JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

PATRICK GONZALEZ

Généralisation d'un résultat de Loxton et van der Poorten

Journal de Théorie des Nombres de Bordeaux, tome 4, n° 1 (1992), p. 43-51

<http://www.numdam.org/item?id=JTNB_1992__4_1_43_0>

Séminaire de Théorie des Nombres,
Bordeaux **4** *(1992), 43-51*

Généralisation d'un résultat de Loxton et van der Poorten.

par PATRICK GONZALEZ

ABSTRACT. In this paper we propose to generalise a result of Loxton and Van der Poorten [1] in the following way. Let g be an integer greater than or equal to two and C be a finite subset of $\mathbb{N}$ containing zero. C will be said to be g-free if, for all integers n, the equality $\sum_{i=0}^{n} c_i g^i = \sum_{i=0}^{n} c'_i g^i$ with $c_i, c'_i \in C$, $0 \leq i \leq n$, implies $c_i = c'_i$ for $i = 0, \ldots, n$. Let P be the polynomial $\sum_{c \in C} X^c$, $P_n = \prod_{i=0}^{n-1} P(X^{g^h})$ and U_{g^n} the set of the g^n-th roots of unity. We shall prove that C is g-free, when Card $C = g$, if and only if, Card $\{x \in U_{g^n},\ P_n(x) \neq 0\}$ is bounded independently of n.

Introduction

Les nombres entiers peuvent s'écrire, en base 4, à l'aide des chiffres -1, 0, 1 et 2. Notons L l'ensemble de ceux obtenus en s'astreignant aux seuls chiffres -1, 0 et 1. On peut se demander quels sont les entiers k non nuls qui sont le quotient de deux éléments de L ?

Ce problème – surnommé "an awful problem about integers in base four"– a été résolu par Loxton et Van der Poorten [1] : k est de la forme voulue si et seulement s'il existe un entier α et un entier k' impair tel que $k = 4^\alpha k'$ (autrement dit si l'écriture de k en base 4 admet un chiffre impair comme premier chiffre non nul en partant de la droite).

Le but de cet article est de retrouver ce résultat dans un cadre plus général que l'on va préciser. L'entier k est solution du problème si et seulement s'il existe l et l' non nuls dans L tels que $lk = l'$. Comme $L = S - S$, où S est l'ensemble des nombres s'écrivant avec les chiffres 0 et 1, il s'ensuit qu'un nombre est solution si et seulement s'il existe s_1, s'_1, s_2, s'_2 dans S tel que $s_1 + s_2 k = s'_1 + s'_2 k$ avec $(s_1, s_1) \neq (s'_1, s'_2)$. En regroupant les puissances de 4 entre elles, ceci équivaut à : il existe deux suites finies distinctes $c_0, \ldots, c_n$ et $c'_0, \ldots, c'_n$, d'éléments de $\{0, 1, k, k+1\}$ telles que

$$\sum_{i=0}^{n} c_i 4^i = \sum_{i=0}^{n} c'_i 4^i.$$

Manuscrit reçu le 14 octobre 1991.

C'est sous cette forme que nous allons généraliser le problème. Soit $g \geq 2$ un entier et C une partie finie de $\mathbb{N}$. A quelle condition existe-t-il deux suites finies distinctes d'éléments de C disons $c_0, \ldots, c_n$ et $c'_0, \ldots, c'_n$ telles que

$$\sum_{i=0}^{n} c_i g^i = \sum_{i=0}^{n} c'_i g^i \ ?$$

Lorsque ce n'est pas le cas on dira que C est g-libre. On peut voir qu'il est nécessaire d'avoir $\operatorname{Card} C \leq g$ pour que C soit $g-$libre. Par commodité on va supposer que $0 \in C$ et on va établir une condition nécessaire et suffisante dans le cas "maximal" ($\operatorname{Card} C = g$) pour que C soit g-libre.

