Canad. Math. Bull. Vol. **39** (4), 1996 pp. 402–407

UNE CARACTÉRISATION DES POLYNÔMES PRENANT DES VALEURS ENTIÈRES SUR TOUS LES NOMBRES PREMIERS

JEAN-LUC CHABERT

RÉSUMÉ. Nous donnons une caractérisation des polynômes à coefficients rationnels prenant des valeurs entières sur tous les nombres premiers: pour tester un polynôme donné de degré n, il suffit de considérer ses valeurs sur les entiers de 1 à $2n-1$.

ABSTRACT. We give a characterization of polynomials with rational coefficients which take integral values on the prime numbers: to test a polynomial of degree n, it is enough to consider its values on the integers from 1 to $2n-1$.

NOTATIONS. Pour toute partie E de $\mathbb{Z}$ et tout sous-anneau A de $\mathbb{Q}$, nous notons $\mathrm{Int}(E,A)$ la A-algèbre formée des polynômes prenant sur E leurs valeurs dans A (*cf.* [1]), c'est-à-dire :

$$\mathrm{Int}(E,A) = \{f(X) \in \mathbb{Q}[X] \mid f(k) \in A \text{ pour tout } k \in E\}.$$

En particulier, $\mathrm{Int}(\mathbb{Z},\mathbb{Z})$ correspond à l'anneau bien connu, noté $\mathrm{Int}(\mathbb{Z})$, des polynômes à valeurs entières sur $\mathbb{Z}$ (*cf.* par exemple [3]).

Désignant par $\mathcal{P}$ l'ensemble des nombres premiers, nous nous intéressons ici à l'anneau $\mathrm{Int}(\mathcal{P},\mathbb{Z}) = \{f(x) \in \mathbb{Q}[X] \mid f(\mathcal{P}) \subset \mathbb{Z}\}$ des polynômes à valeurs entières sur les nombres premiers.

Il est classique qu'un polynôme $f(x)$ de degré n est à valeurs entières sur les entiers, c'est-à-dire appartient à $\mathrm{Int}(\mathbb{Z})$, si et seulement si $f(0), f(1), \ldots, f(n)$ sont des entiers. Cela résulte notamment de ce que les polynômes $\binom{X}{n} = \frac{X(X-1)\cdots(X-n+1)}{n!}$ forment une base du $\mathbb{Z}$-module $\mathrm{Int}(\mathbb{Z})$ et qu'ils vérifient $\binom{k}{n} = 0$ pour $0 \leq k < n$ et $\binom{n}{n} = 1$.

Notons que $\mathrm{Int}(\mathcal{P},\mathbb{Z})$ contient strictement $\mathrm{Int}(\mathbb{Z})$: considérer le polynôme $\frac{(X-1)(X-2)(X-3)}{24}$. Rappelons aussi que $\mathrm{Int}(\mathcal{P},\mathbb{Z})$ est un $\mathbb{Z}$-module libre dont on sait construire une base $\left(C_n(X)\right)_{n\in\mathbb{N}}$ où $\deg(C_n) = n$ (*cf.* [2]). Toutefois il n'existe pas de base de $\mathrm{Int}(\mathcal{P},\mathbb{Z})$ possédant une propriété analogue à celle de la base $\left(\binom{X}{n}\right)_{n\in\mathbb{N}}$ de $\mathrm{Int}(\mathbb{Z})$, sauf en ce qui concerne les petits degrés car on peut choisir pour premiers éléments de la base les polynômes

$$C_0 = 1,\ C_1 = X-1,\ C_2 = \frac{(X-1)(X-2)}{2} \text{ et } C_3 = \frac{(X-1)(X-2)(X-3)}{24},$$

Reçu par les éditeurs le September 27, 1995.
Classification (AMS) par sujet : Primary: 11C08; Secondary: 11A41, 11Y16.

et on a donc

$$C_0(1) = C_1(2) = C_2(3) = C_3(5) = 1.$$

Ainsi, en posant $p_0 = 1$, $p_1 = 2$, $p_2 = 3$ et $p_3 = 5$, on voit qu'un polynôme $f(X)$ de degré $n \leq 3$ appartient à $\mathrm{Int}(\mathcal{P}, \mathbb{Z})$ si et seulement si $f(p_k)$ appartient à $\mathbb{Z}$ pour $0 \leq k \leq n$.

