HX3 Lycée Henri IV Paris

Mathématiques

Devoir en temps libre N^{o}7

À remettre le mercredi 19 mars 2003

Polynômes à valeurs entières sur les nombres premiers.

Objectif : le but de ce problème est l'étude d'ensembles de polynômes prenant sur certaines parties des valeurs particulières et, notamment une caractérisation des polynômes prenant des valeurs entières sur tous les nombres premiers.

NOTATIONS :

Si A et B désignent 2 ensembles, B étant inclus dans A, on note $A\backslash B = \{x \in A;\ x \notin B\}$

On note $\mathbb{P}$ l'ensemble des nombres premiers. Pour tout nombre premier p, on note $\mathbb{Z}_{(p)}$ l'ensemble des rationnels dont une représentation irréductible a un dénominateur non divisible par p.

Pour tout réel x, on appelle partie entière de x et on note $[x]$ l'unique entier k vérifiant $k \leqslant x < k+1$

Pour tout sous-ensembles E et F de $\mathbb{R}$ on note :

$$\mathcal{P}(E,F) = \{P \in \mathbb{R}[X];\ P(E) \subset F\}$$

à savoir l'ensemble des éléments de $\mathbb{R}[X]$ dont la valeur en chaque élément de E appartient à F.

I. Exemples élémentaires : $\mathcal{P}(\mathbb{Q},\mathbb{Q}), \mathcal{P}(\mathbb{R},\mathbb{R}_+), \mathcal{P}(\mathbb{Q},\mathbb{Q}_+)$

1. Comparer l'ensemble $\mathcal{P}(\mathbb{Q},\mathbb{Q})$ avec l'ensemble $\mathbb{Q}[X]$.

   (On pourra introduire les polynômes interpolateurs de Lagranges associés à une suite convenablement choisie.)

2. (a) Montrer la propriété suivante :

   $(*)$ Pour tous $(a,b,c,d) \in \mathbb{Z}^4$, $\exists (x,y) \in \mathbb{Z}^2$ tels que $(a^2+b^2)(c^2+d^2) = x^2+y^2$

   (b) Soit A un anneau commutatif et unitaire (on note 0 et 1 les éléments neutres de l'addition et de la multiplication). Montrer que la propriété $(*)$ reste valable lorsqu'on remplace $\mathbb{Z}$ par A.

   On note : $S = \{z \in A \mid \exists (x,y) \in A^2 \text{ tel que } z = x^2+y^2\}$.

   Montrer que S contient 0 et 1 et est stable par multiplication.

3. Soit P un élément de $\mathcal{P}(\mathbb{R},\mathbb{R}_+)$

(a) On rapelle que P est le produit d'une constante par des facteurs de la forme $(X-a)^\alpha$ et $(X^2+bX+c)^\beta$ où a, b, c sont réels, α et β des entiers positifs ou nuls et X^2+bX+c un polynôme irréductible de $\mathbb{R}[X]$.

Montrer que P est de degré pair. Donner le signe de la constante et préciser la parité des entiers α.

(b) En déduire que P est la somme des carrés de deux polynômes.

(c) Donner une caractérisation de l'ensemble $\mathcal{P}(\mathbb{R}, \mathbb{R}_+)$.

4. Montrer que $\mathcal{P}(\mathbb{Q}, \mathbb{Q}_+)$ est contenu dans $\mathcal{P}(\mathbb{R}, \mathbb{R}_+)$.

5. Soit $P = 2X^2 + 4$.

(a) Soient a, b, c, d quatre réels tels que l'on ait : $P = (aX + b)^2 + (cX + d)^2$.
Montrer qu'il existe $\theta \in \mathbb{R}$ et $\varepsilon \in \{-1, 1\}$ tel que

$$a = \sqrt{2}\cos\theta, \quad b = -2\varepsilon\sin\theta, \quad c = \sqrt{2}\sin\theta, \quad d = 2\varepsilon\cos\theta.$$

(b) En déduire que le polynôme P ne peut pas être la somme des carrés de deux éléments de $\mathbb{Q}[X]$.

