Annales Univ. Sci. Budapest., Sect. Comp. 44 (2015) 183–196

UNE APPLICATION ARITHMÉTIQUE DU THÉORÈME DU QUOTIENT DE HADAMARD

Bruno Langlois (Châtenay-Malabry, France)

Communicated by Imre Kátai
(Received September 10, 2015; accepted December 14, 2015)

Abstract. In 1998, the American Mathematical Monthly journal published a problem [1] that could not be solved by any reader of the journal but the author [2]:

($\mathcal{P}_0$) : Let a, b be natural numbers greater than 1. Suppose that $a^n - 1$ divides $b^n - 1$ for every positive integer n. Prove that $b = a^k$ for some positive integer k.

The author's solution was short and elementary, but the background was not clearly exposed. Today this problem is a classic, especially known by the Mathematical Olympiads' participants.

In this paper, I will generalize the result of ($\mathcal{P}_0$), by examining when we can have $P(a^n, n) \,|\, Q(b^n, n)$ for all n large enough, with a, b in $\mathbb{Z}\backslash\{-1; 0; 1\}$ and $P(X, Y)$, $Q(X, Y)$ in $\mathbb{Z}[X, Y]$.

I will focus on the case where $P = Q$ and thus etablish that:

- If $P(X, Y)$ cannot be written as $P(X, Y) = U(X)V(Y)$, with $(U, V) \in \mathbb{Z}[X] \times \mathbb{Z}[Y]$, and if for all n large enough $P(a^n, n) \,|\, P(b^n, n)$, then $b = \pm a$.
- If $P \in \mathbb{Z}[X]$ is not a monomial and if for all n large enough, $P(a^n) \,|\, P(b^n)$, then there exists $k \in \mathbb{N}^*$ such that $b = \pm a^k$

I will take advantage of the theorem known as *Hadamard Quotient Theorem* concerning linear recurring sequences.

1. Introduction : le Théorème du Quotient de Hadamard

Rappelons brièvement ce que sont les suites récurrentes linéaires et la propriété classique qui les caractérise (pour une introduction aux suites récurrentes linéaires, on peut consulter [3]).

Key words and phrases: Hadamard Quotient Theorem, linear recurring sequences.
2010 Mathematics Subject Classification: 11B99.
https://doi.org/10.71352/ac.44.183

Définition 1. Une suite complexe $(u_n)_{n\geqslant N}$ est dite *récurrente linéaire* lorsqu'il existe un entier $k \geqslant 1$ et des complexes $t_1, \cdots, t_k$ tels que :

$$\forall n \geqslant N,\ u_{n+k} = \sum_{i=0}^{k-1} t_i u_{n+i} \tag{1}$$

Propriété 1. *Une suite complexe $(u_n)_{n\geqslant N}$ non constante égale à 0 est récurrente linéaire si et seulement s'il existe un entier $m \geqslant 1$, des complexes non nuls et deux à deux distincts $\theta_1, \cdots, \theta_m$ et des polynômes non nuls $P_1, \cdots, P_m$ à coefficients complexes tels que :*

$$\forall n \geqslant N,\ u_n = \sum_{j=1}^{m} P_j(n)\theta_j^n \tag{2}$$

Remarque 1. (a) Si (u_n) est une suite vérifiant (1), chaque θ_j est une racine du *polynôme caractéristique* $R = X^k - \sum_{i=0}^{k-1} t_i X^i$. De plus, le degré de chaque P_j est strictement inférieur à la multiplicité de θ_j comme racine de R.

(b) Les suites $(n^p\theta^n)_{n\geqslant N}$, $(p,\theta) \in \mathbb{N}\times\mathbb{C}^*$ formant une famille libre dans le $\mathbb{C}-$espace vectoriel des suites complexes, la décomposition de (u_n) sous la forme (2) est unique, à l'ordre des termes près. J'appellerai celle-ci *forme réduite*.

(c) La remarque précédente entraîne en particulier que si $\theta_1, \cdots, \theta_m$ sont des complexes non nuls et deux à deux distincts et $P_1, \cdots, P_m$ des polynômes à coefficients complexes tels que pour tout $n \geqslant N$, $\sum_{j=1}^{m} P_j(n)\theta_j^n = 0$, alors $P_1 = \cdots = P_m = 0$.

Si (u_n) et (v_n) sont deux suites récurrentes linéaires, la propriété précédente montre que le produit $(u_n v_n)$ donne également une suite récurrente linéaire. En revanche, en général, le quotient $\left(\frac{v_n}{u_n}\right)$ n'est pas une suite récurrente linéaire (considérer par exemple $v_n = 1$ et $u_n = n$), même si, à condition d'ajouter une hypothèse forte, la propriété devient valide :

Théorème du Quotient de Hadamard: *Soient $(u_n)_{n\geqslant N}$ et $(v_n)_{n\geqslant N}$ deux suites complexes récurrentes linéaires, on suppose que pour tout $n \geqslant N$, $u_n \neq 0$ et $\frac{v_n}{u_n} \in \mathbb{Z}$. Alors $\left(\frac{v_n}{u_n}\right)_{n\geqslant N}$ est une suite récurrente linéaire.*

Remarque 2. Ce résultat a été conjecturé par Charles Pisot dans les années 1950 et démontré entièrement par Van der Poorten dans les années 1980, grâce à des arguments pointus d'analyse p-adique (pour un énoncé général accompagné d'une démonstration complète, voir [5]).