I. Automate non déterministe associé au problème.

1. Définition et lien avec le problème

G. Rauzy a montré [2] que l'ensemble des entiers s'écrivant sous la forme $\sum c_i g^i$ avec $c_i \in C$ est reconnaissable par un g-automate déterministe dont les états sont les parties de $\{0, \ldots, N\}$ où $N = \left[\dfrac{\operatorname{Max} C}{g-1}\right]$.

Nous allons nous intéresser à l'automate non-déterministe qu'il induit en prenant les éléments (au lieu des parties) de $\{0, \ldots, N\}$ comme états. Définissons $D_{(\gamma)}(A)$, où $A \subset \mathbb{N}$ et $0 \leq \gamma \leq g-1$, par :

$$D_{(\gamma)}(A) = \frac{C + A - \gamma}{g} \cap \mathbb{N}$$

On vérifie aisément que si $A \subset \{0, 1, \ldots, N\}$ alors $D_{(\gamma)}(A) \subset \{0, 1, \ldots, N\}$.

Les "flèches" de l'automate non déterministe seront :

$$i \xrightarrow{(\gamma)} j \quad \text{si} \quad i \in D_{(\gamma)}(\{j\}).$$

Le symbole $D_{(m)}$ est défini de proche en proche pour les mots de l'alphabet $\{0, \ldots, g-1\}$ par :

$D_{\emptyset}(A) = A$ et $D_{(mm')}(j) = D_{(m)}\left(D_{(m')}(A)\right)$ où A est une partie de $\mathbb{N}$ et (mm') est le concaténé du mot (m) par (m'). Les chemins d'étiquette (m) sont définis par $i \xrightarrow{(m)} j$ si et seulement si $i \in D_{(m)}(j)$ (par abus dorénavant on note $D_{(m)}(j)$ pour $D_{(m)}(\{j\})$). La relation $i \in D_{(m)}(j)$ se traduit par

$$i = \sum_{k=0}^{n-1} \frac{c_k - \gamma_k}{g^{n-k}} + \frac{j}{g^n}$$

pour certains $c_k \in C$ où $(m) = (\gamma_{n-1} \dots \gamma_0)$ est un mot dont les lettres γ_i appartiennent à l'ensemble $\{0, \dots, g-1\}$, $0 \leq i \leq n-1$. Le nombre de chemins $a_{i,j}^{(m)}$ d'étiquette (m), allant de i vers j, est donc égal au nombre de manières d'écrire $ig^n - j + \sum_{k=0}^{n-1} \gamma_k g^k$ sous la forme $\sum_{k=0}^{n-1} c_k g^k$ avec $c_k \in C$.

LEMME 1. *Il y a équivalence entre les assertions suivantes :*

i) *C est g-libre.*

ii) *Pour tout i, j de $\{0, \dots, N\}$ et tout mot (m) on a $a_{i,j}^{(m)} = 0$ ou 1.*

iii) *Pour tout mot (m) on a $a_{0,0}^{(m)} = 0$ ou 1.*

Démonstration. Il est clair que i) $\Rightarrow$ ii) $\Rightarrow$ iii). Supposons que C ne soit pas g-libre. Il existe alors deux suites distinctes $c_0, \dots, c_p$ et $c'_0, \dots, c'_p$ d'éléments de C telles que $\sum_{i=0}^{p} c_i g^i = \sum_{i=0}^{p} c'_i g^i$. Soit $m = \sum_{i=0}^{p} c_i g^i$, m s'écrit en base g, $\gamma_0 + \gamma_1 g + \dots + \gamma_q g^q$ avec $\gamma_k \in \{0, \dots, g-1\}$. Comme $0 \in C$, on peut égaliser les longueurs et il existe $\gamma_0, \dots, \gamma_{n-1}$ dans $\{0, \dots, g-1\}$ et deux suites finies distinctes $c_0, \dots, c_{n-1}$ et $c'_0, \dots, c'_{n-1}$ d'éléments de C telles que $\sum_{i=0}^{n-1} \gamma_i g^i = \sum_{i=0}^{n-1} c_i g^i = \sum_{i=0}^{n-1} c'_i g^i$. Si $(m) = (\gamma_{n-1} \dots \gamma_0)$ on a alors $a_{0,0}^{(m)} \geq 2$ et par conséquent iii) $\Rightarrow$ i).

