ARITHMÉTIQUE
ENTIERS ET POLYNÔMES

Exercice 1 Soit p un entier premier.

1. Montrer que p divise C_p^q avec $1 \leq q \leq p-1$. En déduire que dans l'anneau $\mathbb{Z}/_{p\mathbb{Z}}$ avec p premier $(a+b)^p = a^p + b^p$ puis que $(a-b)^p = a^p - b^p$ et enfin que $(a_1 + a_2 + ... + a_k)^p = a_1^p + a_2^p + ... + a_k^p$.
2. En considérant le corps $\mathbb{Z}/_{pZ}$, montrer que $k^p \equiv k[p]$(petit théorème de **FERMAT**).

Exercice 2

1. Soient a et b deux entiers naturels non nuls premiers entre eux supérieurs ou égales à 2. Montrer que
$$\forall (u_0, v_0) \in \mathbb{N}^2, \ \ u_0 a - v_0 b = 1, \ \text{ avec } \ u_0 < b \ \text{ et } \ v_0 < a$$
et exprimer en fonction de u_0, v_0, a et b tous les couples $(u, v) \in \mathbb{Z}$ solutions de $ua - vb = 1$.
2. Déterminer deux entiers u et v vérifiant $47u + 11v = 1$.

Exercice 3 Soient m et n deux entiers premiers entre eux.

1. Montrer que $\mathbb{Z}/_{mn\mathbb{Z}}$ et $\mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}}$ sont isomoprphes.
En déduire que : $\varphi(mn) = \varphi(m)\varphi(n)$. $(\varphi(n) = \text{card}\{k \ / \ 1 \leq k \leq n \text{ et } n \wedge k = 1\})$
2. Soit p un nombre premier, calculer $\varphi(p^k)$ pour $k \in \mathbb{N}^*$, en déduire $\varphi(n)$ pour tout $n \in \mathbb{N}^*$.
3. Trouver toutes les solutions des systèmes suivantes :
$$\begin{cases} x \equiv 1 \ [3] \\ x \equiv 3 \ [5] \\ x \equiv 4 \ [7] \\ x \equiv 2 \ [11] \end{cases} \qquad \begin{cases} x \equiv 998 \ [2011] \\ x \equiv 999 \ [2012] \end{cases}$$

Exercice 4 Soit $f : \mathbb{C} \to \mathbb{C}$ un endomorphisme de l'anneau $(\mathbb{C}, +, .)$ tel que $\forall x \in \mathbb{R} \ f(x) = x$. Montrer que f est l'identité ou la conjugaison complexe.

Exercice 5 Soit $\mathbb{K}$ un corps commutatif fini. Calculer $\prod_{x \in \mathbb{K}^*} x$.

Exercice 6 Résoudre les équations suivantes :

$$a) \quad 3x + 5 = 0 \ \text{ dans } \ \mathbb{Z}/_{10\mathbb{Z}} \quad b) \quad x^2 = 1 \ \text{ dans } \ \mathbb{Z}/_{8\mathbb{Z}} \quad c) \ x^2 + 2x + 2 = 0 \ \text{ dans } \ \mathbb{Z}/_{5\mathbb{Z}}$$

Exercice 7 Résoudre les systèmes suivantes :

$$a) \quad \begin{cases} x \equiv 1[6] \\ x \equiv 2[7] \end{cases} \qquad b) \quad \begin{cases} 3x \equiv 2[5] \\ 5x \equiv 1[6] \end{cases} \qquad c) \quad \begin{cases} x + y \equiv 4[11] \\ xy \equiv 10[11] \end{cases}$$

Exercice 8 Soit A l'ensemble défini par :

$$A = \{z \in \mathbb{C} / \exists (a, b) \in \mathbb{Z}^2 \ \text{ tel que } z = a + jb\}$$

avec $j = e^{\frac{2\pi i}{3}}$

1. Montrer que A muni de l'addition et de la multiplication dans $\mathbb{C}$ est un anneau commutatif.
2. Montrer que l'ensemble des éléments inversibles de A est l'ensemble U défini par :
$$U = \{z \in A / |z| = 1\}$$

Exercice 9 Soit $\mathbb{K}$ un corps commutatif.

1. Montrer que $(\mathbb{K} \times \mathbb{K}, +, \cdot)$ n'est pas un corps.
2. Montrer que le diagonale de $\mathbb{K} \times \mathbb{K}$ est un corps isomorphe à $\mathbb{K}$.

Exercice 10 On considère $\mathbb{R}$ comme espace vectoriel sur $\mathbb{Q}$. Soit $\alpha = \sqrt[3]{2}$ ($\alpha \notin \mathbb{Q}$).

1. Montrer que les nombres $1, \alpha, \alpha^2$ sont linéairement indépendants. En utilisant $\alpha^3 = 2$, on montrera que toute relation de dépendance linéaire entrainerait que α soit rationnel.
2. Montrer que le sous-espace vectoriel L de $\mathbb{R}$ engendré par 1,α, α^2 est un sous-anneau intègre de $\mathbb{R}$.
3. Soit $x \in L^*$. Montrer que l'application de L dans lui même qui à y associé xy est une bijection. En déduire que L est un corps. Donner l'expression de l'inverse de $x \neq 0$

Exercice 11 Déterminer le reste de la division euclidienne du polynôme $X^n + X + b$ par $(X - a)^2$.

Exercice 12 Décomposer le polynôme $P = X^5 - 13X^4 + 67X^3 - 171X^2 + 216X - 108$ sachant qu'il admet des racines multiples.

Exercice 13 Soit a et b deux éléments distincts de $\mathbb{K}$.
Montrer que la suite des polynômes $E_p = (X - a)^{n-p}(X - b)^p$ pour $p = 0, 1, ..., n$ est une base de l'espace des polynômes de degré inférieur ou égal à n.

Exercice 14 Calculer la somme $S_4 = \sum_{i=1}^{5} x_i^4$ des puissances quatrièmes des racines de l'équation :

$$X^5 + pX^3 + qX^2 + r = 0.$$

Exercice 15 Soit $P \in \mathbb{R}[X]$ et $\alpha + \beta X$ le reste de la division euclidienne par $X^2 + 1$, φ l'application de $\mathbb{R}[X]$ dans $\mathbb{R}^2$ définie par $\varphi(P) = (\alpha, \beta)$.
Montrer que l'on peut définir une addition et une multiplication sur $\mathbb{R}^2$ de manière que φ soit un hommorphisme d'anneau et que l'anneau image est un corps isomorphe au corps $\mathbb{C}$.
Application :
Montrer que $P(X) = (\cos(a) + X\sin(a))^n - (\cos(na) + X\sin(na))$ est divisible par $X^2 + 1$ $(n \in \mathbb{N}^*)$.

Exercice 16 Soit $n \in \mathbb{N}^*$, $P \in \mathbb{R}_{n-1}[X]$, Montrer que :

$$P(0) = \frac{1}{n} \sum_{\omega \in \Omega_n} P(\omega)$$

Où Ω_n désigne l'ensemble des racines $n^{ième}$ de l'unité dans $\mathbb{C}$.

Exercice 17 Soit $P = X^n - \alpha_1 X^{n-1} - ... - \alpha_n$,$\forall k \in [1, n]$, $\alpha_k \geq 0$

1. Montrer qu'il existe un seul $\varrho > 0$ tel que $P(\varrho) = 0$.
2. Prouver que le module de toute racine de P est inférieure à ϱ et que si $\alpha_1 \neq 0$, le module de toute racine de P autre que ϱ est $< \varrho$.

•••••••••