Comme me l'a signalé Jean-Paul Bézivin, le théorème précédent permet d'apporter une solution courte au problème $(\mathcal{P}_0)$. Posons en effet $u_n = a^n - 1$ et $v_n = b^n - 1$. Les suites (u_n) et (v_n) étant récurrentes linéaires, le Théorème du Quotient de Hadamard entraîne l'existence d'un $N \in \mathbb{N}$ tel que la suite $\left(\dfrac{b^n-1}{a^n-1}\right)_{n \geqslant N}$ est récurrente linéaire. Il existe donc $m \in \mathbb{N}^*$, des complexes non nuls et deux à deux distincts $\theta_1, \cdots, \theta_m$ (supposons que $|\theta_m| \geqslant \cdots \geqslant |\theta_1|$) et des polynômes non nuls $P_1, \cdots, P_m$ de $\mathbb{C}[X]$ tels que pour tout $n \geqslant N$,

$$\frac{b^n-1}{a^n-1} = \sum_{j=1}^{m} P_j(n)\theta_j^n,$$

d'où pour tout $n \geqslant N$,

$$b^n - 1 = \sum_{j=1}^{m} P_j(n)(a\theta_j)^n - \sum_{j=1}^{m} P_j(n)\theta_j^n.$$

Comme $a > 1$ et $|\theta_m| \geqslant \cdots \geqslant |\theta_1|$, après avoir mis sous forme réduite le membre de droite de l'égalité précédente (voir remarque 1.b), les termes $P_m(n)(a\theta_m)^n$ et $-P_1(n)\theta_1^n$ demeurent intacts, et vu le membre de gauche, ce sont les deux seuls qui restent ; on a donc $a\theta_m = b$ et $\theta_1 = 1$. Les autres termes se sont compensés dans la réduction, ce qui implique en particulier que les ensembles $\{a\theta_1, \cdots, a\theta_{m-1}\}$ et $\{\theta_2, \cdots, \theta_m\}$ sont égaux (dans le cas particulier où $m = 1$, on a simplement $a = b$). On a par conséquent $\prod_{j=1}^{m-1}(a\theta_j) = \prod_{j=2}^{m}\theta_j$, d'où $b = a^m$, ce qui résout le problème $\mathcal{P}_0$.

Dans la suite, nous allons généraliser en appliquant le Théorème du Quotient de Hadamard au cas où $u_n = P(a^n, n)$ et $v_n = Q(b^n, n)$, avec P, Q dans $\mathbb{Z}[X, Y]$ et a, b dans $\mathbb{Z}\backslash\{-1; 0; 1\}$.

2. Généralisation du problème $\mathcal{P}_0$

Dans ce qui suit, si U et V sont dans $\mathbb{Z}[X]$ (resp. $\mathbb{Z}[X, Y]$), j'écrirai $U \mid V$ pour indiquer que U divise V dans $\mathbb{Q}[X]$ (resp. $\mathbb{Q}[X, Y]$).
D'autre part a et b désigneront deux éléments de $\mathbb{Z}\backslash\{-1; 0; 1\}$

2.1. Étude du cas où $P(a^n, n)$ divise $Q(b^n, n)$

Dans cette partie P, Q désigneront des polynômes de $\mathbb{Z}[X, Y]$, qui ne sont pas dans $\mathbb{Z}[Y]$. On notera $P(X,Y) = \sum_{i=0}^{p} P_i(Y)X^i$ et $Q(X,Y) = \sum_{j=0}^{q} Q_j(Y)X^j$, avec $p = \deg_X P$ et $q = \deg_X Q$.

Nous aurons besoin de quelques résultats préliminaires:

Lemme 1. *Soient $m \in \mathbb{N}^*$, $c_1, \cdots, c_m$ des réels non nuls et $\theta_1, \cdots, \theta_m$ des rationnels non nuls et deux à deux distincts. Si pour tout $n \in \mathbb{N}$ assez grand, on a $\sum_{k=1}^{m} c_k\theta_k^n \in \mathbb{Z}$, alors $\forall k \in [\![1; m]\!]$, $\theta_k \in \mathbb{Z}$ et $c_k \in \mathbb{Q}$.*

Démonstration. On raisonne par récurrence sur m.

– La propriété est clairement vraie si $m = 1$.

– Supposons que la propriété soit vraie au rang $m \geqslant 1$ et que $\sum_{k=1}^{m+1} c_k\theta_k^n \in \mathbb{Z}$, pour $n \geqslant N$. En notant $\theta_{m+1} = \dfrac{u}{v}$ (u, v dans $\mathbb{Z}^*$), on a pour $n \geqslant N$:

$$\sum_{k=1}^{m} c_k(u - v\theta_k)\theta_k^n = u\sum_{k=1}^{m+1} c_k\theta_k^n - v\sum_{k=1}^{m+1} c_k\theta_k^{n+1} \in \mathbb{Z}.$$

L'hypothèse de récurrence montre alors que pour tout $k \in [\![1; m]\!]$, $\theta_k \in \mathbb{Z}$ et $c_k \in \mathbb{Q}$.

De la même façon, si on note $\theta_1 = \dfrac{u'}{v'}$ (u', v' dans $\mathbb{Z}^*$), on a pour tout $n \geqslant N$, $\sum_{k=2}^{m+1} c_k(u' - v'\theta_k)\theta_k^n \in \mathbb{Z}$ et l'hypothèse de récurrence montre que pour tout $k \in [\![2; m+1]\!]$, $\theta_k \in \mathbb{Z}$ et $c_k \in \mathbb{Q}$. On a finalement $\theta_k \in \mathbb{Z}$ et $c_k \in \mathbb{Q}$ pour tout $k \in [\![1; m+1]\!]$, ce qui prouve la proposition au rang $m+1$. ■

Lemme 2. *Soit $\alpha \in \mathbb{Q}\backslash\{1\}$ et $H \in \mathbb{R}[X]$ tel que $\alpha H(X+1) - H(X) \in \mathbb{Q}[X]$, alors $H \in \mathbb{Q}[X]$.*

Démonstration. Notons $H(X) = \sum_{j=0}^{m} a_jX^j$ et pour $0 \leqslant j \leqslant m$, b_j le coefficient de X^j dans le polynôme $\alpha H(X+1) - H(X)$. On a $b_j = (\alpha - 1)a_j + {}$ $+\alpha \sum_{k=j+1}^{m} \binom{k}{j} a_k$, d'où $a_j = \dfrac{1}{\alpha - 1}b_j - \dfrac{\alpha}{\alpha - 1}\sum_{k=j+1}^{m} \binom{k}{j} a_k$. Par hypothèse, α et les b_j sont rationnels donc $a_m = \dfrac{1}{\alpha - 1}b_m \in \mathbb{Q}$ et un raisonnement par récurrence descendante permet de prouver que $a_{m-1} \in \mathbb{Q}, \cdots, a_0 \in \mathbb{Q}$. ■