Essayer cependant d'utiliser une base pour tester l'appartenance à $\mathrm{Int}(\mathcal{P}, \mathbb{Z})$ d'un polynôme $f(X)$ de degré élevé risque d'être très long car, d'une part la construction de la base $\big(C_n(X)\big)$ nécessite un calcul pour chaque degré n, calcul qui s'avère n'être ni récurrent, ni récursif, d'autre part le calcul des coefficients de $f(X)$ dans cette base serait vite fastidieux.

Nous montrons toutefois dans cet article que, pour savoir si un polynôme de degré n est à valuers entières sur les nombres premiers, il suffit de calculer au plus $2n$ valeurs de ce polynôme. Très précisément :

1. THÉORÈME. *Un polynôme $f(X)$ à coefficients rationnels de degré $n > 0$ est à valeurs entières sur les nombres premiers si et seulement si :*

(i) pour tout nombre premier $p \leq n + 1$, $f(p)$ est un entier,

(ii) pour tout entier naturel $h \leq 2n - 1$, $h^{2n-5} f(h)$ est un entier.

La démonstration de ce théorème nécessite un certain nombre de résultats préliminaires. Rappelons tout d'abord une conséquence du théorème de Dirichlet sur les nombres premiers.

2. PROPOSITION [2]. *Soient $f \in \mathrm{Int}(\mathcal{P}, \mathbb{Z})$, $p \in \mathcal{P}$ et $h \in \mathbb{Z}$. Si p ne divise pas h, alors p ne divise pas le dénominateur de $f(h)$. Autrement dit, pour tout nombre premier p, on a :*

$$\mathrm{Int}(\mathcal{P}, \mathbb{Z}) \subset \mathrm{Int}(\mathbb{Z} \setminus p\mathbb{Z}, \mathbb{Z}_{(p)}).$$

En effet, soit v un entier tel que $p^v f(X)$ appartienne à $\mathbb{Z}_{(p)}[X]$ et soit q un nombre premier apparaissant dans la suite $(h + np^v)_{n \in \mathbb{N}}$. Alors $p^v\big(f(h) - f(q)\big) \in (h - q)\mathbb{Z}_{(p)} \subset p^v\mathbb{Z}_{(p)}$ et donc $f(h) \in \mathbb{Z}_{(p)}$.

3. PROPOSITION. *Pour tout $p \in \mathcal{P}$, $\mathrm{Int}(\mathcal{P}, \mathbb{Z}_{(p)}) = \mathrm{Int}\big(\{p\} \cup (\mathbb{Z} \setminus p\mathbb{Z}), \mathbb{Z}_{(p)}\big)$.*

En effet, $\mathcal{P} \subset \{p\} \cup (\mathbb{Z} \setminus p\mathbb{Z})$.

On a par ailleurs la formule immédiate :

$$\mathrm{Int}(\mathcal{P}, \mathbb{Z}) = \cap_{p \in \mathcal{P}} \mathrm{Int}(\mathcal{P}, \mathbb{Z}_{(p)}).$$

NOTATION. Désormais, sauf mention contraire, p désigne un nombre premier fixé et ν_p la valuation associée. Pour tout entier $k \geq 1$, posons $u_k = k + [\frac{k-1}{p-1}]$. La suite (u_k) est alors la suite croissante des entiers naturels non multiples de p et on a $\mathbb{Z} \setminus p\mathbb{Z} = \{\pm u_k \mid k \in \mathbb{N}^*\}$.