II. Etude de $\mathcal{P}(\mathbb{Z}, \mathbb{Z})$

Pour tout entier naturel n, on note Γ_n le polynôme défini par :

$$\Gamma_0(X) = 1 \text{ et pour } n > 0 \quad \Gamma_n(X) = \frac{X(X-1)\dots(X-n+1)}{n!}$$

1. Montrer que pour tout n, le polynôme Γ_n appartient à $\mathcal{P}(\mathbb{Z}, \mathbb{Z})$.

2. Montrer que, pour tout entier naturel m, la famille $(\Gamma_n)_{0 \leqslant n \leqslant m}$ forme une base de l'espace vectoriel réel $\mathbb{R}_m[X]$.

Soit P un élément de $\mathbb{R}_m[X]$. On écrit

$$P = \sum_{n=0}^{m} d_n \Gamma_n \quad \text{avec } d_0, d_1, \dots, d_m \in \mathbb{R}$$

3. Montrer que les quatre assertions suivantes sont équivalentes :

(a) $P \in \mathcal{P}(\mathbb{Z}, \mathbb{Z})$.

(b) $d_0, d_1, \dots, d_m \in \mathbb{Z}$.

(c) $P(0), P(1), \dots, P(m) \in \mathbb{Z}$.

(d) Il existe $m + 1$ entiers consécutifs en lesquels les valeurs de P sont des entiers.

III. Etude de $\mathcal{P}(E, \mathbb{Z}_{(p)})$

Dans toute cette partie, p désigne un nombre premier fixé et E une partie infinie de $\mathbb{Z}$.

1. Montrer que, pour tout rationnel non nul x, il existe un unique entier relatif k tel que x s'écrive sous la forme $p^k \frac{a}{b}$ où a et b sont des entiers non multiples de p. Cet entier k est noté $v_p(x)$. On pose de plus $v_p(0) = +\infty$. On définit ainsi une application v_p de $\mathbb{Q}$ dans $\mathbb{Z} \cup \{+\infty\}$.

   On adopte les conventions usuelles:

$$k + (+\infty) = (+\infty) + k = +\infty \text{ et } k \leqslant +\infty \text{ pour tout } k \in \mathbb{Z} \cup \{+\infty\}$$

2. Montrer que

   (a) Pour tous x, y de $\mathbb{Q}$ $\quad v_p(xy) = v_p(x) + v_p(y)$.

   (b) Pour tous x, y de $\mathbb{Q}$ $\quad v_p(x+y) \geqslant \min\{v_p(x), v_p(y)\}$.

   (c) Pour tous x, y de $\mathbb{Q}$ $\quad v_p(\frac{x}{y}) = v_p(x) - v_p(y)$.

3. Vérifier que $\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \mid v_p(x) \geqslant 0\}$, et que $\mathbb{Z}_{(p)}$ est un sous-anneau de $\mathbb{Q}$.

4. (a) Montrer que $\mathbb{Z} = \bigcap_{l \in \mathbb{P}} \mathbb{Z}_{(l)}$.

   (b) Vérifier que $\mathcal{P}(E, \mathbb{Z}) = \bigcap_{l \in \mathbb{P}} \mathcal{P}(E, \mathbb{Z}_{(l)})$.

   On dit qu'une suite $(u_n)_{n \in \mathbb{N}}$ d'éléments distincts de E est p-ordonnée dans E si elle vérifie

$$\text{Pour tout } n \in \mathbb{N}^* \quad v_p\left(\prod_{k=0}^{n-1}(u_n - u_k)\right) = \min_{x \in E} v_p\left(\prod_{k=0}^{n-1}(x - u_k)\right)$$

5. Soit $(u_n)_{n \in \mathbb{N}}$ une suite p-ordonnée dans E. On lui associe la suite de polynômes $(P_n)_{n \in \mathbb{N}}$ définie par :

$$P_0(X) = 1 \text{ et, pour } n \geqslant 1,\ P_n(X) = \prod_{k=0}^{n-1} \frac{X - u_k}{u_n - u_k}$$

   (a) Montrer que les polynômes P_n appartiennent à $\mathcal{P}(E, \mathbb{Z}_{(p)})$.
   Préciser les valeurs de $P_n(u_k)$ pour n dans $\mathbb{N}$ et $0 \leqslant k \leqslant n$.