Lemme 3. *Soit $H \in \mathbb{R}[X]$ de degré $d \geqslant 0$. On suppose qu'il existe des rationnels $r_0, \cdots, r_d$ deux à deux distincts tels que pour tout $k \in [\![0;d]\!]$, $H(r_k) \in \mathbb{Q}$, alors $H \in \mathbb{Q}[X]$.*

Démonstration. On a $H(X) = \sum_{k=0}^{d} H(r_k)L_k(X)$, avec

$$L_k = \prod_{i \in [\![0;d]\!] \setminus \{k\}} \frac{X - r_i}{r_k - r_i} \in \mathbb{Q}[X],$$

donc $H \in \mathbb{Q}[X]$. ■

Lemme 4. *Soient $m \in \mathbb{N}^*$, $R_1, \cdots, R_m$ des éléments non nuls de $\mathbb{R}[X]$ et $\theta_1, \cdots, \theta_m$ des rationnels non nuls et deux à deux distincts. Si pour tout $n \in \mathbb{N}$ assez grand, on a $\sum_{k=1}^{m} R_k(n)\theta_k^n \in \mathbb{Z}$, alors $\forall k \in [\![1;m]\!]$, $\theta_k \in \mathbb{Z}$ et $R_k \in \mathbb{Q}[X]$.*

Démonstration. On raisonne par récurrence sur $s = \sum_{k=1}^{m} \deg R_k$.

– Si $s = 0$, le lemme 1 permet de conclure.

– Admettons que la proposition soit vraie au rang $s \geqslant 0$ et supposons que $\sum_{k=1}^{m} \deg R_k = s + 1$.

Soit $j \in [\![1;m]\!]$ tel que $\deg R_j \geqslant 1$; notons $\theta_j = \dfrac{u}{v}$ avec $(u,v) \in (\mathbb{Z}^*)^2$.

Pour tout n assez grand, on a

$$v\sum_{k=1}^{m} R_k(n+1)\theta_k^{n+1} - u\sum_{k=1}^{m} R_k(n)\theta_k^n \in \mathbb{Z},$$

soit

$$\sum_{k=1}^{m} H_k(n)\theta_k^n \in \mathbb{Z},$$

en posant $H_k = u\left[\dfrac{\theta_k}{\theta_j}R_k(X+1) - R_k(X)\right]$. On a $\deg H_j = \deg R_j - 1$ et $\deg H_k = \deg R_k$ lorsque $k \neq j$. Par conséquent, $\sum_{k=1}^{m} \deg H_k = s$ et l'hypothèse de récurrence s'applique : on a donc pour tout $k \in [\![1;m]\!]$, $H_k \in \mathbb{Q}[X]$ et $\theta_k \in \mathbb{Z}$. Si $k \in [\![1;m]\!]\setminus\{j\}$, on déduit du lemme 2 que $R_k \in \mathbb{Q}[X]$. Pour finir, remarquons que pour tout n assez grand,

$$R_j(n)\theta_j^n = \sum_{k=1}^{m} R_k(n)\theta_k^n - \sum_{k\neq j} R_k(n)\theta_k^n \in \mathbb{Q},$$

ce qui prouve que $R_j(n) \in \mathbb{Q}$ pour tout n assez grand et donc que $R_j \in \mathbb{Q}[X]$, d'après le lemme 3. ■

Lemme 5. *Soient $s \in \mathbb{R}^*$ et $R \in \mathbb{R}[X,Y]$ tels que pour tout n assez grand, $R(a^n, ns) = 0$, alors $R = 0$.*

Démonstration. En posant $R(X,Y) = \sum_{j=0}^{m} R_j(Y)X^j$, on obtient pour tout n assez grand, $\sum_{j=0}^{m} R_j(sn)(a^j)^n = 0$ et comme les a^j sont non nuls et deux à deux distincts, la remarque 1.c entraîne que $R_j(sX) = 0$ (et donc que $R_j = 0$) pour tout $j \in [\![0; m]\!]$. ■

Nous pouvons maintenant prouver le résultat principal de cette partie :

Théorème 1. *Si P n'est pas un monôme en X (c'est à dire ne s'écrit pas sous la forme $H(Y)X^p$ avec $p \in \mathbb{N}$ et $H \in \mathbb{Z}[Y]$) et si pour tout $n \in \mathbb{N}$ assez grand, on a $P(a^n, n) \,|\, Q(b^n, n)$, alors il existe $(s,t) \in (\mathbb{N}^*)^2$ tel que $s \leqslant \deg_X Q$, $b^s = a^t$ et $P(X^s, Y) \,|\, Q(X^t, Y)$.*

Démonstration. Posons $i_0 = \min\{i \in \mathbb{N} \mid P_i(Y) \neq 0\}$ et $j_0 = \min\{j \in \mathbb{N} \mid Q_j(Y) \neq 0\}$; il est important de noter pour la suite que $i_0 < p$, car P n'est pas un monôme en X.

Remarquons que si $n \in \mathbb{N}$,

$$P(a^n, n) = \sum_{i=i_0}^{p} P_i(n)(a^i)^n \quad \text{et} \quad Q(b^n) = \sum_{j=j_0}^{q} Q_j(n)(b^j)^n,$$

donc les suites $(P(a^n, n))$ et $(Q(b^n, n))$ sont récurrentes linéaires. D'après le Théorème du Quotient de Hadamard, il existe donc $N \in \mathbb{N}$ tel que la suite $\left(\dfrac{Q(b^n, n)}{P(a^n, n)}\right)_{n \geqslant N}$ soit récurrente linéaire. On en déduit qu'on a, pour tout $n \geqslant N$,

$$\frac{Q(b^n, n)}{P(a^n, n)} = \sum_{k=1}^{m} R_k(n)\theta_k^n \tag{3}$$

où $\theta_1, \cdots, \theta_m$ sont des complexes non nuls et deux à deux distincts (supposons que $|\theta_1| \leqslant \cdots \leqslant |\theta_m|$) et $R_1, \cdots, R_m$ des polynômes non nuls à coefficients dans $\mathbb{C}$.

