CAPES externe de Mathématiques
session 2002
deuxième composition

Enoncé

http://perso.wanadoo.fr/megamaths

[0] [ag54e]

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
$$A \setminus B = \{x \in A \,;\, x \notin B\}.$$
On note :
$\mathbb{N}$ l'ensemble des entiers naturels, $\mathbb{N}^*$ l'ensemble $\mathbb{N} \setminus \{0\}$;
$\mathbb{Z}$ l'ensemble des entiers relatifs ;
$\mathbb{Q}$ l'ensemble des nombres rationnels, $\mathbb{Q}_+$ l'ensemble des rationnels positifs ou nuls, $\mathbb{Q}^*$ l'ensemble $\mathbb{Q} \setminus \{0\}$;
$\mathbb{R}$ l'ensemble des nombres réels, $\mathbb{R}_+$ l'ensemble des réels positifs ou nuls ;
$\mathbb{P}$ 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 $k \leq x < k+1$.

On note :
$\mathbb{Q}[X]$ l'ensemble des polynômes en l'indéterminée X à coefficients rationnels, $\mathbb{R}[X]$ l'ensemble des polynômes en l'indéterminée X à coefficients réels et, pour tout entier naturel n, $\mathbb{R}_n[X]$ le sous-ensemble de $\mathbb{R}[X]$ formé des polynômes de degré inférieur ou égal à n.

Pour tous 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.

Les parties A, B, C sont indépendantes, la partie D utilise des notions et résultats de la partie C uniquement, la partie E utilise des résultats antérieurs qui seront en général précisés dans le cours de l'énoncé.

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

A - I. *Caractérisation de $\mathcal{P}(\mathbb{Q},\mathbb{Q})$ à l'aide des polynômes de Lagrange.*

Soit m un entier naturel. Pour tous les entiers i et j compris entre 0 et m, on note $\delta_{i,j}$ le symbole de Kronecker défini par : $\delta_{i,j} = 0$ si $i \neq j$ et $\delta_{i,i} = 1$. Soient $q_0, q_1, \ldots, q_m$, $m+1$ réels distincts.

A - I. 1. Expliciter, pour $j = 0, 1, \ldots, m$, le polynôme L_j de $\mathbb{R}_m[X]$ vérifiant :

$$L_j(q_i) = \delta_{i,j} \text{ pour } i = 0, 1, \ldots, m.$$

A - I. 2. Montrer que la famille $(L_j)_{0\leq j\leq m}$ forme une base de l'espace vectoriel réel $\mathbb{R}_m[X]$.

A - I. 3. Pour tout polynôme P de $\mathbb{R}_m[X]$, exprimer P dans la base $(L_j)_{0\leq j\leq m}$ en fonction des réels $(P(q_j))_{0\leq j\leq m}$.

A - I. 4. Comparer l'ensemble $\mathcal{P}(\mathbb{Q},\mathbb{Q})$ avec l'ensemble $\mathbb{Q}[X]$.

A - II. *Caractérisation de l'ensemble $\mathcal{P}(\mathbb{R},\mathbb{R}_+)$.*

A - II. 1. Montrer la propriété suivante :

(*) $\qquad \forall (a,b,c,d) \in \mathbb{R}^4,\ \exists (x,y) \in \mathbb{R}^2\ \ (a^2+b^2)(c^2+d^2) = x^2+y^2.$

On exprimera x et y en fonction de a, b, c, d. (Pour tous réels t et z, on pourra interpréter t^2+z^2 comme le carré du module d'un nombre complexe.)

A - II. 2. Soit A un anneau commutatif 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 $\mathbb{R}$ par A.
On note :

$$S = \{z \in A \mid \exists x \in A,\ \exists y \in A,\ z = x^2 + y^2\}.$$

Montrer que S contient 0 et 1 et est stable pour la multiplication.

A - II. 3. Soit P un élément non nul de $\mathcal{P}(\mathbb{R},\mathbb{R}_+)$.

A - II. 3. i. On rappelle 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 des réels, α et β des entiers positifs ou nuls et X^2+bX+c un polynôme irréductible dans $\mathbb{R}[X]$. Montrer que P est de degré pair. Donner le signe de la constante et préciser la parité des entiers α.

A - II. 3. ii. En déduire que P est la somme des carrés de deux polynômes de $\mathbb{R}[X]$.

A - II. 3. iii. Donner une caractérisation de l'ensemble $\mathcal{P}(\mathbb{R},\mathbb{R}_+)$.

