\frac{n}{d})$ où $\phi(k)$ est le cardinal du groupe des inversibles de $(\mathbb{Z}/k\mathbb{Z})^\times$.

5. Écrire l'équation aux classes ainsi obtenue :
   $$n = \sum_{d|n} \phi(d).$$