Nous allons montrer successivement que:

(i) $\forall\ k \in [\![1; m]\!]$, θ_k est de la forme $\dfrac{b^j}{a^i}$, où i et j sont des entiers tels que $i \geqslant i_0$ et $j_0 \leqslant j \leqslant q$,

(ii) il existe $(s,t) \in (\mathbb{N}^*)^2$ tel que $s \leqslant \deg Q$ et $b^s = a^t$,
(iii) $\forall\ k \in [\![1;m]\!]$, $P_k \in \mathbb{Q}[X]$ et $\theta_k \in \mathbb{Z}^*$,
(iv) on a $P(X^s,Y) \,|\, Q(X^t,Y)$.

(i) L'égalité (3) s'écrit

$$\sum_{j=j_0}^{q} Q_j(n)(b^j)^n = \sum_{k=1}^{m}\sum_{i=i_0}^{p} P_i(n)R_k(n)(a^i\theta_k)^n \tag{4}$$

Soit $(k,i) \in [\![1;m]\!] \times [\![i_0;p]\!]$ tel que $(k,i) \neq (m,p)$. Dans le cas où $i < p$, on a $|a^i\theta_k| < |a^p\theta_k| \leqslant |a^p\theta_m|$ et dans celui où $i = p$, on a $k \neq m$, d'où $\theta_k \neq \theta_m$. Dans les deux cas, on a $a^i\theta_k \neq a^p\theta_m$. Un raisonnement identique montre que si $(k,i) \neq (1,i_0)$, alors $a^i\theta_k \neq a^{i_0}\theta_1$.

Par conséquent, après réduction du membre de droite de (4), les termes

$$P_p(n)R_m(n)(a^p\theta_m)^n \quad \text{et} \quad P_{i_0}(n)R_1(n)(a^{i_0}\theta_1)^n$$

demeurent intacts. Vu le membre de gauche de (4), on en déduit que $a^p\theta_m = b^q$ (en effet, dans le cas contraire on aurait $a^p\theta_m = b^j$ avec $j < q$ et il existerait $(k,i) \in [\![1;m]\!] \times [\![i_0;p]\!]$ tel que $b^q = a^i\theta_k$, d'où $|a^i\theta_k| = |b|^q > |b|^j = |a^p\theta_m|$, ce qui est impossible); de la même façon, on tire que $a^{i_0}\theta_1 = b^{j_0}$. Ainsi, $\theta_m = \dfrac{b^q}{a^p}$ et $\theta_1 = \dfrac{b^{j_0}}{a^{i_0}}$.

Raisonnons par l'absurde en supposant qu'il existe $k \in [\![1;m]\!]$ tel que θ_k ne s'écrive pas sous la forme $\dfrac{b^j}{a^i}$, avec $i \geqslant i_0$ et $j_0 \leqslant j \leqslant q$. Considérons k_1 le plus grand de ces entiers k (On a donc $i_0 < k_1 < m$). Après réduction du membre de droite de (4), il ne peut pas rester de terme de la forme $H(n)(a^p\theta_{k_1})^n$ avec $H \in \mathbb{C}[X]\backslash\{0\}$ (sinon, vu le membre de gauche de (4), on aurait $a^p\theta_{k_1} = b^j$ pour un certain $j \in [\![j_0;q]\!]$, ce qui est impossible). Par conséquent, il existe un $i \in [\![i_0;p]\!]$ et un entier k tel que $k_1 < k \leqslant m$ avec $a^p\theta_{k_1} = a^i\theta_k$. Or, vu le caractère maximal de k_1, il existe $i' \geqslant i_0$ et $j' \in [\![j_0;q]\!]$ tels que $\theta_k = \dfrac{b^{j'}}{a^{i'}}$, d'où $\theta_{k_1} = \dfrac{b^{j'}}{a^{i'+p-i}}$, avec $i'+p-i \geqslant i' \geqslant i_0$, ce qui est absurde et achève de prouver (i).

(ii) Remarquons qu'après avoir réduit le membre de droite de l'égalité (4), deux cas de figure se présentent:

– Il reste un terme de la forme $H(n)(a^p\theta_1)^n$ avec $H \in \mathbb{Q}[X]\backslash\{0\}$. Dans ce cas, vu le membre de gauche de (4), il existe $j \in [\![j_0;q]\!]$ tel que $a^p\theta_1 = b^j$, et comme $\theta_1 = \dfrac{b^{j_0}}{a^{i_0}}$, on obtient $b^s = a^t$ avec $t = p - i_0 \geqslant 1$ et $s = j - j_0 \in [\![1;q]\!]$.

– Dans le cas contraire, il existe k et i tels que $1 < k \leqslant m$ et $i_0 \leqslant i < p$ vérifiant $a^p\theta_1 = a^i\theta_k$. Or d'après (ii), on a $\theta_k = \dfrac{b^j}{a^{i'}}$, où $i' \geqslant i_0$ et $j \in [\![j_0; q]\!]$, ce qui permet d'obtenir $b^s = a^t$, avec $t = p - i + i' - i_0 \geqslant 1$ et $s = j - j_0 \in [\![1; q]\!]$.

(iii) On a pour tout $n \geqslant N$, $\sum\limits_{k=1}^{m} R_k(n)\theta_k^n = \dfrac{Q(b^n)}{P(a^n)} \in \mathbb{Z}$, donc comme on vient de prouver que les θ_k étaient rationnels, les polynômes R_k sont à coefficients réels. On peut alors appliquer le lemme 4, qui permet d'établir que pour tout $k \in [\![1; m]\!]$, $R_k \in \mathbb{Q}[X]$ et $\theta_k \in \mathbb{Z}$.

(iv) Posons $\theta_k = \dfrac{b^{j_k}}{a^{i_k}}$, avec $i_k \geqslant i_0$ et $j_0 \leqslant j_k \leqslant q$, pour $k \in [\![1; m]\!]$. On a $\theta_k^s = a^{\mu_k}$ avec $\mu_k = tj_k - si_k$; notons que $\mu_k \in \mathbb{N}$ car $\theta_k \in \mathbb{Z}^*$, donc $|a|^{\mu_k} \geqslant 1$.