https://doi.org/10.4153/CMB-1996-048-7 Published online by Cambridge University Press

4. LEMME. *Pour tout $n \in \mathbb{N}^*$ et pour tout $m \in \mathbb{Z} \setminus p\mathbb{Z}$, on a :*

$$v_p\Big(\prod_{1\le k\le n}(m-u_k)\Big) \ge v_p\Big(\prod_{1\le k\le n}(u_{n+1}-u_k)\Big) = \sum_{s\ge 0}\Big[\frac{n}{p^s(p-1)}\Big].$$

DÉMONSTRATION. Comme $v_p(u_{n+1}) = 0$, en ajoutant des termes, on obtient

$$v_p\Big(\prod_{1\le k\le n}(u_{n+1}-u_k)\Big) = v_p\Big(\prod_{0\le k<u_{n+1}}(u_{n+1}-k)\Big) = v_p\big((u_{n+1})!\big).$$

De même,

$$v_p\Big(\prod_{1\le k\le n}(m-u_k)\Big) = v_p\Big(\prod_{0\le k<u_{n+1}}(m-k)\Big) = v_p\Big(\frac{m!}{(m-u_{n+1})!}\Big).$$

L'inégalité résulte alors de ce que $\binom{m}{u_{n+1}} \in \mathbb{Z}$.

Pour l'égalité, on sait que

$$v_p\big((u_{n+1})!\big) = \sum_{s\ge 1}\Big[\frac{u_{n+1}}{p^s}\Big];$$

il suffit donc de vérifier que

$$\Big[\frac{u_{n+1}}{p}\Big] = \Big[\frac{n}{p-1}\Big],$$

puisqu'on aura alors

$$\Big[\frac{u_{n+1}}{p^s}\Big] = \Big[\frac{n}{p^{s-1}(p-1)}\Big].$$

Soient q et r tels que

$$n = q(p-1) + r \text{ avec } 0 \le r < p-1.$$

Alors

$$u_{n+1} = n + 1 + \Big[\frac{n}{p-1}\Big] = qp + (r+1) \text{ avec } 1 \le r+1 < p.$$

NOTATION. Pour tout entier $n \ge 0$, posons $\omega_p(n) = \sum_{s\ge 0}[\frac{n-1}{p^s(p-1)}]$.

Cette fonction $\omega_p(n)$ rappelle la fonction $w_p(n) = \sum_{s\ge 1}[\frac{n}{q^s}]$ qui intervient dans la détermination des polynômes à valeurs entières sur un corps de nombres (*cf.* [4] et [5]).

Posons aussi $D_0(X) = 1$ et, pour $n \ge 1$:

$$D_n(X) = p^{-\omega_p(n+1)} \prod_{1\le k\le n}(X-u_k).$$

Il résulte du Lemme 4 que les polynômes $D_n(X)$ appartiennent à $\mathrm{Int}(\mathbb{Z}\setminus p\mathbb{Z}, \mathbb{Z})$ et qu'ils forment une base du $\mathbb{Z}_{(p)}$-module $\mathrm{Int}(\mathbb{Z}\setminus p\mathbb{Z}, \mathbb{Z}_{(p)})$. En effet, pour $k = 1, \dots, n$, $D_n(u_k) = 0$ et $D_n(u_{n+1})$ est inversible dans $\mathbb{Z}_{(p)}$. Par suite :

5. LEMME. *(i) Un polynôme $f(X) \in \mathbb{Q}[X]$ de degré n appartient à* $\mathrm{Int}(\mathbb{Z} \setminus p\mathbb{Z}, \mathbb{Z}_{(p)})$ *si et seulement si $f(u_k) \in \mathbb{Z}_{(p)}$ pour $k = 1, \ldots, n+1$.*

(ii) Si un polynôme $f(X) \in \mathbb{Q}[X]$ de degré n appartient à $\mathrm{Int}(\mathbb{Z} \setminus p\mathbb{Z}, \mathbb{Z}_{(p)})$, *alors $p^{\omega_p(n+1)} f(X)$ appartient à $\mathbb{Z}_{(p)}[X]$.*

