Devoir Surveillé n° 2

Mercredi 13 Nvembre - Durée 2h

La calculatrice n'est pas autorisée, ainsi que les documents de cours et de TD. Chaque réponse doit être justifiée. Un soin particulier devra être apporté à la rédaction. Les exercices, notamment les différentes parties de l'exercice 3, sont largement indépendantes.

Exercice 1. On considère un anneau commutatif $(A, +, \times)$. On dit qu'un élément $a \in A$ est nilpotent s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$. On note $\mathcal{N}(A)$ l'ensemble des éléments nilpotents de A.

1. Que vaut $\mathcal{N}(A)$ si A est intègre ?
2. Montrer que $\mathcal{N}(A)$ est un idéal de l'anneau A.
3. Soit $a \in \mathcal{N}(A)$. Montrer que $u = 1_A + a$ est un élément inversible de A.
4. Soit $n \geq 2$, $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ sa décomposition en facteurs premiers. Montrer que

$$\overline{x} \in \mathcal{N}(\mathbb{Z}/n\mathbb{Z}) \Leftrightarrow p_1 \cdots p_k \text{ divise } x.$$

En déduire l'ensemble $\mathcal{N}(\mathbb{Z}/125\mathbb{Z})$.

Exercice 2.

On considère l'équation d'inconnues u, v

$$ua + vb = c \tag{E}$$

avec a, b, c donnés, $a, b \neq 0$.

1. Déterminer une condition nécessaire et suffisante d'existence de solutions de (E).
2. On suppose connu un couple (u_0, v_0) de solutions de (E). Déterminer l'ensemble des solutions de (E) en fonction de (u_0, v_0).
3. Résoudre dans $\mathbb{Z}^2$ l'équation $56u + 72v = 40$.

Exercice 3.

On rappelle que si $(A, +, \times)$, $(B, +, \times)$ sont des anneaux, $A \times B$ est munit d'une structure d'anneaux en posant

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),\ (a_1, b_1) \times (a_2, b_2) = (a_1 \times a_2, b_1 \times b_2),$$

avec $0_{A\times B} = (0_A, 0_B)$, $1_{A\times B} = (1_A, 1_B)$.

Théorème des restes chinois

Supposons que $m \wedge n = 1$. Le but de cette section est de montrer l'isomorphisme d'anneaux

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

On considère l'application

$$\Phi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

définie par $\Phi(\overline{x}^{mn}) = (\overline{x}^m, \overline{x}^n)$ (où $\overline{x}^k$ désigne la classe de l'entier x dans $\mathbb{Z}/k\mathbb{Z}$).

1. Montrer que l'application Φ est bien définie.
2. Montrer que Φ est un morphisme d'anneaux de $\mathbb{Z}/mn\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
3. En utilisant la question 2 de l'Exercice 2, montrer que Φ est surjective. En déduire que Φ est bijective, et que $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Indicatrice d'Euler

Si $(A, +, \times)$ est un anneau, on note A^* son groupe des inversibles. Soit $n > 1$ un entier. On appelle indicatrice d'Euler de n l'entier

$$\varphi(n) = \mathrm{Card}((\mathbb{Z}/n\mathbb{Z})^*).$$

1. Montrer que
$$(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{k} \in \mathbb{Z}/n\mathbb{Z} \mid k \wedge n = 1\}.$$
En particulier, $\varphi(n)$ est aussi le nombre d'entiers $k \in \{1, 2, \cdots, n\}$ tels que $k \wedge n = 1$.
2. Soit $p \in \mathbb{P}$ et $\alpha \in \mathbb{N}^*$. Montrer que $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
3. Montrer que $(A \times B)^* = A^* \times B^*$. En déduire que si $m \wedge n = 1$, alors $\varphi(mn) = \varphi(m)\varphi(n)$.
4. Soit $n \geq 2$, $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ sa décomposition en facteurs premiers. Montrer que
$$\varphi(n) = p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1) \cdots (p_k - 1) = n(1 - 1/p_1) \cdots (1 - 1/p_k).$$

Formule de Gauss

Le but est de montrer pour tout $n \geq 2$ la formule suivante

$$\sum_{d|n, d>0} \varphi(d) = n.$$

1. Soit $d > 0$ un diviseur de n, et soit
$$E_d = \{x \in \{1, 2, \cdots, n\} | x \wedge n = d\}.$$
Montrer que $E_{d_1} \cap E_{d_2} = \emptyset$ si $d_1 \neq d_2$.
2. Montrer que $\{1, 2, \cdots, n\}$ est la réunion des E_d pour chaque $d > 0$ diviseur de n.
3. Montrer que le nombre d'éléments dans chaque E_d est $\varphi(n/d)$.
4. Conclure.

Exercice 4. ♠

1. Montrer que si $p, p + 2, p + 4 \in \mathbb{P}$, alors $p = 3$.
2. En déduire que 5 est le seul nombre premier qui est somme et différence de nombres premiers.