En substituant ns à n dans (3), on obtient pour tout $n \geqslant N$,

$$Q(a^{nt}, ns) = P(a^{ns}, ns) \sum_{k=1}^{m} R_k(ns) a^{\mu_k n},$$

soit, pour tout $n \geqslant N$,

$$R(a^n, ns) = 0,$$

en posant $R(X, Y) = P(X^s, Y) \sum\limits_{k=1}^{m} R_k(Y)X^{\mu_k} - Q(X^t, Y) \in \mathbb{Q}[X, Y]$. Le lemme 5 montre alors que $R = 0$ et donc que $P(X^s, Y) \,|\, Q(X^t, Y)$. ■

Remarque 3. (a) Une conséquence est qu'on a $\deg_Y P \leqslant \deg_Y Q$ et lorsque $\deg_Y P = \deg_Y Q$, il existe $R \in \mathbb{Q}[X]$ tel que $Q(X^t, Y) = R(X)P(X^s, Y)$.

(b) Le point précédent implique en particulier que si $S \in \mathbb{Z}[X]\backslash\{0\}$ et $P(n, a^n) \,|\, S(b^n)$ pour tout n assez grand, alors $P \in \mathbb{Z}[X]$.

Le théorème 1 entraîne par exemple la généralisation de la propriété $\mathcal{P}_0$ dans une première direction :

Propriété 1. *Soient P_0, P_1, Q_0 et Q_1 dans $\mathbb{Z}[X]$ avec P_0, P_1 et Q_1 non nuls. Si pour tout $n \in \mathbb{N}$ assez grand, on a $P_1(n)a^n + P_0(n) \,|\, Q_1(n)b^n + Q_0(n)$, alors il existe $t \in \mathbb{N}^*$ tel que $b = a^t$ et $Q_0P_1^t = (-1)^{t+1}Q_1P_0^t$.*

Démonstration. Il suffit de prendre $P(X, Y) = P_1(Y)X + P_0(Y)$ et $Q(X, Y) = = Q_1(Y)X + Q_0(Y)$. Comme $P(a^n, n) \,|\, Q(b^n, n)$ pour tout n assez grand, le théorème 1 montre qu'il existe $t \in \mathbb{N}^*$ tel que $b = a^t$ et

$$P_1(Y)X + P_0(Y) \,|\, Q_1(Y)X^t + Q_0(Y).$$

En particulier si $y \in \mathbb{R}$, le polynôme $P_1(y)X + P_0(y)$ divise $Q_1(y)X^t + Q_0(y)$ dans $\mathbb{R}[X]$. Si y n'est pas une racine de P_1, $-\dfrac{P_0(y)}{P_1(y)}$ est une racine de $P_1(y)X +$

$+P_0(y)$, donc également une racine de $Q_1(y)X^t+Q_0(y)$, d'où $Q_1(y)\left[-\dfrac{P_0(y)}{P_1(y)}\right]^t+$ $+Q_0(y)=0$. Le polynôme $Q_1(-P_0)^t+Q_0P_1^t$ possède donc une infinité de racines, ce qui prouve qu'il est nul. ■

Remarque 4. Si on suppose les polynômes P_0 et P_1 premiers entre eux et leurs contenus également premiers entre eux, la réciproque de la propriété précédente est vraie. En effet comme $Q_0P_1^t=(-1)^{t+1}Q_1P_0^t$, il est facile de voir que P_1^t divise Q_1 dans $\mathbb{Z}[X]$. Or si $n\in\mathbb{N}$, on a

$$P_1(n)^t[Q_1(n)a^{tn}+Q_0(n)]=Q_1(n)[(P_1(n)a^n)^t-(-P_0(n))^t],$$

donc comme $P_1(n)^t \mid Q_1(n)$, on a pour tout $n\in\mathbb{N}$ qui n'est pas racine de P_1,

$$P_1(n)a^n+P_0(n) \;\mid\; (P_1(n)a^n)^t-(-P_0(n))^t \;\mid\; Q_1(n)a^{tn}+Q_0(n).$$

2.2. Étude du cas où $P(a^n)$ divise $P(b^n)$

Dans cette partie, P désigne cette fois un polynôme à coefficients entiers.

Lemme 6. *Si P n'est pas un monôme, et si $(t,s)\in(\mathbb{N}^*)^2$ est tel que $t\neq s$ et $P(X^s)\mid P(X^t)$, alors les racines non nulles de P sont des racines de l'unité et $s\mid t$.*

Démonstration. Posons $h=\dfrac{t}{s}$. Si $\xi=re^{i\theta}$ est une racine non nulle de P ($r\in\mathbb{R}_+^*$ et $\theta\in\mathbb{R}^*$) alors $r^{\frac{1}{s}}e^{i\frac{\theta}{s}}$ est une racine de $P(X^s)$ donc de $P(X^t)$, ce qui prouve que $r^he^{ih\theta}$ est aussi une racine de P. Une récurrence sur n montre alors que pour tout $n\in\mathbb{N}$, $\xi_n=r^{h^n}e^{ih^n\theta}$ est une racine de P. Or, P possédant un nombre fini de racines, il existe deux entiers naturels distincts n_1 et n_2 tels que $\xi_{n_1}=\xi_{n_2}$, c'est-à-dire tels que $r^{h^{n_1}}=r^{h^{n_2}}$ et $h^{n_1}\theta\equiv h^{n_2}\theta\,[2\pi]$. Comme $h\neq 1$, cela implique que $r=1$ et $\theta\in\pi\mathbb{Q}^*$, et donc que ξ est bien une racine de l'unité.

