Examen Partiel

Mercredi 13 mars 2024 - Durée 1h30
Documents interdits - Calculettes interdites

Exercice 1.1. — Soit $E = \{P \in \mathbf{Q}[X] \mid P(\mathbf{Z}) \subset \mathbf{Z}\}$.

1. Soit $n \in \mathbf{Z}$. On note $E_n = \{P \in \mathbf{Q}[X] \mid P(n) \in \mathbf{Z}\}$.
   (a) Montrer que E_n est un sous-anneau de $\mathbf{Q}[X]$.
   (b) En déduire que E est un anneau contenant $\mathbf{Z}[X]$.
2. (a) Montrer que E est un anneau intègre.
   (b) Quels sont les éléments inversibles de E ?
3. Soit p un nombre premier. Montrer que $\frac{1}{p}(X^p - X) \in E$.

Exercice 1.2. — Soit $n = 2024$.

1. (a) Rappeler pourquoi $\mathbf{Z}/n\mathbf{Z} \simeq \mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/11\mathbf{Z} \times \mathbf{Z}/23\mathbf{Z}$.
   (b) Quel est le cardinal de $(\mathbf{Z}/n\mathbf{Z})^*$?
2. On considère l'application S de $(\mathbf{Z}/n\mathbf{Z})^*$ vers $(\mathbf{Z}/n\mathbf{Z})^*$ définie par $S(x) = x^2$.
   (a) Montrer que S définit un morphisme de groupe.
   (b) Montrer que $|\ker S| = 16$.
3. (a) Montrer que $5^8 \equiv 2017 \pmod{n}$. *Indication : on pourra montrer que* $5^8 \equiv -7 \pmod{n}$.
   (b) En déduire une solution de l'équation $x^2 = \overline{2017}$ dans $\mathbf{Z}/n\mathbf{Z}$.
   (c) Quel est le nombre de solutions de l'équation $x^2 = \overline{2017}$ dans $\mathbf{Z}/n\mathbf{Z}$?

Exercice 1.3. —
On note $\mathcal{P}$ l'ensemble des nombres premiers p congrus à 1 modulo 8. Le but de cet exercice est de montrer que $\mathcal{P}$ est infini (cas particulier du théorème de la progression arithmétique de Dirichlet).

1. Donner la liste des 3 plus petits éléments de $\mathcal{P}$.
2. Soit p un nombre premier impair et a un entier tel que p divise $a^4 + 1$. On note $\overline{a}$ la classe de a modulo p.
   (a) Montrer que $\overline{a} \in (\mathbf{Z}/p\mathbf{Z})^*$. Quel est l'inverse de $\overline{a}$?
   (b) Montrer que $\overline{a}$ est d'ordre 8.
   (c) En déduire que $p \in \mathcal{P}$.
3. On suppose que $\mathcal{P}$ est fini et on note $a = \prod_{p \in \mathcal{P}} p$. Soit p_0 un diviseur premier de $1 + 16a^4$.
   (a) Montrer que 8 divise $p_0 - 1$.
   (b) En déduire que p_0 divise a.
   (c) En déduire que p_0 divise 1.
4. En déduire que l'ensemble $\mathcal{P}$ est infini.