TD DU 18/11/11 ET DU 25/11/11

EXERCICE 1. Oral ENS 1998 Soit $n \in \mathbb{N}$, on note $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. À $P \in \mathbb{Z}[X]$ on associe $\varphi_n(P) \in \mathcal{F}(\mathbb{Z}_n, \mathbb{Z}_n)$ définie par

$$\forall x \in \mathbb{Z}_n,\ \varphi_n(P)(x) \equiv P(x)[n]$$

Pour quelles valeurs de n a-t-on

$$\forall f \in \mathcal{F}(\mathbb{Z}_n, \mathbb{Z}_n),\ \exists P \in \mathbb{Z}[X] \text{ tel que } f = \varphi_n(P) \ ?$$

EXERCICE 2.

(1) Soit $P = aX^2 + bX + c$ vérifiant $\exists N \in \mathbb{N},\ \forall n \geqslant N,\ \sqrt{P(n)} \in \mathbb{Z}$.
En utilisant un développement asymptotique de $\sqrt{P}$, montrer qu'il existe $(\alpha, \beta) \in \mathbb{Z}^2,\ P = (\alpha X + \beta)^2$

(2) On suppose maintenant $\exists N \in \mathbb{N},\ \forall n \geqslant N,\ \sqrt{P(n)} \in \mathbb{Q}$.
Montrer qu'il existe $(\alpha, \beta) \in \mathbb{Q}^2,\ P = (\alpha X + \beta)^2$.

Solution 1 On a $\operatorname{Card} \mathcal{F}(\mathbb{Z}_n, \mathbb{Z}_n) = n^n$. On note $\mathcal{P}_n$ l'ensemble des fonctions polynomiales de $\mathbb{Z}_n$ et $\mathcal{F}_n$ l'ensemble des fonctions de $\mathbb{Z}_n$ dans $\mathbb{Z}_n$. On a évidemment $\mathcal{P}_n \subset \mathcal{F}_n$, le but du jeu est de savoir si on a égalité entre ces deux sous-ensembles ou non.

- Si n est premier :
  - Première solution : on utilise les polynômes de Lagrange. Soit $f \in \mathcal{F}_n$, on pose $f(i) = a_i$ et $\bar{P} = \sum_{i=0}^{n-1} a_i L_i$ où $L_i = \prod_{i \neq j} \frac{X - j}{i - j}$. $\bar{P}_i$ s'écrit $\sum_{i=0}^{n-1} \bar{\alpha}_i X^i$ où $\bar{\alpha}_i \in \mathbb{Z}_n$ donc $\bar{P}_i(x) = \varphi_n(P)(x)$ où $P = \sum_{i=0}^{n-1} \alpha_i X^i$, α_i étant un représentant de $\bar{\alpha}_i$.
    $\varphi_n(P)(x) = P(x)$ est bien une fonction polynomiale qui prend les mêmes valeurs que f donc on a bien $f = \varphi(P_n)$ et par conséquent $\mathcal{F}_n = \mathcal{P}_n$.
  - Deuxième solution : $\mathcal{F}_n$ est un espace vectoriel de dimension n sur $\mathbb{Z}_n$. Comme $x^n = x$ dans $\mathbb{Z}_n$ alors on peut prouver que $\forall m \in \mathbb{N}$, $\exists p \in [0, n-1]$ tq $x^m = x^p$ dans $\mathbb{Z}_n$. La famille $(\varphi_n(1), \varphi_n(X), \ldots, \varphi_n(X^{n-1}))$ est une famille génératrice de $\mathcal{P}_n$.
    Montrons que cette famille est libre : soit $\bar{P} = \sum_{i=0}^{n-1} \bar{\alpha}_i X^i$ un polynôme tel que $\bar{P}(x) = 0$ pour tout x de $\mathbb{Z}_n$, il est donc divisible par $X^n - X = \prod_{i=0}^{n-1} (X - i)$. Comme il est de degré $\leqslant n-1$ c'est le polynôme nul donc $\alpha_i = 0$ pour tout i. Ceci permet de conclure que la famille est libre.
    Conclusion : la famille de fonctions $x \mapsto x^i$, pour $i = 0, ..., n-1$ est une base de $\mathcal{P}_n$ donc $\dim \mathcal{P}_n = n$ et $\operatorname{Card} \mathcal{P}_n = n^n$ ce qui permet d'affirmer que $\mathcal{P}_n = \mathcal{F}_n$.
- Si n n'est pas premier : par exemple si $n = 4$ alors, pour $P = 2(X^2 - X)$ on a $\varphi_4(P) = 0$ donc $\operatorname{Card} \mathcal{P}_4 < 64 = 4^4 = \operatorname{Card} \mathcal{F}_4$ ($\psi : (a_0, a_1, a_2, a_3) \in (\mathbb{Z}/4\mathbb{Z})^4 \mapsto (x \mapsto a_0 + a_1 x + a_2 x^2 + a_3 x^3)$ n'est pas injective) donc $\mathcal{P}_4 \not\subset \mathcal{F}_4$.
  Plus généralement toute fonction polynomiale sur $\mathbb{Z}_n$ est de degré $\leqslant n-1$: en effet,