Notons $\theta=\dfrac{p\pi}{q}$ avec $(p,q)\in(\mathbb{Z}^*)^2$. La suite $(\xi_n)_{n\in\mathbb{N}}$ ne prenant qu'un nombre fini de valeurs, elle possède une sous-suite constante $(\xi_{n_k})_{k\in\mathbb{N}}$. On a alors $\forall k\in\mathbb{N}$, $h^{n_k}\theta\equiv h^{n_0}\theta\,[2\pi]$. Si M est un entier tel que $h^{n_0}M\in\mathbb{Z}^*$, on a alors $\forall k\in\mathbb{N}$, $h^{n_k}pM\in\mathbb{Z}^*$, ce qui prouve que $h\in\mathbb{N}^*$ et donc que $s\mid t$. ■

J'utiliserai à plusieurs reprises le résultat suivant :

Lemme 7. *Soient A un anneau commutatif, $m\in\mathbb{N}^*$, U et V des éléments de $A[X]$ tels que $U(X^m)$ divise $V(X^m)$ dans $A[X]$, alors U divise V dans $A[X]$.*

Démonstration. Soit $W \in A[X]$ tel que $V(X^m) = U(X^m)W(X)$. Notons $W(X) = \sum_{i=0}^{d} a_i X^i$ et $W_0(X) = \sum_{m \mid i} a_i X^i$; il existe $T \in A[X]$ tel que $W_0(X) = T(X^m)$. On obtient alors

$$V(X^m) - U(X^m)T(X^m) = U(X^m)[W(X) - W_0(X)] \tag{5}$$

Après avoir réduit les deux membres de l'égalité précédente, on voit que celui de gauche s'écrit sous la forme $\sum_{k\in E} \alpha_k X^k$ avec $\alpha_k \in A$ et $E \subset m\mathbb{N}$, alors que celui de droite s'écrit sous la forme $\sum_{k\in F} \beta_k X^k$ avec $\beta_k \in A$ et $F \subset \mathbb{N}\backslash m\mathbb{N}$. On en déduit que les deux membres de l'égalité (5) sont des polynômes nuls, d'où $V(X^m) = U(X^m)T(X^m)$, ce qui prouve que $V(X) = U(X)T(X)$. ■

Propriété 2. *Si P n'est pas un monôme et si pour tout $n \in \mathbb{N}$ assez grand, on a $P(a^n) \mid P(b^n)$, alors il existe $h \in \mathbb{N}^*$ tel que $b = \pm a^h$ et $P(X) \mid P(X^h)$.*

Démonstration. D'après le théorème 1 (voir aussi la remarque 3.a qui suit), il existe $(s,t) \in (\mathbb{N}^*)^2$ tel que $b^s = a^t$ et $P(X^s) \mid P(X^t)$. Si $s = t$, on a $b = \pm a$, donc $h = 1$ convient. Si $s \neq t$, on peut appliquer le lemme 6 qui permet de déduire que $t = hs$ avec $h \in \mathbb{N}^*$; on a alors $b = \pm a^h$ et $P(X^s) \mid P(X^{sh})$, d'où $P(X) \mid P(X^h)$ (voir lemme 7). ■

Remarque 5. Dans le cas où $b = a^h$ (ce qui arrive par exemple lorsque a et b sont positifs), la réciproque de la propriété 2 est vraie. En effet, comme $P(X)$ et $P(X^h)$ ont même contenu, $P(X) \mid P(X^h)$ est une relation de divisibilité dans $\mathbb{Z}[X]$. Si $b = a^h$ et $P(X) \mid P(X^h)$, on a donc pour tout $n \in \mathbb{N}$, $P(a^n) \mid P(a^{nh}) = P(b^n)$.

D'après le lemme 6, lorsque $P(X) \mid P(X^h)$ avec $h \geqslant 2$, les racines non nulles de P sont des racines de l'unité. Afin de préciser la propriété 2 dans le cas où P est irréductible dans $\mathbb{Q}[X]$, nous aurons besoin des polynômes cyclotomiques (voir [4] pour leurs propriétés de base).

Si $m \in \mathbb{N}^*$, on notera Φ_m le $m-$ième polynôme cyclotomique sur $\mathbb{Q}$.

Rappelons que si $m \equiv 0\,[4]$, on a $\Phi_m(X) = \Phi_{m/2}(X^2)$.

Lemme 8. *Soit $(m,h) \in (\mathbb{N}^*)^2$; alors $\Phi_m(X) \mid \Phi_m(X^h)$ si et seulement si* $\operatorname{pgcd}(h,m) = 1$.

Démonstration. Φ_m étant le polynôme minimal de $\mathrm{e}^{\mathrm{i}\frac{2\pi}{m}}$ sur $\mathbb{Q}$, on a: $\Phi_m(X) \mid \Phi_m(X^h)$ si et seulement si $\mathrm{e}^{\mathrm{i}\frac{2\pi}{m}}$ est une racine de $\Phi_m(X^h)$, c'est-à-dire si et seulement si $\mathrm{e}^{\mathrm{i}\frac{2h\pi}{m}}$ est une racine de Φ_m, ce qui équivaut à $\operatorname{pgcd}(h,m) = 1$.

■

Remarque 6. D'après le lemme 6, si $P \in \mathbb{Z}[X]$ est unitaire et vérifie $P(X) \mid P(X^h)$ avec $h \geqslant 2$, les racines non nulles de P sont des racines de l'unité. Le polynôme P est alors nécessairement de la forme $X^d \prod_{i=1}^{n} \Phi_{m_i}$, avec $d \in \mathbb{N}$, $n \in \mathbb{N}$ et $m_i \in \mathbb{N}^*$. Même s'il ne semble pas facile d'expliciter la forme générale des couples (P, h) tels que $P(X) \mid P(X^h)$, le lemme 8 montre néanmoins que si $P(X) = X^d \prod_{i=1}^{n} \Phi_{m_i}(X)$ et si h est premier avec chacun des m_i, alors $P(X) \mid P(X^h)$. Précisons qu'on peut très bien avoir $P(X) \mid P(X^h)$ sans que h soit premier avec chacun des m_i, comme par exemple lorsque $h = 2$ et $P = \Phi_3\Phi_6\Phi_{12}$ (on peut vérifier dans ce cas que $P(X^h) = (\Phi_3\Phi_6\Phi_{12}\Phi_{24})(X)$).

