L2 MTH1314 2016-2017

Feuille 4. L'anneau $\mathbb{Z}/n\mathbb{Z}$.

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. Soient n et x deux entiers naturels. Démontrer que les deux propositions suivantes sont équivalentes.
   (a) x et n sont premiers entre eux.
   (b) tout élément de $\mathbb{Z}/n\mathbb{Z}$ est multiple de $\overline{x}$ dans $\mathbb{Z}/n\mathbb{Z}$.
4. Calculer l'inverse de $\overline{4}$ dans $\mathbb{Z}/9\mathbb{Z}$ et l'inverse de $\overline{8}$ dans $\mathbb{Z}/15\mathbb{Z}$.

Exercice 2. Résoudre les équations suivantes dans $\mathbb{Z}/37\mathbb{Z}$:

1. $\begin{cases} \overline{3}x + \overline{7}y = \overline{3} \\ \overline{6}x - \overline{7}y = \overline{0} \end{cases}$
2. $x^2 - \overline{31}x + \overline{18} = \overline{0}$
   Indication : $\overline{6}^2 = -\overline{1}$.

Exercice 3.

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 $\mathbb{Z}/6\mathbb{Z}$ l'équation $x^5 - \overline{1} = \overline{0}$.

Exercice 4. Soit p un entier tel que p, $4p + 1$ et $7p - 4$ soient premiers.

1. Calculer $4p + 1$ et $7p - 4$ dans $\mathbb{Z}/3\mathbb{Z}$.
2. En déduire l'unique valeur possible de p.

Exercice 5. Trouver les entiers relatifs $n \in \mathbb{Z}$ tels que $\begin{cases} n \equiv 7\ [8] \\ n \equiv 1\ [13] \end{cases}$.

Exercice 6. Trouver les entiers relatifs $n \in \mathbb{Z}$ tels que $\begin{cases} n \equiv 1\ [2] \\ n \equiv 2\ [7] \\ n \equiv 6\ [9] \end{cases}$.

Exercice 7. 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 8. Résoudre les équations suivantes :

1. $3x \equiv 4 \mod 7$.
2. $9x \equiv 12 \mod 21$.
3. $103x \equiv 612 \mod 676$.

Exercice 9.

1. pour tout $k \in \mathbb{N}$, calculer $2^{2^{2k}}$ et $2^{2^{2k+1}}$ modulo 7.
2. En déduire pour tout $n \in \mathbb{N}$ la valeur de $4^{2^n} + 2^{2^n} + 1$ modulo 7.

Exercice 10. Montrer que pour tout $n \in \mathbb{Z}/42\mathbb{Z}$, on a $n^7 = n$.

Exercice 11.

1. Soit n un entier naturel non premier, $n \geqslant 5$. 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 $\geqslant 5$. 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 12. Soient p et q deux entiers premiers distincts. Montrer que $p^{q-1} + q^{p-1} = 1$ $[pq]$.

Exercice 13. 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 14. Calculer 10^{100} (le gogol) modulo 247.

Exercice 15. Soit $\overline{a_n a_{n-1} \dots a_1 a_0}$ l'écriture décimale du nombre $a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_1 \times 10 + a_0$ en base 10.

1. Vérifier que $\overline{a_n a_{n-1} \dots a_1 a_0} = a_n + \cdots + a_0$ [9].
2. Soient A la somme des chiffres de 4444^{4444}, B la somme des chiffres de A et C la somme des chiffres de B. Calculer C modulo 9.
3. Montrer que $C < 16$ et en déduire la valeur de C.

Exercice 16. Soient $p \neq 2$ un nombre premier et $a, b \in \mathbb{N}$ non divisibles par p. On suppose que p divise $a^2 + b^2$.

1. Montrer qu'il existe $x \in \mathbb{Z}/p\mathbb{Z}$ tel que $x^2 = -1$.
2. En évaluant de deux façons le carré de $x^{\frac{p-1}{2}}$, montrer que $p \equiv 1$ [4].

Exercice 17. Soient p et q deux nombres premiers distincts, $n = pq$ et t un entier tel que $t \equiv 1$ $[\varphi(n)]$ où φ est l'indicatrice d'Euler.

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 $\mathbb{Z}/\varphi(n)\mathbb{Z}$. Montrer que les fonctions ψ_u et ψ_v de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ 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.