3MA262
Licence de mathématiques
Année académique 2023-2024

SCIENCES SORBONNE UNIVERSITÉ

Feuille d'exercices n° 3

Énoncés

Exercice 1 – Soit n un entier naturel et considérons l'application $f : \mathbb{Z} \to \mathbb{Z}/n^2\mathbb{Z}$ qui associe à un entier a la classe de a^n modulo n^2.

1. Montrer qu'étant donné un entier a, l'élément $f(a)$ ne dépend que que la classe de a modulo n. L'application f induit donc une application $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n^2\mathbb{Z}$.
2. Vérifier que, par restriction, on obtient un homomorphisme de groupes $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/n^2\mathbb{Z})^\times$. Décrire son image et son noyau.

Exercice 2 – Dans cet exercice, on se propose de décrire le groupe $(\mathbb{Z}/p^n\mathbb{Z})^\times$ pour $n > 1$. On admettra que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique. On commence e supposant p impair. L'entier naturel n est fixé.

1. Montrer que quels que soient $x, y \in \mathbb{Z}$, on a la congruence
$$(x + p^n y)^p \equiv x^p + yx^{p-1}p^{n+1} \pmod{p^{n+2}}.$$
2. En déduire la congruence
$$(1 + p)^{p^n} \equiv 1 + p^{n+1} \pmod{p^{n+2}}$$
3. Montrer que pour $n > 0$, l'élément $1+p \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ est d'ordre p^{n-1} et en déduire que $(\mathbb{Z}/p^n\mathbb{Z})^\times$ est cyclique.

On s'intéresse maintenant au cas $p = 2$.

4. Vérifier que pour $n > 1$, l'élément -1 n'est pas un carré dans $(\mathbb{Z}/2^n\mathbb{Z})^\times$.
5. Montrer que pour tout entier naturel $n \geq 0$, on a la congruence
$$5^{2^n} \equiv 1 + 2^{n+1} \pmod{2^{n+2}}.$$
6. En déduire que pour $n > 1$, l'élément $5 \in (\mathbb{Z}/2^n\mathbb{Z})^\times$ est d'ordre 2^{n-2}, puis que le groupe $(\mathbb{Z}/2^n\mathbb{Z})^\times$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$. Déterminer explicitement ses éléments d'ordre 2.

Exercice 3 – L'application qui $\rho : \mathbb{N}_{>0} \to \mathbb{N}_{>0}$ qui associe à un entier n l'exposant du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est la ***fonction indicatrice de Carmichael***.

1. Soient n et m deux entiers. Justifier le fait que $\rho(n)$ divise $\varphi(n)$, que si n divise m alors $\rho(n)$ divise $\rho(m)$ et que pour $(n, m) = 1$, on a $\rho(nm) = [\rho(n), \rho(m)]$.
2. Montrer que l'on a l'identité
$$\mathrm{rad}(n)\rho(n) = n[p - 1 \mid p|n],$$
où $\mathrm{rad}(n) = \prod_{p|n} p$ est le ***radical*** de n.

3. Montrer que les seules entiers sans facteurs carrés pour lesquels $\rho(n)$ divise n sont $2, 3, 7$ et 43.
4. Construire une famille infinie d'entiers n divisibles par 31 tels que $\rho(n)$ divise n.

Exercice 4 – Étant donnés deux polynômes $f, g \in \mathbb{Z}[X]$, avec g primitif, comsidérons la division euclidienne $f = gq + r$ dans $\mathbb{Q}[X]$. Montrer que l'on a $q \in \mathbb{Z}[X]$ si et seulement si $r \in \mathbb{Z}[X]$ (indication : on utilisera le contenu d'un polynôme).

Exercice 5 – Considérons deux polynômes $f, g \in \mathbb{Z}[X]$, avec g non nul.

1. Montrer que l'on a une écriture unique

$$af = qg + r,$$

avec $a \in \mathbb{N}_{>0}$, $q, r \in \mathbb{Z}[X]$, $\deg(r) < \deg(f)$ et $(c(q), a) = 1$, où $c(q)$ désigne le contenu de q.
2. On suppose que pour tout nombre premier p, l'image de g dans $\mathbb{F}_p[X]$ divise celle de f. Montrer que g divise f dans $\mathbb{Q}[X]$.
3. Posons $f = a_0 + a_1X + \cdots + a_dX^d$ et $|f| = \max_i\{|x_i|\}$. Soient $p_1 < \cdots < p_n$ des nombres premiers tels que $p_1 \cdots p_n > |f|$. Montrer que si g divise f dans $\mathbb{F}_{p_i}[X]$ pour tout $i \in \{1, \ldots, n\}$ alors g divise f dans $\mathbb{Q}[X]$.

Exercice 6 – Soient $f \in \mathbb{Z}[X]$ un polynôme unitaire et p un nombre premier. Montrer que si l'image canonique de f dans $\mathbb{F}_p[X]$ est irréductible alors f est irréductible dans $\mathbb{Q}[X]$. Qu'en est-il si f n'est pas supposé unitaire ?