   (b) Montrer que pour tout entier naturel m, la famille $(P_n)_{0 \leqslant n \leqslant m}$ est une base de l'espace vectoriel $\mathbb{R}_m[X]$. Dans la suite, m désigne un entier naturel et P un élément de $\mathbb{R}_m[X]$. Ecrivons

$$P(X) = \sum_{n=0}^{m} c_n P_n(X) \text{ avec } c_0, c_1, \ldots, c_m \in \mathbb{R}$$

   (c) Montrer que les assertions suivantes sont équivalentes.

   i. $P \in \mathcal{P}(E, \mathbb{Z}_{(p)})$.

   ii. $c_0, c_1, \ldots, c_m \in \mathbb{Z}_{(p)}$.

   iii. $P(u_0), P(u_1), \ldots, P(u_m) \in \mathbb{Z}_{(p)}$.

(d) On pose $\omega(0) = 0$ et, pour tout élément n de $\mathbb{N}^*$ on note $\omega(n)$ l'entier $v_p\left(\prod_{k=0}^{n-1}(u_n - u_k)\right)$
Montrer que si P appartient à $\mathcal{P}(E, \mathbb{Z}_{(p)})$ alors, les coefficients de $p^{\omega(m)}P$ appartiennent $\mathbb{Z}_{(p)}$.

(e) Vérifier que $\mathcal{P}(E, \mathbb{Z}_{(p)})$ est un sous-anneau de $\mathbb{Q}[X]$.

IV. Etude de $\mathcal{P}(\mathbb{N}\backslash p\mathbb{N}, \mathbb{Z}_{(p)})$

Dans toute cette partie, p désigne un nombre premier. On note $p\mathbb{N}$ l'ensemble des entiers naturels multiples de p et $\mathbb{N}\backslash p\mathbb{N}$ l'ensemble des entiers naturels non multiples de p.

Pour tout entier naturel n, on pose :

$$\varphi_p(n) = n + 1 + \left[\frac{n}{p-1}\right] \text{ et } \quad \omega_p(n) = \sum_{k\geqslant 0}\left[\frac{n}{(p-1)p^k}\right]$$

On admettra dans la suite que pour tout entier naturel n, $\quad v_p(\varphi_p(n)!) = \omega_p(n)$

1. (a) A l'aide de la division euclidienne par $p-1$, montrer que

$$\left[\frac{\varphi_p(n)}{p}\right] = \left[\frac{n}{p-1}\right] \text{ et } \varphi_p(n) \in \mathbb{N}\backslash p\mathbb{N}$$

(b) En déduire que φ_p est une bijection croissante de $\mathbb{N}$ sur $\mathbb{N}\backslash p\mathbb{N}$.

(c) Vérifier que tout entier naturel :

i. $\omega_p(n) \leqslant 2n$.

ii. Si $n < p-1$ alors $\omega_p(n) = 0$.

2. (a) Montrer que, pour (r, s) dans $p\mathbb{N} \times \mathbb{N}$, $v_p(r - \varphi_p(s)) = 0$.

(b) Justifier, pour $n > 0$, les égalités :

$$v_p\left(\prod_{k=0}^{n-1}(\varphi_p(n) - \varphi_p(k))\right) = v_p\left(\prod_{r=0}^{\varphi_p(n)-1}(\varphi_p(n) - r)\right) = v_p\left(\varphi_p(n)!\right)$$

(c) Justifier, pour $0 < n \leqslant s$ les égalités :

$$v_p\left(\prod_{k=0}^{n-1}(\varphi_p(s) - \varphi_p(k))\right) = v_p\left(\prod_{r=0}^{\varphi_p(n)-1}(\varphi_p(s) - r)\right) = v_p\left(\frac{\varphi_p(s)!}{(\varphi_p(s) - \varphi_p(n))!}\right)$$

(d) En déduire que la suite $(\varphi_p(n))_{n\in\mathbb{N}}$ est une suite p-ordonnée dans $\mathbb{N}\backslash p\mathbb{N}$.