A - III. *La caractérisation précédente n'est pas valable pour $\mathcal{P}(\mathbb{Q},\mathbb{Q}_+)$.*

A - III. 1. Montrer que $\mathcal{P}(\mathbb{Q},\mathbb{Q}_+)$ est contenu dans $\mathcal{P}(\mathbb{R},\mathbb{R}_+)$.

A - III. 2. i. Donner deux décompositions du polynôme $2X^2+4$ en la somme des carrés de deux polynômes de $\mathbb{R}[X]$.

A - III. 2. ii. Soient a, b, c, d des réels tels que l'on ait :

$$2X^2+4 = (aX+b)^2 + (cX+d)^2.$$

Montrer que la matrice

$$\begin{pmatrix} \frac{a}{\sqrt{2}} & \frac{b}{2} \\ \frac{c}{\sqrt{2}} & \frac{d}{2} \end{pmatrix}$$

possède une propriété remarquable à préciser. En déduire que les réels a, b, c, d ne peuvent pas tous être dans $\mathbb{Q}$.

A - III. 2. iii. Le polynôme $2X^2 + 4$ peut-il être la somme des carrés de deux éléments de $\mathbb{Q}[X]$?

B - ETUDE DE $\mathcal{P}(\mathbb{Z}, \mathbb{Z})$

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

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

B - I. 1. Montrer que, pour tout n, le polynôme Γ_n appartient à $\mathcal{P}(\mathbb{Z}, \mathbb{Z})$. (Pour k élément de $\mathbb{Z}$, on distinguera selon que $0 \leq k < n$, $k \geq n$ et $k < 0$.)

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

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

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

B - II. Ecrire, à l'aide des valeurs $(P(n))_{0 \leq n \leq m}$, un système linéaire dont la famille $(d_n)_{0 \leq n \leq m}$ est solution. Calculer le déterminant de ce système.

B - III. Montrer que les quatre assertions suivantes sont équivalentes :
(i) $P \in \mathcal{P}(\mathbb{Z}, \mathbb{Z})$,
(ii) $d_0, d_1, \ldots, d_m \in \mathbb{Z}$,
(iii) $P(0), P(1), \ldots, P(m) \in \mathbb{Z}$,
(iv) il existe $m+1$ entiers consécutifs en lesquels les valeurs de P sont des entiers.

B - IV. 1. Dans cette question, $m = 5$ et

$$P(X) = X^5 - 15X^4 + 85X^3 - 225X^2 + 274X - 120.$$

Déterminer les entiers $(d_n)_{0 \leq n \leq 5}$ tels que $P = \sum_{n=0}^{5} d_n \Gamma_n$. Montrer que P est scindé sur $\mathbb{Q}$.

B - IV. 2. Pour $m > 0$ arbitraire, déterminer les zéros du polynôme

$$P = \sum_{n=0}^{m} (-1)^n \Gamma_n.$$

En déduire la décomposition de P en produit de polynômes irréductibles sur $\mathbb{Q}$. Exprimer P à l'aide du seul polynôme Γ_m.

C - ETUDE DE $\mathcal{P}(E, \mathbb{Z}_{(p)})$

Dans toute cette partie, p désigne un nombre premier fixé.

C - I. 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 : $k + (+\infty) = (+\infty) + k = +\infty$ et $k \leq +\infty$ pour tout k de $\mathbb{Z} \cup \{+\infty\}$.

C - I. 2. Montrer que :
(i) L'application v_p est surjective,
(ii) Pour tous x, y de $\mathbb{Q}$, $v_p(xy) = v_p(x) + v_p(y)$,
(iii) Pour tous x, y de $\mathbb{Q}$, $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$.

C - I. 3. Que vaut $v_p(1)$? Que vaut $v_p(-1)$? Pour tout (x, y) de $\mathbb{Q} \times \mathbb{Q}^*$, exprimer $v_p\left(\frac{x}{y}\right)$ en fonction de $v_p(x)$ et $v_p(y)$.

C - I. 4. Vérifier que $\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \mid v_p(x) \geq 0\}$ et que $\mathbb{Z}_{(p)}$ est un sous-anneau de $\mathbb{Q}$. Caractériser les éléments inversibles de $\mathbb{Z}_{(p)}$ à l'aide de v_p.