Lemme 9. *Soit $m \in \mathbb{N}^*$; Φ_m possède deux racines opposées si et seulement si $m \equiv 0\,[4]$.*

Démonstration. Soit ξ une racine de Φ_m ; il existe un entier p premier avec m tel que $\xi = e^{\frac{2ip\pi}{m}}$, d'où $-\xi = e^{\frac{i(2p+m)\pi}{m}}$. Si $-\xi$ est une racine de Φ_m, il existe donc un entier q premier avec m tel que $2p + m = 2q$, ce qui entraîne que m est pair, donc que p et q sont impairs et finalement que m est divisible par 4. Réciproquement, si $m \equiv 0\,[4]$, on a $\Phi_m(X) = \Phi_{m/2}(X^2)$ donc si ξ est une racine de Φ_m, $-\xi$ en est une également. ■

Nous utiliserons également le résultat suivant :

Lemme 10. *Soient P_1 et Q_1 deux polynômes à coefficients dans $\mathbb{Z}$ avec $\deg P_1 \geqslant 1$ et $\deg Q_1 \geqslant 1$. S'il existe une infinité d'entiers relatifs n tels que $P_1(n) \mid Q_1(n)$, alors $P_1 \mid Q_1$.*

Démonstration. Soit $Q_1 = SP_1 + R$ l'identité de division euclidienne de Q_1 par P_1 dans $\mathbb{Q}[X]$. Il existe $\alpha \in \mathbb{N}^*$ tel que αS et αR soient à coefficients dans $\mathbb{Z}$. Comme $\alpha Q_1(n) = \alpha S(n)P_1(n) + \alpha R(n)$, on en déduit que $\alpha R(n)$ est divisible par $P_1(n)$ pour une infinité d'entiers n, ce qui prouve que R est nul, car $\deg P_1 > \deg R$. ■

Propriété 3. *Soit $m \in \mathbb{N}^*$ tel que $m \not\equiv 0\,[4]$ (resp. $m \equiv 0\,[4]$). Alors les deux assertions qui suivent sont équivalentes :*

(i) *Pour tout $n \in \mathbb{N}$ assez grand, $\Phi_m(a^n) \mid \Phi_m(b^n)$*

(ii) *Il existe un entier h premier avec m tel que $b = a^h$ (resp. $b = \pm a^h$)*

Démonstration. Si (i) est vrai, la propriété 2 montre qu'il existe $h \in \mathbb{N}^*$ tel que $b = \pm a^h$ et $\Phi_m(X) \mid \Phi_m(X^h)$. D'après le lemme 8, on a donc $\operatorname{pgcd}(h, m) = 1$.

Supposons que $b = -a^h$ et montrons que $m \equiv 0\,[4]$. Pour tout n assez grand, on a $\Phi_m(a^{2n+1}) \,|\, \Phi_m(b^{2n+1})$, soit $\Phi_m(a^{2n+1}) \,|\, \Phi_m(-a^{(2n+1)h})$, ou encore $P_1(a^{2n+1}) \,|\, Q_1(a^{2n+1})$ avec $P_1(X) = \Phi_m(X)$ et $Q_1(X) = \Phi_m\left(-X^h\right)$. Le lemme 10 entraîne alors que $\Phi_m(X) \,|\, \Phi_m(-X^h)$. Posons $\xi = \mathrm{e}^{\mathrm{i}\frac{2\pi}{m}}$; ξ est une racine de Φ_m donc comme $\Phi_m(X)$ divise $\Phi_m(X^h)$ et $\Phi_m(-X^h)$, ξ^h et $-\xi^h$ sont des racines de Φ_m, ce qui prouve bien, en vertu du lemme 9, que $m \equiv 0\,[4]$.

Réciproquement, supposons que (ii) soit vrai. D'après le lemme 8, on a $\Phi_m(X) \,|\, \Phi_m(X^h)$, cette relation de divisibilité ayant lieu dans $\mathbb{Z}[X]$, car Φ_m est unitaire et à coefficients dans $\mathbb{Z}$. Cela entraîne que : $\forall n \in \mathbb{N}$, $\Phi_m(a^n) \,|\, \Phi_m(a^{nh})$.

- Si $b = a^h$, on a bien $\Phi_m(a^n) \,|\, \Phi_m(b^n)$.

- Si $b = -a^h$ et $m \equiv 0\,[4]$, on a $\Phi_m(b^n) = \Phi_{\frac{m}{2}}(b^{2n}) = \Phi_{\frac{m}{2}}(a^{2nh}) = \Phi_m(a^{nh})$. On a donc également $\Phi_m(a^n) \,|\, \Phi_m(b^n)$. ■

Exemple 1. Dans le cas où $n = 3$, on obtient par exemple le résultat suivant:

$a^{2n} + a^n + 1 \,|\, b^{2n} + b^n + 1$ pour tout n assez grand, si et seulement s'il existe un entier h non divisible par 3 tel que $b = a^h$.

2.3. Étude du cas où $P(a^n, n)$ divise $P(b^n, n)$

Dans cette partie, P désigne un polynôme de $\mathbb{Z}[X, Y]$ qui n'est pas dans $\mathbb{Z}[X]$. On notera $P(X, Y) = \sum_{j=0}^{d} \pi_j(X) Y^j = \sum_{i=0}^{p} P_i(Y) X^i$, avec $d = \deg_Y P$ et $p = \deg_X P$.

