Université Saclay-Paris-Sud Feuille de TD 5 M303

Exercice 1. 1. Montrer que l'ensemble

$$\{a^2+b^2+c^2 \in \mathbb{Z}/8\mathbb{Z} \mid a,b,c \in \mathbb{Z}/8\mathbb{Z}\}$$

est strictement contenu dans $\mathbb{Z}/8\mathbb{Z}$.

2. En déduire qu'il existe une infinité d'entiers n'étant pas somme de 3 carrés.

Exercice 2. Résoudre l'équation $n^{13} \equiv n \bmod 1365$ en entiers.

Exercice 3. Calculer 10^{10^n} modulo 7 pour tout entier $n \in \mathbb{N}$.

Exercice 4. Trouver tous les x dans $\mathbb{Z}$ vérifiant simultanément $3x-10 \in 7\mathbb{Z}$, $11x+8 \in 17\mathbb{Z}$ et $16x-1 \in 5\mathbb{Z}$.

Exercice 5. Résoudre le système de congruences simultanées :

$$\begin{cases} 14x & \equiv & 7 & \pmod{1789} \\ 18x & \equiv & 6 & \pmod{1940} \end{cases}$$

Exercice 6. Soient p et ℓ deux nombres premiers.

1. Montrer qu'il existe un élément d'ordre ℓ dans $(\mathbb{Z}/p\mathbb{Z})^\times$ si et seulement si $p-1$ est un multiple de ℓ. Dans ce cas, combien de solutions y a-t-il ?

2. On suppose p impair. Montrer que l'équation $x^2+x+1=0$ a une solution dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si l'équation $x^2+3=0$ a une solution dans $\mathbb{Z}/p\mathbb{Z}$.

3. On suppose $p \geq 5$. Montrer que -3 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1 \bmod 3$.

Exercice 7. Pour tout ensemble fini E, on note $\operatorname{Card} E$ le nombre d'éléments de E. Dans tout cet exercice, p est un nombre premier impair et l'on note $\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, *)$ le corps à p éléments.

1. Montrer que l'on définit bien des morphismes du groupe $(\mathbb{F}_p^\times, *)$ par $\chi(x) := x^2$ et $\lambda(x) := x^{\frac{p-1}{2}}$ pour tout $x \in \mathbb{F}_p^\times$.

2. (a) Pour tout $x \in \mathbb{F}_p^\times$, calculer

$$\chi \circ \lambda(x) \text{ et } \lambda \circ \chi(x).$$

(b) En déduire que

$$\operatorname{Im}\lambda \subset \operatorname{Ker}\chi \text{ et } \operatorname{Im}\chi \subset \operatorname{Ker}\lambda.$$

3. (a) Pour tout polynôme P de degré d, à coefficients dans $\mathbb{F}_p$, donner, en justifiant brièvement votre réponse, un majorant du nombre de racines de P dans $\mathbb{F}_p$.

(b) En déduire que

$$\operatorname{Card}\operatorname{Ker}\chi = 2 \text{ et } \operatorname{Card}\operatorname{Ker}\lambda \leq \frac{p-1}{2}.$$

(c) Montrer finalement que

$$\operatorname{Im}\chi \;=\; \operatorname{Ker}\lambda\ .$$

4. Déduire de ce qui précède que -1 est un carré modulo p si et seulement si $p \equiv 1 \pmod 4$.

5. Montrer qu'il existe une infinité de premiers p tels que -1 est un carré modulo p. *Indication : Par l'absurde on pourra considérer un p maximal, et choisir un diviseur premier de $(p!)^2+1$.*

Exercice 8. Soit p un nombre premier et m un entier. Calculer

$$\sum_{x\in\mathbb{Z}/p\mathbb{Z}} x^m.$$

Exercice 9. Calculer $\left(\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)^{20212022}$