C - I. 5. i. Montrer que, pour (k, n) dans $\mathbb{N}^* \times \mathbb{N}^*$, le cardinal de l'ensemble $\{j \in \mathbb{N} \mid 1 \leq j \leq n,\ v_p(j) = k\}$ est égal à $\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]$.
C - I. 5. ii. Justifier la formule suivante due à Legendre :

$$\forall n \in \mathbb{N}, \quad v_p(n!) = \sum_{k>0} \left[\frac{n}{p^k}\right].$$

Dans la suite de cette partie, E désigne une partie infinie de $\mathbb{Z}$.

C - II. 1. Montrer que

$$\mathbb{Z} = \cap_{l \in \mathbb{P}} \mathbb{Z}_{(l)}$$

C - II. 2. Vérifier que

$$\mathcal{P}(E, \mathbb{Z}) = \cap_{l \in \mathbb{P}} \mathcal{P}(E, \mathbb{Z}_{(l)}).$$

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

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

C - III. 1. Dans cette question uniquement, on suppose que $p = 3$, $E = \{1\} \cup \{3k \mid k \in \mathbb{N}\}$ et $(u_n)_{n \in \mathbb{N}}$ est une suite 3-ordonnée de E où $u_0 = 0$. Quelles sont les valeurs possibles pour u_1 et u_2 ?

C - III. 2. Montrer que si $E = \mathbb{Z}$, la suite $(n)_{n \in \mathbb{N}}$ est p-ordonnée.

C - III. 3. Montrer par récurrence que, pour tout a dans E, il existe au moins une suite $(u_n)_{n \in \mathbb{N}}$, p-ordonnée dans E et vérifiant $u_0 = a$. Y a-t-il en général unicité d'une telle suite ?

C - IV. *Dans cette question, on considère une suite* $(u_n)_{n\in\mathbb{N}}$ *p-ordonnée dans* E. On lui associe la suite de polynômes $(P_n)_{n\in\mathbb{N}}$ définie par :

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

C - IV. 1. i. Montrer que les polynômes P_n appartiennent à $\mathcal{P}(E,\mathbb{Z}_{(p)})$.

C - IV. 1. ii. Montrer que, pour tout entier naturel m, la famille $(P_n)_{0\leq n\leq m}$ est une base de l'espace vectoriel réel $\mathbb{R}_m[X]$.

C - IV. 1. iii. Préciser les valeurs $P_n(u_k)$ pour n dans $\mathbb{N}$ et $0\leq k\leq n$.

Dans la suite de cette partie, m désigne un entier naturel et P un élément de $\mathbb{R}_m[X]$. Ecrivons :

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

C - IV. 2. 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) $P(u_0),\ P(u_1),\ldots,P(u_m)\in\mathbb{Z}_{(p)}$.

C - IV. 3. 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 à $\mathbb{Z}_{(p)}$. Vérifier que $\mathcal{P}(E,\mathbb{Z}_{(p)})$ est un sous-anneau de $\mathbb{Q}[X]$.

D - Caractérisation de $\mathcal{P}(\mathbb{N}\setminus p\mathbb{N},\mathbb{Z}_{(p)})$

Dans toute cette partie, p désigne un nombre premier.

On note $p\mathbb{N}$ l'ensemble des entiers naturels multiples de p et $\mathbb{N}\setminus p\mathbb{N}$ l'ensemble des entiers naturels non multiples de p. Pour tout entier naturel n, on pose :

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

D - I. 1. A l'aide de la division euclidienne par $p-1$, montrer que :

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

D - I. 2. En déduire que :
(i) φ_p n'est autre que la bijection croissante de $\mathbb{N}$ sur $\mathbb{N}\setminus p\mathbb{N}$,
(ii) pour tout entier naturel n, $v_p(\varphi_p(n)!)=\omega_p(n)$.

(Pour cette dernière question, on pourra utiliser en le justifiant le fait que, pour x dans $\mathbb{R}$, a et b dans $\mathbb{N}^*$, on a $\left[\frac{x}{ab}\right]=\left[\frac{\left[\frac{x}{a}\right]}{b}\right]$.)

D - I. 3. Vérifier que pour n entier naturel :
(i) $\omega_p(n) \leq 2n$,
(ii) si $n < p-1$, alors $\omega_p(n) = 0$.

D - II. 1. Montrer que, pour (r,s) dans $p\mathbb{N} \times \mathbb{N}$, $v_p(r - \varphi_p(s)) = 0$.

D - II. 2. Justifier, pour $n > 0$, les égalités :

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

D - II. 3. Justifier, pour $0 < n \leq s$, les égalités :

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

D - II. 4. En déduire que la suite $(\varphi_p(n))_{n\in\mathbb{N}}$ est une suite p-ordonnée dans $\mathbb{N} \setminus p\mathbb{N}$.