Lemme 11. *Soient $h \geqslant 2$ un entier et R, S des polynômes de $\mathbb{Q}[X]\backslash\{0\}$ tels que $R(X)S(X^h) = S(X)R(X^h)$, alors il existe $\lambda \in \mathbb{Q}^*$ tel que $S = \lambda R$.*

Démonstration. Soit $Q = \mathrm{pgcd}(R, S)$; on a $S = QS_1$ et $R = QR_1$ avec S_1 et R_1 dans $\mathbb{Q}[X]\backslash\{0\}$ tels que $\mathrm{pgcd}(S_1, R_1) = 1$ (on a donc également $\mathrm{pgcd}(S_1(X^h), R_1(X^h)) = 1$). Comme $R_1(X)S_1(X^h) = S_1(X)R_1(X^h)$, on a $R_1(X^h) \,|\, R_1(X)$, ce qui prouve que $\deg R_1 = 0$ et donc qu'il existe $\lambda \in \mathbb{Q}^*$ tel que $S = \lambda R$. ■

Propriété 4. *On suppose que P n'est pas un monôme en X et que $|a| \neq |b|$. Si $P(a^n, n) \,|\, P(b^n, n)$ pour tout $n \in \mathbb{N}$ assez grand, alors il existe $U \in \mathbb{Z}[X]$, $V \in \mathbb{Z}[Y]$ et un entier $h \geqslant 2$, tels que $b = \pm a^h$, $P(X, Y) = U(X)V(Y)$ et $U(X) \,|\, U(X^h)$.*

Démonstration. D'après le théorème 1, on sait qu'il existe $(s, t) \in (\mathbb{N}^*)^2$ tel que $b^s = a^t$ et $P(X^s, Y) \,|\, P(X^t, Y)$. Notons que $s \neq t$ car $|a| \neq |b|$. Si $y \in \mathbb{N}$ n'est racine d'aucun des coefficients P_i non nuls, le polynôme $P(X, y)$ de

$\mathbb{Z}[X]$ n'est pas un monôme. Donc comme $P(X^s, y)$ divise $P(X^t, y)$ dans $\mathbb{Q}[X]$, le lemme 6 entraîne que $h = \dfrac{t}{s} \in \mathbb{N}^*$ (remarquons qu'on a alors $b = \pm a^h$). Puisqu'on a $P(X^s, Y) \mid P(X^{sh}, Y)$, on déduit du lemme 7 que $P(X, Y) \mid P(X^h, Y)$ et donc qu'il existe $H \in \mathbb{Q}[X]\backslash\{0\}$ tel que

$$P(X^h, Y) = H(X)P(X, Y),$$

c'est-à-dire

$$\sum_{j=0}^{d} \pi_j(X^h)Y^j = \sum_{j=0}^{d} H(X)\pi_j(X)Y^j.$$

Pour tous j_1 et j_2 dans $[\![0; d]\!]$, on a donc

$$\pi_{j_1}(X)\pi_{j_2}(X^h) = \pi_{j_2}(X)\pi_{j_1}(X^h),$$

ce qui montre, en vertu du lemme 11, qu'il existe $U \in \mathbb{Q}[X]\backslash\{0\}$ et $\lambda_0, \cdots, \lambda_d$ dans $\mathbb{Q}$ (avec $\lambda_j \neq 0$ si et seulement si $\pi_j \neq 0$) tels que pour tout $j \in [\![0; d]\!]$,

$$\pi_j(X) = \lambda_j U(X).$$

On obtient alors $P(X, Y) = \sum_{j=0}^{d} \pi_j(X)Y^j = U(X)V(Y)$, avec $V(Y) = \sum_{j=0}^{d} \lambda_j Y^j$, et comme $P(X^h, Y) = H(X)P(X, Y)$, on a $U(X^h) = H(X)U(X)$, ce qui prouve que $U(X) \mid U(X^h)$.

Notons que P étant à coefficients entiers, on peut faire en sorte que U et V aient aussi leurs coefficients entiers, en les remplaçant respectivement par $\dfrac{\delta_1}{\delta_2}U$ et $\dfrac{\delta_2}{\delta_1}V$, où δ_1 (resp. δ_2) est le plus petit multiple commun des dénominateurs des coefficients non nuls (mis sous forme irréductible) de U (resp. V). ■

Voici une conséquence immédiate:

Propriété 5. *Si $P(X, Y)$ n'est pas du type $U(X)V(Y)$ avec (U, V) dans $\mathbb{Z}[X]\times\mathbb{Z}[Y]$ et si $P(a^n, n) \mid P(b^n, n)$ pour tout n assez grand, alors $b = \pm a$.*

Remarque 7. Dans le cas où $b = -a$, $P(X, Y)$ est nécessairement du type $R(X^2, Y)$ ou $XR(X^2, Y)$ avec $R \in \mathbb{Z}[X, Y]$.
En effet, supposons que $P(a^n, n) \mid P((-a)^n, n)$ pour tout n assez grand. Notons $\varepsilon = (-1)^p$ et raisonnons par l'absurde en supposant qu'il existe $i_1 \in [\![0; p]\!]$ de parité différente de celle de p tel que $P_{i_1} \neq 0$; choisissons i_1 maximal. On a pour tout n assez grand

$$P(a^{2n+1}, 2n+1) \ \mid \ P(a^{2n+1}, 2n+1) - \varepsilon P(-a^{2n+1}, 2n+1),$$

et en notant $f(n) = P(a^{2n+1}, 2n+1) - \varepsilon P(-a^{2n+1}, 2n+1)$, on peut vérifier que

$$f(n) \sim 2P_{i_1}(2n+1)a^{(2n+1)i_1} \quad (n \to +\infty).$$

Comme

$$P(a^{2n+1}, 2n+1) \sim P_p(2n+1)a^{(2n+1)p} \quad (n \to +\infty),$$

cela contredit le fait que $P(a^{2n+1}, 2n+1) \leqslant f(n)$ pour tout n assez grand.

Note: je tiens à remercier Jean-Paul Bézivin pour son aide précieuse.

References

[1] Problem 10674, *Amer. Math. Monthly*, **105** (1998), 560.

[2] **Cavachi, M.,** A powerful property, *Amer. Math. Monthly*, **107** (2000), 654.

[3] **Cerlencio, L., M. Mignotte and F. Piras,** Suites récurrentes linéaires: propriétés algébriques et arithmétiques, *Enseign. Math.*, **33** (1987), 67–108.

[4] **Nagell, T.,** *Introduction to Number Theory*, chapter V, AMS Chelsea Publishing, 1964.

[5] **Rumely, R.,** Notes on Van der Poorten's proof of the Hadamard Quotient Theorem, *Séminaire de Théorie des Nombres, Paris*, (1986-87), 349–382.

Bruno Langlois
69, Avenue Jean Jaurès
92290 Châtenay-Malabry
FRANCE
bruno.langlois@ac-versailles.fr