De façon analogue, considérons les polynômes $C_0(X) = 1$ et, pour $n \geq 1$:

$$C_n(X) = (X - p)D_{n-1}(X).$$

Les polynômes $C_n(X)$ appartiennent à $\mathrm{Int}(\mathcal{P}, \mathbb{Z})$ et forment une base du $\mathbb{Z}_{(p)}$-module $\mathrm{Int}\big(\{p\} \cup (\mathbb{Z} \setminus p\mathbb{Z}), \mathbb{Z}_{(p)}\big)$ (*cf.* aussi [2]). Par suite, compte tenu de la Proposition 3 :

6. LEMME. *(i) Un polynôme $f(X) \in \mathbb{Q}[X]$ de degré n appartient à* $\mathrm{Int}(\mathcal{P}, \mathbb{Z}_{(p)})$ *si et seulement si $f(p) \in \mathbb{Z}_{(p)}$ et $f(u_k) \in \mathbb{Z}_{(p)}$ pour $k = 1, \ldots, n$.*

(ii) Si un polynôme $f(X) \in \mathbb{Q}[X]$ de degré n appartient à $\mathrm{Int}(\mathcal{P}, \mathbb{Z}_{(p)})$, *alors $p^{\omega_p(n)} f(X)$ appartient à $\mathbb{Z}_{(p)}[X]$.*

Il nous faut maintenant majorer la quantité $\omega_p(n)$.

7. LEMME. *Pour tout entier $n \geq 1$, on a :*

$$\omega_p(n) \leq \frac{(n-1)p}{(p-1)^2} - \frac{1}{p-1}.$$

En particulier, pour $n \geq 3$, $\omega_2(n) \leq 2n - 3$ et, pour tout $p \geq 3$, $\omega_p(n) \leq 2n - 5$.

DÉMONSTRATION. On a

$$\begin{aligned}\omega_p(n) &= \sum_{s \geq 0} \left[\frac{n-1}{p^s(p-1)}\right] \\ &= \sum_{0 \leq s \leq r} \left[\frac{n-1}{p^s(p-1)}\right]\end{aligned}$$

où r vérifie

$$p^r \leq \frac{n-1}{p-1} < p^{r+1}.$$

Alors

$$\begin{aligned}\omega_p(n) &\leq \frac{n-1}{p-1} \sum_{0 \leq s \leq r} \frac{1}{p^s} \\ &\leq \frac{n-1}{(p-1)^2}\left(p - \frac{p-1}{n-1}\right) \\ &= \frac{(n-1)p}{(p-1)^2} - \frac{1}{p-1}.\end{aligned}$$

En particulier, pour $p = 2$,

$$\omega_2(n) \leq 2n - 3,$$

https://doi.org/10.4153/CMB-1996-048-7 Published online by Cambridge University Press

et, pour $p \geq 3$,

$$\begin{aligned}\omega_p(n) &\leq \omega_3(n)\\ &\leq \frac{3}{4}(n-1)-\frac{1}{2}\\ &\leq 2n-5.\end{aligned}$$

8. PROPOSITION. *Soit $f(X)$ un polynôme de degré $n \geq 3$. Si $f(X)$ appartient à* $\mathrm{Int}(\mathcal{P},\mathbb{Z})$, *alors $X^{2n-5}f(X)$ appartient à* $\mathrm{Int}(\mathbb{Z})$.

DÉMONSTRATION. Soit $h \in \mathbb{Z}$. Il suffit de montrer que, pour tout $p \in \mathcal{P}$, $h^{2n-5}f(h)$ appartient à $\mathbb{Z}_{(p)}$. Soit p fixé dans $\mathcal{P}$. Si p ne divise pas h alors $f(h)$ appartient à $\mathbb{Z}_{(p)}$ (Proposition 2). Tandis que si p divise h, on a $v_p(h) \geq 1$ et par suite $v_p\big(h^{2n-5}f(h)\big) \geq 2n-5-\omega_p(n)$ (Lemme 6). De sorte que, si $p \neq 2$, on a bien $v_p\big(h^{2n-5}f(h)\big) \geq 0$ (Lemme 7).