D - III. *Soit P un élément de $\mathbb{R}_m[X]$.*

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

D - III. 2. Montrer que si P appartient à $\mathcal{P}(\mathbb{N}\setminus p\mathbb{N}, \mathbb{Z}_{(p)})$ alors les coefficients de $p^{\omega_p(m)}P$ sont dans $\mathbb{Z}_{(p)}$.

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

E - I. Montrer successivement que :
(i) $\frac{X(X-1)(X-2)(X-3)}{24} \in \mathcal{P}(\mathbb{P}, \mathbb{Z})$,
(ii) $\frac{(X-1)(X-2)(X-3)}{24} \in \mathcal{P}(\mathbb{P}, \mathbb{Z})$,
(iii) $\mathcal{P}(\mathbb{Z}, \mathbb{Z}) \neq \mathcal{P}(\mathbb{P}, \mathbb{Z})$.

E - II. *Dans cette question p désigne un nombre premier fixé.*
On utilise le théorème de Dirichlet suivant (que l'on ne cherchera pas à démontrer) :
Si a et b sont deux entiers naturels premiers entre eux, alors il existe au moins un entier naturel k tel que $a + bk$ soit un nombre premier.

E - II. 1. *Soit Q un élément de $\mathcal{P}(\mathbb{P}, \mathbb{Z}_{(p)})$.*
Soit α un entier naturel tel que les coefficients de $p^\alpha Q$ appartiennent à $\mathbb{Z}_{(p)}$.

E - II. 1. i. Soit a un entier naturel. Montrer que, pour tout entier relatif k, $Q(a + kp^\alpha) - Q(a)$ appartient à $\mathbb{Z}_{(p)}$.

E - II. 1. ii. Soit a un élément de $\mathbb{N} \setminus p\mathbb{N}$. Montrer qu'il existe un entier naturel k tel que $Q(a + kp^\alpha)$ appartienne à $\mathbb{Z}_{(p)}$.

E - II. 1. iii. En déduire que Q appartient à $\mathcal{P}(\mathbb{N} \setminus p\mathbb{N}, \mathbb{Z}_{(p)})$.

E - II. 2. Pour tout nombre premier l, on pose $E_l = \{l\} \cup (\mathbb{N} \setminus l\mathbb{N})$.

E - II. 2. i. Montrer l'inclusion $\mathbb{P} \subset E_p$.

E - II. 2. ii. En déduire que :

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

E - II. 2. iii. A l'aide de C - II. 2, montrer que :

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

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

E - III. Montrer que si Q est un élément de $\mathcal{P}(\mathbb{P}, \mathbb{Z})$ de degré $\leq m$ alors $X^{2m}Q(X)$ appartient à $\mathcal{P}(\mathbb{Z}, \mathbb{Z})$.
(On pourra utiliser E - II. 1. iii ; D - III. 2 ; D - I. 3. i ; C - II. 1 et B - III.)

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

$$\forall k \in \mathbb{N} \left((1 \leq k \leq 2m+1) \Rightarrow (k^{2m}Q(k) \in \mathbb{Z}) \right).$$

E - IV. 1. A l'aide de D - III. 1, montrer que :

$$\forall p \in \mathbb{P} \quad Q \in \mathcal{P}(\mathbb{N} \setminus p\mathbb{N}, \mathbb{Z}_{(p)}).$$

E - IV. 2. A l'aide de D - III. 2 et D - I. 3. ii, montrer que :

$$\forall p \in \mathbb{P} \left((p > m+1) \Rightarrow Q(p) \in \mathbb{Z}_{(p)} \right).$$

E - V. *Caractérisation de $\mathcal{P}(\mathbb{P}, \mathbb{Z})$.*
Soit Q un élément de $\mathbb{R}_m[X]$. Montrer que les deux assertions suivantes sont équivalentes :
(a) Q appartient à $\mathcal{P}(\mathbb{P}, \mathbb{Z})$,
(b) Pour tout nombre premier $p \leq m+1$, $Q(p)$ appartient à $\mathbb{Z}$,
et, pour tout entier naturel $k \leq 2m+1$, $k^{2m}Q(k)$ appartient à $\mathbb{Z}$.

E - VI. Appliquer la caractérisation précédente pour prouver :
quel que soit le nombre premier p, on a la congruence suivante

$$(p+1)(p-1)(p-2)(p-3)(p-5)(p-7)(p-193) \equiv 0 \pmod{2\,903\,040}.$$