MP – CPGE Mohammed VI-Kénitra

Année scolaire 21/22

Devoir libre $n^\circ 1$

à rendre le 18/09/2023

Exercice 1 : Dans $(\mathscr{S}_n, \circ)$ on considère les permutations $\tau = \begin{pmatrix} 1 & 2 \end{pmatrix}$ et $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \end{pmatrix}$.

1. Calculer $\sigma^k \circ \tau \circ \sigma^{-k}$ pour $0 \leq k \leq n-2$.

2. En déduire que tout élément de $\mathscr{S}_n$ peut s'écrire comme un produit de τ et de σ.

Exercice 2 : Pour tout entier $n \geq 1$, on note $f_n = 2^n + 1$ et $M_n = 2^n - 1$. $\mathbb{F}_n^*$ désigne le groupe multiplicatif des éléments inversibles de l'anneau $\mathbb{Z}/_{n\mathbb{Z}}$.

1. Soit $n \geq 1$ un entier.

Démontrer que si M_n est premier, alors n aussi, et que si f_n est premier alors n est une puissance de 2.

Indication : Remarquer que, pour $a \in \mathbb{Z}$ et $k, m \in \mathbb{N}$, $a^k - 1$ divise $a^{km} - 1$ et, si m est impair $a^k + 1$ divise $a^{mk} + 1$.

On pose $F_k = f_{2^k}$.

2. Soient k, l deux nombres entiers avec $k < l$. Démontrer que $2^{2^l} \equiv 1[F_k]$. En déduire que F_k et F_l sont premiers entre eux.

3. Soit $p > 2$ un nombre premier et soit q un diviseur premier de M_p. Quel est l'ordre de 2 dans le groupe $(\mathbb{F}_q^*, .)$? En déduire que q est de la forme $2kp + 1$.

4. Démontrer que M_{13} est premier.

5. De même soit $l \in \mathbb{N}$ et q un diviseur premier de F_l.

5a. Quel est l'ordre de 2 dans le groupe $(\mathbb{F}_q^*, .)$?

5b. En déduire que q est de la forme $2^{l+1}k + 1$.

5c. On suppose que $l \geq 2$. Notons w la classe de $2^{2^{l-2}}$ dans $\mathbb{F}_q$. Remarquant que $w^4 = -1$, démontrer que $2 = (w + w^{-1})^2$ est un carré modulo q. En déduire que 2^{l+2} divise $q - 1$.

5d. Démontrer que le plus petit diviseur de F_5 distinct de 1 est supérieure ou égal à 641.

5e. En remarquant que $641 = 5^4 + 2^4$, démontrer que $F_5 \equiv 1 - 5^4 2^{28}[641]$.

5f. Démontrer que 641 divise F_5.

Exercice 3 : Pour $n \in \mathbb{N}$, on note $(\mathbb{Z}/_{n\mathbb{Z}})^*$ le groupe multiplicatif des éléments inversibles de l'anneau $\mathbb{Z}/_{n\mathbb{Z}}$. Le but de cet exercice est de voir pour quels n ce groupe est cyclique.

1. Soit m un nombre impair démontrer que les groupes $(\mathbb{Z}/_{2m\mathbb{Z}})^*$ et $(\mathbb{Z}/_{m\mathbb{Z}})^*$ sont isomorphes.

2. ***2a.*** Quels sont les nombres entiers $n \in \mathbb{N}^*$ dont l'indicatrice d'Euler $\varphi(n)$ est impaire ?

2b. Soient $m, n \in \mathbb{N}$ deux nombres premiers entre eux, supérieurs ou égaux à 3. Démontrer que le groupe $(\mathbb{Z}/_{mn\mathbb{Z}})^*$ n'est pas cyclique.

2c. Le groupe $(\mathbb{Z}/_{8\mathbb{Z}})^*$ est-il cyclique ?

2d. Pour quels $k \in \mathbb{N}$ le groupe $(\mathbb{Z}/_{2^k\mathbb{Z}})^*$ est-il cyclique ?

3. Soient G un groupe commutatif et $f : G \to H$ un homomorphisme de groupes. On suppose que $f(G)$ et $\mathrm{Ker}\, f$ sont cycliques et que leurs ordres sont premiers entre eux. Démontrer que G est cyclique.

4. Soient p un nombre premier distinct de 2 et $n \in \mathbb{N}^*$. L'homomorphisme d'anneaux $g : \mathbb{Z}/_{p^n\mathbb{Z}} \to \mathbb{Z}/_{p\mathbb{Z}}$ qui à la classe de x modulo p^n associe la classe de x modulo p induit un homomorphisme surjectif de groupes $f : (\mathbb{Z}/_{p^n\mathbb{Z}})^* \to (\mathbb{Z}/_{p\mathbb{Z}})^*$.

4a. Démontrer que $(1+p)^{p^k} \equiv 1 + p^{k+1}[p^{k+2}]$, pour tout $k \in \mathbb{N}$.

4b. En déduire que le groupe $\mathrm{Ker}\, f$ est cyclique.

4c. Démontrer que le groupe $(\mathbb{Z}/_{p^n\mathbb{Z}})^*$ est cyclique.

5. Quels sont les entiers $m \in \mathbb{N}^*$, tels que le groupe $(\mathbb{Z}/_{m\mathbb{Z}})^*$ soit cyclique ?

Exercice 4 : $\mathscr{B} = (e_1, e_2, ..., e_n)$ désigne la base canonique de $\mathbb{R}^n$ ($n \in \mathbb{N}^* \setminus \{1\}$) et f l'endomorphisme de $\mathbb{R}^n$ définie par $f(e_1) = e_n$ et $f(e_i) = e_{i-1}$ pour $2 \leq i \leq n$.

1. Montrer que f est inversible.

2. M désigne la matrice de f dans la base $\mathscr{B}$. Soit $G = \left\{ M^k \;\middle|\; k \in \mathbb{Z} \right\}$. Montrer que G est une groupe cyclique et préciser son cardinal.

Fin de l'épreuve