L2 MTH1314 2014-2015

Feuille 3. $\mathbb{Z}/n\mathbb{Z}$

Exercice 1.

1. Ecrire l'ensemble des multiples de $\overline{x}$ dans $\mathbb{Z}/5\mathbb{Z}$ pour $x = 0, \cdots, 4$.
2. Ecrire l'ensemble des multiples de $\overline{x}$ dans $\mathbb{Z}/6\mathbb{Z}$ pour $x = 0, \cdots, 5$.
3. Ecrire l'ensemble des multiples de $\overline{x}$ dans $\mathbb{Z}/8\mathbb{Z}$ pour $x = 0, \cdots, 7$.
4. Soient n et x deux entiers naturels. Démontrer que les trois propositions suivantes sont équivalentes.
   (a) $\overline{x}$ admet un inverse pour la multiplication dans $\mathbb{Z}/n\mathbb{Z}$.
   (b) x et n sont premiers entre eux.
   (c) tout élément de $\mathbb{Z}/n\mathbb{Z}$ est multiple de $\overline{x}$ dans $\mathbb{Z}/n\mathbb{Z}$.
5. Calculer l'inverse de $\overline{4}$ dans $\mathbb{Z}/9\mathbb{Z}$.
6. Calculer l'inverse de $\overline{8}$ dans $\mathbb{Z}/15\mathbb{Z}$.

Exercice 2.

1. Soit n un entier naturel non premier, $n \geq 5$. Montrer qu'il existe deux éléments de $\mathbb{Z}/n\mathbb{Z}$, différents de $\overline{0}$, dont le produit est $\overline{0}$. En déduire que $(n-1)!$ est divisible par n.
2. Soit p un nombre premier ≥ 5. Montrer que pour tout entier $x = 2, \cdots, p-2$, il existe un entier $y = 2, \cdots, p-2$ différent de x, tel que le produit xy soit congru à 1 modulo p. En déduire que si p est un nombre premier, alors $(p-1)! + 1$ est divisible par p. (C'est le théorème de Wilson).

Exercice 3. Soit $k \in \mathbb{Z}$, n un entier naturel supérieur ou égal à 2. On rappelle que l'ordre de l'élément $\overline{k}$ dans $(\mathbb{Z}/n\mathbb{Z}, +)$ est le plus petit $m \in \mathbb{N}$ tel que $m\overline{k} = \overline{0}$. Montrer qu'il est égal à $\frac{n}{n \wedge k}$.

Exercice 4.

1. Justifier que l'anneau $\mathbb{Z}/6\mathbb{Z}$ est isomorphe à l'anneau $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
2. Observer que si $u \in \mathbb{Z}/2\mathbb{Z}$ alors $u^2 = u$, et si $u \in \mathbb{Z}/3\mathbb{Z}$ alors $u^3 = u$. En déduire que si $x \in \mathbb{Z}/6\mathbb{Z}$ alors $x^3 = x$.
3. Résoudre dans $\mathbb{Z}/6\mathbb{Z}$ les équations suivantes:
   (a) $x^5 - \overline{1} = \overline{0}$.
   (b) $x^5 - \overline{2} = \overline{0}$.
   (c) $x^4 + x^3 + \overline{2} = \overline{0}$.

Exercice 5. Trouver les entiers relatifs n tels que $\begin{cases} n \equiv 3\ [17] \\ n \equiv 4\ [11] \end{cases}$.

Exercice 6. On veut résoudre dans $\mathbb{Z}/33\mathbb{Z}$ l'équation $x^2 + \overline{2} = \overline{0}$.

1. Montrer que $n \in \mathbb{Z}$ vérifie $n^2 + 2 \equiv 0\ [33]$ si et seulement si:
$$n^2 + 2 \equiv 0\ [3] \text{ et } n^2 + 2 \equiv 0\ [11].$$
2. Observer que si $n \in \mathbb{Z}$, alors $n^2 \equiv 0\ [3]$ si $n \in 3\mathbb{Z}$, et $n^2 \equiv 1\ [3]$ sinon.
3. Observer que $3^2 \equiv -2\ [11]$, et en déduire que dans $\mathbb{Z}/11\mathbb{Z}$ on a
$$x^2 + \overline{2} = (x - \overline{3})(x + \overline{3}).$$
4. Donner toutes les solutions de l'équation $x^2 + \overline{2} = \overline{0}$ dans $\mathbb{Z}/33\mathbb{Z}$.

Exercice 7. Résoudre dans $\mathbb{Z}$ le système $\begin{cases} x \equiv 1 \mod 27 \\ x \equiv 13 \mod 17 \end{cases}$

Exercice 8. Trouver les $n \in \mathbb{Z}$ tels que $n \equiv 12\ [1530]$ et $n \equiv 30\ [6762]$. On commencera par décomposer en produit de facteurs premiers les nombres 1530 et 6762.

Exercice 9. Trouver tous les entiers naturels $n \in \mathbb{N}$ tels que $1 \leq n \leq 105$ et les restes des divisions euclidiennes de n par 3, 5, 7 sont respectivement 1, 2, 3.

Exercice 10. Montrez que tous les facteurs premiers impairs de $n^2 + 1$, où $n \in \mathbb{Z}$, sont de la forme $4k + 1$. Pour cela, on évaluera de deux manières le carré de $n^{\frac{p-1}{2}}$ modulo p.

Exercice 11. Soient p et q deux entiers premiers entre eux. Démontrer que $(\mathbb{Z}/pq\mathbb{Z})^\times$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$.

Exercice 12. Soit $n = 561 = 3 \times 11 \times 17$. Montrer grâce au théorème chinois que si a est premier avec n, alors $a^{n-1} \equiv 1\ [n]$.

Exercice 13. Soit $n \geqslant 3$, on veut montrer que l'ensemble des inversibles de $\mathbb{Z}/2^n\mathbb{Z}$, noté $(\mathbb{Z}/2^n\mathbb{Z})^\times$ n'est pas cyclique, c'est-à-dire n'est pas engendré par un élément. On procède par l'absurde et on suppose que $(\mathbb{Z}/2^n\mathbb{Z})^\times$ est cyclique, ce qui s'écrit encore,
$$\exists a \in (\mathbb{Z}/2^n\mathbb{Z})^\times, \quad \text{tel que} \quad \langle a \rangle = \{1, a, a^2, \ldots\} = (\mathbb{Z}/2^n\mathbb{Z})^\times.$$

1. Montrer que $\left(2^{n-1} + 1\right)^2 \equiv 1\ [2^n]$.
2. Donner l'ordre de a et montrer que $a^{2^{n-2}} = 2^{n-1} + 1$.
3. Montrer que l'on a aussi $\left(2^{n-1} + 1\right)^2 \equiv 1\ [2^n]$ et conclure a une contradiction.

Exercice 14. Soient p et q deux nombres premiers distincts, $n = pq$ et t un entier tel que $t \equiv 1\ [\varphi(n)]$.

1. Montrer que $\forall x \in \mathbb{Z}/n\mathbb{Z}$, $x^t = x$ en distinguant les quatre cas possibles pour $d = pgcd(x, pq)$.
2. On considère u un entier premier avec $\varphi(n)$ et v son inverse dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$ (cf l'exercice 1 pour l'existence). Montrer que les fonctions ψ_u et ψ_v de $Z/n\mathbb{Z}$ dans $Z/n\mathbb{Z}$ définies par $\forall x \in \mathbb{Z}/n\mathbb{Z}$, $\psi_u(x) = x^u$ et $\psi_v(x) = x^v$ sont des fonctions réciproques l'une de l'autre et sont donc bijectives.