3. Soit P un élément de $\mathbb{R}_m[X]$

(a) Montrer que P appartient à $\mathcal{P}(\mathbb{N}\backslash p\mathbb{N}, \mathbb{Z}_{(p)})$ si et seulement si $P(\varphi_p(k))$ appartient à $\mathbb{Z}_{(p)}$ pour $k = 0, 1, \ldots, m$.

(b) Montrer que si P appartient à $\mathcal{P}(\mathbb{N}\backslash p\mathbb{N}, \mathbb{Z}_{(p)})$ alors les coefficients de $p^{\omega_p(m)}P$ sont dans $\mathbb{Z}_{(p)}$.

V. Un algorithme pour déterminer les éléments de $\mathcal{P}(\mathbb{P}, \mathbb{Z})$

1. Dans cette question p désigne un nombre premier fixé. On pourra utiliser le théorème de Dirichlet suivant : si a et b sont deux entiers premiers entre eux, alors il éxiste au moins un entier naturel k tel que $a + bk$ soit un nombre premier.

   (a) Soit Q un élément de $\mathcal{P}(\mathbb{P}, \mathbb{Z}_{(p)})$ et soit α un entier naturel tel que les coefficients de $p^\alpha Q$ appartiennent à $\mathbb{Z}_{(p)}$.

      i. Soit a un entier naturel, montrer que, pour tout entier relatif k, $Q(a+kp^\alpha)-Q(a)$ appartient à $\mathbb{Z}_{(p)}$.

      ii. Soit a un élément de $\mathbb{N}\backslash p\mathbb{N}$. Montrer qu'il existe un entier naturel k tel que $Q(a + kp^\alpha)$ appartienne à $\mathbb{Z}_{(p)}$.

      iii. En déduire que Q appartient à $\mathcal{P}(\mathbb{N}\backslash p\mathbb{N}, \mathbb{Z}_{(p)})$.

   (b) Pour tout nombre premier l, on pose $E_l = \{l\} \cup (\mathbb{N}\backslash l\mathbb{N})$.

      i. Montrer l'inclusion $\mathbb{P} \subset E_p$.

      ii. En déduire que $\mathcal{P}(\mathbb{P}, \mathbb{Z}_{(p)}) = \mathcal{P}(E_p, \mathbb{Z}_{(p)})$.

      iii. $\mathcal{P}(\mathbb{P}, \mathbb{Z}) = \bigcap_{l\in\mathbb{P}} \mathcal{P}(E_l, \mathbb{Z}_{(l)})$.

   Pour la fin du problème on considère un entier naturel m.

2. Montrer que si Q est un élément de $\mathcal{P}(\mathbb{P}, \mathbb{Z})$ de degré $\leqslant m$ alors $X^{2m}Q(X)$ appartient à $\mathcal{P}(\mathbb{Z}, \mathbb{Z})$.

   (On pourra utiliser V.1.c.iii),IV.3.b),IV.1.c.i),III.4.a) et II.3))

3. On suppose dans cette question que l'élément Q de $\mathbb{R}_m[X]$ vérifie

$$\text{pour tout } k \in \mathbb{N}, \quad \big((1 \leqslant k \leqslant 2m+1) \Rightarrow \ (k^{2m}Q(k) \in \mathbb{Z})\big)$$

   (a) Montrer que
   pour tout $p \in \mathbb{P}$, $\quad Q \in \mathcal{P}(\mathbb{N}\backslash p\mathbb{N}, \mathbb{Z}_{(p)})$.

   (b) Montrer que
   pour tout $p \in \mathbb{P}$, $\quad \big((p > m+1) \Rightarrow \ Q(p) \in \mathbb{Z}_{(p)}\big)$.

4. Caractérisation de $\mathcal{P}(\mathbb{P}, \mathbb{Z})$

   Soit Q un élément de $R_m[X]$. Montrer que les deux assertions suivantes sont équivalentes :

   (a) Q appartient à $\mathcal{P}(\mathbb{P}, \mathbb{Z})$.

   (b) Pour tout nombre premier $p \leqslant m+1$, $Q(p)$ appartient à $\mathbb{Z}$ et, pour tout entier naturel $k \leqslant 2m+1$, $k^{2m}Q(k)$ appartient à $\mathbb{Z}$.