Considérons donc le seul cas où l'on ne peut conclure, celui où $v_2(h) \geq 1$ et $v_2\big(f(h)\big) < 0$. Posons $f(X)-f(2) = (X-2)g(X)$; on sait que $2^{2n-3}f(X) \in \mathbb{Z}_{(2)}[X]$ (Lemmes 6 et 7), donc $2^{2n-3}g(X) \in \mathbb{Z}_{(2)}[X]$ puisque $f(2) \in \mathbb{Z}$. Enfin, comme $v_2\big(f(h)\big) = v_2\big((h-2)g(h)\big)$ et que $v_2\big(h(h-2)\big) \geq 3$, on a bien :

$$\begin{aligned}v_2\big(h^{2n-5}f(h)\big) &\geq 2n-6+v_2\big(hf(h)\big)\\ &\geq 2n-6+v_2\big(h(h-2)\big)+v_2\big(g(h)\big)\\ &\geq 0.\end{aligned}$$

Par exemple, $\frac{(X-1)(X-2)(X-3)}{24}$ appartient à $\mathrm{Int}(\mathcal{P},\mathbb{Z})$ et n'appartient pas à $\mathrm{Int}(\mathbb{Z})$, tandis que $X\cdot\frac{(X-1)(X-2)(X-3)}{24} = \binom{X}{4}$ appartient à $\mathrm{Int}(\mathbb{Z})$.

La Proposition 8 met en particulier en évidence le fait qu'un élément de $\mathrm{Int}(\mathcal{P},\mathbb{Z})$ prend toujours des valeurs entières pour $X = +1$ et $X = -1$ (ce qui en fait était clair dès la Proposition 2).

DÉMONSTRATION DU THÉORÈME 1. Les cas $n = 1$ ou 2 se vérifiant "à la main", on suppose $n \geq 3$. La condition est nécessaire : (i) est évident, (ii) est une conséquence de la Proposition 8. Inversement, supposons que $f(X)$ vérifie (i) et (ii) et montrons que, pour tout $p \in \mathcal{P}$, $f(X)$ appartient à $\mathrm{Int}(\mathcal{P},\mathbb{Z}_{(p)})$.

Premier cas : $p \leq n+1$. Alors, pour $k = 1,\ldots,n$, $u_k = k+[\frac{k-1}{p-1}] \leq n+[\frac{n-1}{p-1}] \leq 2n-1$. Donc, d'aprés (ii), $u_k^{2n-5}f(u_k) \in \mathbb{Z}$ et par suite $f(u_k) \in \mathbb{Z}_{(p)}$ puisque p ne divise pas u_k. D'après (i), $f(p) \in \mathbb{Z}$ et donc $f(X) \in \mathrm{Int}(\mathcal{P},\mathbb{Z})_{(p)})$ (Lemme 6).

Second cas : $p > n+1$. Alors, pour $k = 1,\ldots,n+1$, $u_k \leq n+1+[\frac{n}{p-1}] = n+1$. Donc, là encore, $f(u_k) \in \mathbb{Z}_{(p)}$ et $f(X) \in \mathrm{Int}(\mathbb{Z}\setminus p\mathbb{Z},\mathbb{Z}_{(p)})$ (Lemme 5). Par suite, $p^{\omega_p(n+1)}f(X) \in \mathbb{Z}_{(p)}[X]$; mais $\omega_p(n+1) = 0$, donc $f(X) \in \mathbb{Z}_{(p)}[X]$.

