Conditions multiplicatives sur l'ensemble des valeurs d'un polynôme

MAURICE MIGNOTTE

Centre scientifique, Saint-Denis, France

Introduction

Soit P un polynôme unitaire sur $\mathbf{Z}$ de degré $d \geq 1$. On désigne par E l'ensemble des valeurs $P(x)$ quand x parcourt $\mathbf{Z}$.

On s'intéresse d'abord à la condition suivante

M1: E est stable par multiplication.

Si on choisit x dans E et si M1 est vérifiée, E contient toutes les puissances de x. Ceci amène à envisager la condition suivante

M2: E contient toutes les puissance d'un même nombre x telque $|x| > 1$.

On peut encore affaiblir cette condition en

M3: E contient une infinité de puissances d'un même nombre g tel que $|g| > 1$.

A ce stade, il se pose les problèmes suivants: trouver les polynômes unitaires qui vérifient les conditions Mi, les conditions Mi sont-elles équivalentes?

Nous nous proposons de résoudre ces deux problèmes.

Préliminaires

Pour p premier et a entier, soit h tel que $p^h | a$ et $p^{h+1} X a$, on pose $|a|_p = p^{-h}$.

Soit $g = \pm p_1^{e_1} \ldots p_r^{e_r}$ la décomposition de g en facteurs premiers. Pour a entier, on pose

$$|a|_g = \max\left(|a|_{p_1}^{1_1}, \ldots, |a|_{p_r}^{1_r}\right)$$

où

$$1_i = \log(g)(e_i \log p_i)^{-1}, \qquad i = 1, \ldots, r.$$

En particulier, pour n entier, on a

$$|g^n|_g = g^{-n}. \tag{1}$$

Si la condition M3 a lieu, soit (x_k) une suite infinie d'entiers tels que

$$P(x_k) = g^{n_k}, \quad k = 1, \ldots, r, \ldots$$

D'après (1), l'égalité précédente implique $|P(x_k)|_g = g^{-n_k}$. De plus, si $|x|$ tend vers l'infini, on a bien sûr $P(x) \sim x^d$. Il en résulte que $|x_k^d| \geq \frac{1}{2}|g^{n_k}|$ si k assez grand. La condition M3 implique donc

M3′: Il existe une constante $c > 0$ et une suite infinie (x_k) d'entiers tels que

$$P(x_k)_g \leq c x_k^{-d}, \quad k = 1, 2, \ldots$$

On peut encore affaiblir cette condition en

M4: Il existe deux constantes c et h, $c > 0$ et $h > d - 1$ et une suite infinie (x_k) d'entiers tels que $|P(x_k)|_g \leq c|x_k|^{-h}$.

On utilisera le résultat suivant ([1], p. 158).

LEMME. *Soit* $z = (z_1, \ldots, z_r)$ *avec* $z_1 \neq 0, \ldots, z_r \neq 0$ *un entier algébrique g-adique. S'il existe deux constantes positives* c *et* h *et une suite infinie* (x_k) *d'entiers tels que pour tout* k *on ait* $|z - x_k|_g \leq c x_k^{-h}$ *alors* $h \leq 1$.

Caractérisation des polynômes qui vérifient M4

Désignons par K_i la clôture algébrique de $\mathbf{Q}_{p_i}$ pour $i = 1, \ldots, r$. Considérons d'abord le cas où P a au moins deux zéros distincts dans chacun des K_i. La condition M4 implique

$$\lim_{k \to \infty} |P(x_k)|_{p_i} = 0, \quad i = 1, \ldots, r.$$

On en déduit facilement l'existence d'une sous-suite de (x_k) (encore notée (x_k)), d'une racine z_i de P dans K_i et d'une constante $c' > 0$ tels que

$$|x_k - z_i|_{p_i}^{(d-1)} \leq c' |P(x_k)|_{p_i}, \quad i = 1, \ldots, r.$$

Si on désigne par g le nombre g-adique $z = (z_1, \ldots, z_r)$, c'est un zéro de $P(x)$. De plus, on a $|x_k - z|_g^{d-1} \leq c''|P(x_k)|_g$. D'après M4, il vient

$$|x_k - z|_g = C|x_k|^{-t} \tag{2}$$

avec $C = cc''$ et $t = h/(d-1) > 1$. Quitte à faire une translation, on peut supposer $P(0) \neq 0$ et donc $z_i \neq 0$ pour $i = 1, \ldots, r$. Dans ces conditions, le lemme s'applique et (2) est impossible pour k assez grand. Contradiction.

Reste le cas où P se décompose en une puissance d'un polynôme linéaire dans K_1 par exemple. Ceci impose d'abord à P d'être égal à la puissance d'un polynôme irréductible dans $\mathbf{Z}[X]$. On peut se ramener au cas où P est irréductible dans $\mathbf{Z}$. Dans ce cas, P a des racines distinctes dans $\mathbf{C}$, donc le discriminant D de P

est non nul. Mais D est calculé dans $\mathbf{Z}$ et c'est aussi le discriminant de P en tant que polynôme dans K_1, par suite P n'a pas de racines multiples dans K_1 et donc P est linéaire. Réciproquement, il est clair que si P est une puissance d'un polynôme linéaire, il vérifie M1.

Ainsi, nous avons démontré le résultat suivant

THÉOREME. *Soit P un polynôme unitaire de $\mathbf{Z}[X]$, alors les conditions suivantes sont équivalentes*

M1: *L'ensemble E des valeurs de P est stable par multiplication.*

M2: *E contient toutes les puissances d'un entier x tel que $|x| > 1$.*

M3: *E contient une infinité de puissances d'un entier g tel que $|g| > 1$.*

M4: *Il existe deux constantes c et h, $c > 0$ et $h > d - 1$, et une suite infinie (x_k) d'entiers tels que $|P(x_k)|_g \leq c|x_k|^{-h}$.*

M5: *P est égal a la puissance d'un polynôme linéaire.*

Remarques:

1) On pourrait généraliser ce résultat au cas où $P \in A[X]$, A étant l'anneau des entiers d'un corps de nombres.

2) Si on se pose le problème additif analogue au précédent, on montre que les conditions suivantes sont équivalentes

A1: E est stable par addition.

A2: E contient tous les multiples d'un nombre $x \neq 0$.

A3: E a une densité non nulle dans $\mathbf{Z}$.

A4: P est un polynôme linéaire.

Il est clair que A4 $\Rightarrow$ A1 $\Rightarrow$ A2 $\Rightarrow$ A3. Pour montrer que A3 $\Rightarrow$ A4, on raisonne par l'absurde: si P est de degré ≥ 2 il est très facile de voir que la densité de E est nulle.

Référence

1. MAHLER, K., *Lectures on diophantine approximations.* Note dame, 1961.

Received February 28, 1972

Maurice Megnotte
Centre scientifique
Place du 8 mai 45
93 Saint-Denis, France