Université de Paris-Sud, année 2007/2008
Filière Math/Info-L2
Maths 209

Feuille d'exercices numéro 4

Arithmétique, groupes cycliques, $\mathbf{Z}/n\mathbf{Z}$

On rappelle que $(\mathbf{Z}/n\mathbf{Z})^*$ désigne l'ensemble des éléments de $\mathbf{Z}/n\mathbf{Z}$ qui possèdent un inverse pour la multiplication.

1. Résoudre dans $\mathbf{Z}$ les équations :

$$35x + 14y = 10$$

$$35x + 14y = 14$$

2. Soit n un entier au moins égal à 2.

a) On suppose n premier. Résoudre l'équation $x^2 = \bar{1}$ dans $\mathbf{Z}/n\mathbf{Z}$.

b) Soit $y \in \mathbf{Z}$ tel que $\bar{y}^2 = \bar{1}$ dans $\mathbf{Z}/91\mathbf{Z}$. On suppose que y n'est congru ni à 1 ni à -1 modulo 91. Montrer qu'on est dans l'une des deux situations suivantes :

i) $y \equiv 1$ mod. 7 et $y \equiv -1$ mod. 13.

ou

ii) $y \equiv -1$ mod. 7 et $y \equiv 1$ mod. 13.

c) Résoudre l'équation $x^2 = \bar{1}$ dans $\mathbf{Z}/91\mathbf{Z}$.

3. Parmi les groupes suivants, dire lesquels sont cycliques :

a) Le groupe des permutations $\mathcal{S}_3$ de l'ensemble $\{1, 2, 3\}$ (muni de la composition $\circ$).

b) Le groupe $((\mathbf{Z}/7\mathbf{Z})^*, \times)$.

c) Le groupe $((\mathbf{Z}/8\mathbf{Z})^*, \times)$.

d) Le groupe multiplicatif des matrices de la forme

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

avec $a \in \mathbf{Z}/n\mathbf{Z}$.

4. a) Résoudre l'équation $x^2 + y^2 = \bar{0}$ dans $\mathbf{Z}/7\mathbf{Z}$.

b) Même question en remplaçant $\mathbf{Z}/7\mathbf{Z}$ par $\mathbf{Z}/13\mathbf{Z}$.

5. Soient n et d deux entiers non nuls. On suppose que d divise n.

a) Montrer qu'on peut définir un morphisme f de $\mathbf{Z}/n\mathbf{Z}$ dans $\mathbf{Z}/d\mathbf{Z}$ par la formule

$$f(x \text{ mod. } n) = x \text{ mod. } d \quad \forall x \in \mathbf{Z}$$

où x mod. n désigne la classe de x dans $\mathbf{Z}/n\mathbf{Z}$ et x mod. d la classe de x dans $\mathbf{Z}/d\mathbf{Z}$. Montrer que f est surjective.

b) Montrer qu'on peut définir un morphisme g de $\mathbf{Z}/d\mathbf{Z}$ dans $\mathbf{Z}/n\mathbf{Z}$ par la formule

$$g(x \text{ mod. } d) = (n/d)(x \text{ mod. } n) \quad \forall x \in \mathbf{Z}$$

Montrer que g est injective.

6. Soient m et n des entiers strictement positifs. On appelle $f(m, n)$ le nombre de solutions de l'équation $mx = \bar{0}$ dans $\mathbf{Z}/n\mathbf{Z}$.

a) Calculer $f(2, 4)$, $f(5, 15)$, $f(3, 8)$.

b) On suppose que m et n sont premiers entre eux. Que vaut $f(m, n)$?

c) Donner une formule pour $f(m, n)$ quand m et n sont quelconques.

7. a) Déterminer les générateurs du groupe additif $\mathbf{Z}/2008\mathbf{Z}$.

b) Combien y a-t-il de nombres dans $\{1, ..., 2008\}$ qui ne sont pas premiers avec 8 ? Combien y a-t-il de nombres dans $\{1, ..., 2008\}$ qui ne sont pas premiers avec 251 ? Combien y a-t-il de nombres dans $\{1, ..., 2008\}$ qui ne sont premiers ni avec 8 ni avec 251 ?

c) Calculer $\varphi(2008)$.