REMARQUES. 1° La preuve précédent montre que la condition (ii) du Théorème 1 peut être remplacée par la condition plus faible :

(ii bis) pour tout entier naturel $h \leq 2n-1$, il existe un entier naturel v tel que $h^v f(h)$ soit un entier (referee's remark).

L'exposant explicite $2n-5$ confère cependant un caractère algorithmique à la caractérisation donnée par le Théorème 1.

2° Les quantités $n+1$, $2n-5$ et $2n-1$ intervenant dans l'énoncé du Théorème 1 sont optimales.

(a) On ne peut remplacer $2 \leq p \leq n+1$ par $2 \leq p \leq n$ dans la condition (i) : le polynôme $f(X) = \frac{(X-1)(X-2)(X-3)(X-4)}{5}$ vérifie $f(2) = f(3) = 0$ et $X \cdot f(X) \in \mathrm{Int}(\mathbb{Z})$, alors que $f(5) \notin \mathbb{Z}$.

(b) On ne peut diminuer l'exposant $2n-5$ dans la condition (ii) : soit $n = 2^k+1$, alors $f(X) = \frac{1}{2^{2n-3}}(X-2)\prod_{1\leq k\leq n-1}\big(X-(2k+1)\big)$ appartient à $\mathrm{Int}(\mathcal{P}, \mathbb{Z})$ (Lemme 6), tandis que $2^{2n-5}f(6)$ est impair.

(c) On ne peut remplacer $h \leq 2n-1$ par $h < 2n-1$ dans la condition (ii) : le polynôme $f(X) = \frac{(X-1)(X-2)(X-3)(X-5)}{2^5 \cdot 3}$ vérifie $f(2) = f(3) = f(5) = 0$ et $h^3 f(h) \in \mathbb{Z}$ pour $1 \leq h \leq 6$, mais $f(7) \notin \mathbb{Z}$.

3° En revanche, il est possible de diminuer le nombre de valeurs à calculer en différenciant les nombres premiers. Par exemple, en faisant jouer à $p = 2$ un rôle particulier, la condition (ii) peut être remplacée par la condition plus faible :

(ii ter) pour tout $h \in \mathbb{N}$ vérifiant soit $h < \frac{3}{2}n$, soit h est impair et $\frac{3}{2}n \leq h < 2n$, on a $h^{2n-5}f(h) \in \mathbb{Z}$.

En effet, dans la preuve du Théorème 1, si $p > n+1$, il n'y a rien à changer. Si $3 \leq p \leq n+1$, la preuve marche encore car, pour $k \leq n$, $u_k = k + [\frac{k-1}{p-1}] \leq n + [\frac{n-1}{2}] < \frac{3}{2}n$. Enfin, si $p = 2$, la preuve marche toujours car on utilise seulement les valeurs $f(u_k)$ où u_k est impair.

On peut se poser la question d'une estimation asymptotique du nombre minimal de valeurs à calculer. Cet article montre que ce nombre est compris entre $n+1$ et $2n-1$.

RÉFÉRENCES

1. P.-J. Cahen, *Integral-valued polynomials on a subset*, Proc. Amer. Math. Soc. **117**(1993), 919–929.
2. J.-L. Chabert, S. Chapman, W. Smith, *A basis for the ring of polynomials integer-valued on prime numbers*, à paraître.
3. R. Gilmer, *Sets that determine integer-valued polynomials*, J. Number Theory **33**(1989), 95–100.
4. A. Ostrowski, *Ueber ganzwertige Polynome in algebraischen Zahlkörpern*, J. Reine Angew. Math. **149** (1919), 117–124.
5. G. Pólya, *Ueber ganzwertige Polynome in algebraischen Zahlkörpern*, J. Reine Angew. Math. **149**(1919), 97–116.

Département de Mathématiques
Institut Supérieur des Sciences et Techniques de St. Quentin
Université de Picardie
48, rue Raspail
02109 St. Quentin, France
e-mail: jean-luc.chabert@u-picardie.fr