Année 2024-2025

L3 (S6) – Méthodes analytiques dans l'arithmétique.

Contrôle continu.

26 février 2025

Durée 1 heure. Utilisation des documents autorisée, mais pas encouragée.

Exercice 1.

Soit p un nombre premier impair et soient ϕ et ψ deux endomorphismes de $(\mathbb{Z}/p\mathbb{Z})^\times$ définis par $\phi(x) = x^2$ et $\psi(x) = x^{\frac{p-1}{2}}$.

a. Trouver les ordres des noyaux et des images de ϕ et de ψ.

b. Montrer que l'image de ϕ coïncide avec le noyau de ψ.

c. Existe-t-il une solution de l'équation $x^2 + 1 \equiv 0 \mod 2017963$.

Exercice 2.

Soient $f \in \mathbb{Z}[x]$ un polynôme au coefficients entiers et $x_0 \in \mathbb{Z}$ tel que $f(x_0) \equiv 0 \mod p$ et $f'(x_0) \neq 0 \mod p$.

a. Montrer qu'il existe $x_1 \in \mathbb{Z}$ tel que $f(x_1) \equiv 0 \mod p^2$ et $x_1 \equiv x_0 \mod p$.

b. Montrer que pour tout $n \in \mathbb{N}$ il existe $x_n \in \mathbb{Z}$ tel que $f(x_n) \equiv 0 \mod p^{n+1}$ et $x_n \equiv x_{n-1} \mod p^n$

Indication : Soit $g \in \mathbb{Z}$ tel que $gf'(x_0) = 1 \mod p$ et soit $x_n = x_{n-1} - gf(x_{n-1})$. Pour montrer que $f(x_n) \equiv 0 \mod p^{n+1}$ utiliser le développement limité de $f(x)$ en x_{n-1}.

Exercice 3.

Trouver le nombre de groupes abéliens de l'ordre 8000.

Exercice 4.

Pour le groupe $(\mathbb{Z}/7\mathbb{Z})^\times$

a. Expliciter le caractère de l'ordre 2.

b. Expliciter le caractère de l'ordre maximal.

Correction :
1a : L'équation $x^2 = 1$ a deux solution dans $\mathbb{Z}/p\mathbb{Z}$, notamment $x = \pm 1$ car $\mathbb{Z}/p\mathbb{Z}$ est un corps. Donc $|\ker \phi| = 2$. Donc $|\operatorname{Im} \phi| = (p-1)/2$. $\psi^2(x) = x^{p-1} = 1$ donc $\psi(x) = \pm 1$. Il existe au moins un élément $\xi \in (\mathbb{Z}/p\mathbb{Z})^\times$ dont l'ordre est exactement $p-1$ et donc $\psi(\xi) \neq 1$. Donc $\operatorname{Im} \psi = \{\pm 1\}$. Alors $|\operatorname{Im} \psi| = 2$ et $|\ker \psi| = (p-1)/2$.
1b : $\psi(\phi(x)) = x^{p-1} = 1$ donc $\operatorname{Im} \phi \subseteq \ker \psi$. Ils coïncident car ils ont le même nombre d'éléments.
1c : $(-1)^{(2017963-1)/2} = (-1)^{(63-1)/2} = (-1)^{31} = -1$. Alors -1 n'est pas dans l'image de ϕ est donc l'équation $x^2 + 1 \equiv 0 \mod 2017963$ n'a pas de solutions.

2a : Cherchons la solution de la forme $x_1 = x_0 + hp$. Alors $f(x_1) = f(x_0) + hpf'(x_0) + g^2p^2f''(x_0)/2 + \cdots$. Tout les termes sont divisible par p et à partir du troisième terme ils sont divisible par p^2. Donc $f(x_1)$ est divisible par p^2 si $f(x_0)/p + hf'(x_0) \equiv 0 \mod p$. Tel h existe car la multiplication par $f'(x_0)$ est un isomorphisme de $(\mathbb{Z}/p\mathbb{Z})^\times$.
2b : $f(x_n) = f(x_{n-1}) + gf(x_{n-1})f'(x_{n-1}) + (gf(x_{n-1}))^2 f''(x_{n-1}) + \cdots \equiv f(x_{n-1}) + gf(x_{n-1})f'(x_{n-1}) \mod p^n \equiv f(x_n)(1 - gf'(x_{n-1})) \mod p^n$ car $f(x_{n-1})$ est divisible par p^{n-1}. A son tour $f'(x_{n-1}) \equiv f'(x_0) \mod p$ et donc $1 + gf'(x_{n-1}) \equiv 0 \mod p$. Alors $f(x^n) \equiv 0 \mod p^{n-1}$.

3 : $8000 = 2^6 \cdot 5^3$. Tout groupe d'ordre 8000 est un produit de groupes cyclique d'ordre d_i avec $d_i | d_{i+1}$ et $\prod d_i = 8000$. Donc $d_i = 2^{a_i}5^{b_i}$ avec $\sum a_i = 6$ et $\sum b_i = 3$ et $a_i \geqslant a_{i+1}$ et $b_i \geqslant b_{i+1}$. Alors il y a 3 possibilités pour b_i : (3), (2,1) et (1,1,1) et 11 possibilités pour a_i : (6), (5,1), (4,2), (4,1,1), (3,3), (3,2,1),(3,1,1,1), (2,2,2), (2,2,1,1), (2,1,1,1,1), (1,1,1,1,1,1). Donc il y a 33 groupes d'ordre 8000.

4a : Le groupe $(\mathbb{Z}/7\mathbb{Z})$ est cyclique donc le caractère est déterminé par sa valeur sur un générateur. Pour le générateur on peu choisir par exemple 3 car modulo 7 on a $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$. Car le caractère d'ordre 2 doit prendre valeurs ± 1 on a $\chi_2(3) = \chi_2(6) = \chi_2(5) = -1$ et $\chi_2(1) = \chi_2(2) = \chi_2(4) = 1$.
4b : Le caractère à l'ordre 6 si $\chi(3)$ a l'ordre 6. Par exemple on peut prendre $\chi(3) = e^{\pi i/3}$. Donc $(\chi(1), \ldots, \chi(6)) = (1, e^{2\pi i/3}, e^{\pi i/3}, e^{-2\pi i/3}, e^{-\pi i/3}, -1)$.