comme la fonction $x \mapsto \prod_{k=0}^{n-1}(x-k)$ est la fonction nulle dans $\mathbb{Z}_n$ alors il suffit de diviser n'importe quel polynôme P à coefficients dans $\mathbb{Z}_n$ par le polynôme $Q = \prod_{k=0}^{n-1}(X-k)$, $P = QS + R$ avec $\deg R \leqslant n-1$, les fonctions polynomiales $\widetilde{P}$ et $\widetilde{R}$ sont égales.
Pour $n = pq$ avec p premier, on peut essayer $P = q(X^p - X)$. En effet, on sait que $x^p \equiv x[p]$ pour tout x de $\mathbb{Z}$ donc, si $x \in \mathbb{Z}_n$ alors $x^p - x = p.a$ où $a \in \mathbb{Z}_n$ donc $\varphi_n(P)(x) = 0$.
On peut aussi raisonner par l'absurde :
soit p un diviseur strict de n, $f \in \mathcal{F}_n$ telle que $f(0) = 0$ et $f(p) = 1$. Si $f(x) = \varphi_n(P)(x)$ alors $f(x) = a_1 x + \cdots + a_m x^m$ donc

$$p(a_1 + \cdots + a_m p^{m-1}) = 1$$

i.e. p est inversible dans $\mathbb{Z}_n$ ce qui est impossible.

Solution 2

(1) (cas 1) Si $a = b = 0$ $\sqrt{c} \in \mathbb{Z}$ donc c est un carré.
(cas 2) Si $a = 0$, $b \neq 0$: on se ramène au (cas 3) en remplaçant n par n^2.
(cas 3) Si $a \neq 0$; On fait un développement limité : le comportement à l'infini entraîne que $a > 0$ pour que le radical ait un sens ;

$$\begin{aligned} f(n) = \sqrt{an^2 + bn + c} &= \sqrt{a}n\left(1 + \frac{b}{2an} + o\left(\frac{1}{n}\right)\right) \\ &= \sqrt{a}n + \frac{b}{2n\sqrt{a}} + o\left(\frac{1}{n}\right) \end{aligned}$$

$f(n+1) - f(n)$ entier tend vers $\sqrt{a}$ qui est donc entier (ne marche plus pour $\mathbb{Q}$) donc $a = a_1^2 \in \mathbb{N}$.
$f(n) = a_1 n + \frac{b}{2a_1} + o(1)$; pour la même raison $f(n) - na_1$ entier tend vers un entier. Donc $b = 2a_1 k$ où $k \in \mathbb{Z}$ et $o(1) = 0$ ce qui permet de conclure.

(2) On commence d'abord par remarquer que a, b, c sont dans $\mathbb{Q}$ puisque, pour un certain entier p : $ap^2 + bp + c$, $a(p+1)^2 + b(p+1) + c$, $a(p+2)^2 + b(p+2) + c$ sont dans $\mathbb{Q}$.

On choisit ensuite un entier q tel que q^2a, q^2b, q^2c soient entiers (on notera ces trois entiers A, B, C). Alors, pour n assez grand, la racine carrée de $An^2 + Bn + C$ est à la fois un rationnel et la racine carrée d'un entier ... donc un entier.
On est ramené à la première question ...