2. Les matrices des chemins

Notons $A_{(m)} = (a_{i,j}^{(m)})_{0 \leq i,j \leq N}$ et $A_\emptyset = I_N$. Si (mm') est le produit de concaténation de (m) par (m') on a : $A_{(mm')} = A_{(m)} \cdot A_{(m')}$. L'ensemble $\mathcal{M}$ des matrices du type $A_{(m)}$ muni de la multiplication des matrices est un monoïde engendré par $A_{(0)}, \dots, A_{(g-1)}$.

Si P est une matrice quelconque, on notera $N(P)$ la somme de toutes les entrées de P. On emploiera la notation habituelle $|(m)|$ pour désigner la longueur du mot (m).

LEMME 2. *Pour tout entier $n \geq 1$ et $j = 0, \dots, N$ on a :*

$$\sum_{\substack{|(m)|=n \\ 0 \leq i \leq N}} a_{i,j}^{(m)} = (Card\ C)^n.$$

Démonstration. On raisonne par récurrence sur n. Si $n = 0$ alors $(m) = \emptyset$ et c'est évident. Si $n = 1$,

$$\sum_{\substack{0\le\gamma\le g-1\\ 0\le i\le N}} a_{i,j}^{(\gamma)} = \sum_{i,\gamma} \mathcal{X}_{D_\gamma(j)}(i)$$

$$= \sum_{\gamma} \operatorname{Card} D_\gamma(j) = \operatorname{Card} C,$$

où $\mathcal{X}_{D_\gamma(j)}$ est la fonction indicatrice de $D_\gamma(j)$. Supposons le résultat vrai pour $n-1$ avec $n \ge 2$. Tout mot (m) de longueur n s'écrit de manière unique $(m) = (m'\gamma)$ avec $\gamma \in \{0, 1, \dots, g-1\}$ et $|(m')| = n-1$ d'où

$$\sum_{\substack{|(m)|=n\\ 0\le i\le N}} a_{i,j}^{(m)} = \sum_{\substack{i,\gamma\\ |(m')|=n-1}} \sum_{k} a_{i,k}^{(m')} a_{k,j}^{(\gamma)} = \sum_{\gamma,k} a_{k,j}^{(\gamma)} (\operatorname{Card} C)^{n-1}$$

$$= (\operatorname{Card} C)^n.$$

PROPOSITION 1.

i) Si $g >$ Card C alors $0 \in \mathcal{M}$.

ii) Si $g <$ Card C alors $N(A_{(m)})$ est non borné.

iii) Si $g =$ Card C et si $N(A_{(m_0)})$ est un extremum de $N(A_{(m)})$, alors pour tout mot (m) on a $N(A_{(m_0)}) = N(A_{(mm_0)})$.

Démonstration.

D'après le lemme 2 avec $n = 1$, on a :

$$\sum_{\gamma=0,\dots,g-1} N(A_{(\gamma m_0)}) = \sum_{i,j,k,\gamma} a_{i,k}^{(\gamma)} a_{k,j}^{(m_0)} = \sum_{j,k} a_{k,j}^{(m_0)} \cdot \operatorname{Card} C$$

$$= (\operatorname{Card} C)\, N(A_{(m_0)}) \qquad (*).$$

i) Soit (m_0) tel que $N(A_{(m_0)}) = \min\{N(A_{(m)}),\ A_{(m)} \in \mathcal{M}\}$. On a alors

$$\sum_{\gamma=0}^{g-1} N(A_{(\gamma m_0)}) \ge g N(A_{(m_0)})$$

et avec la relation $(*)$ on en déduit $N(A_{(m_0)}) = 0$ puis $A_{(m_0)} = 0$.

ii) On raisonne par l'absurde.

Soit (m_0) tel que $N(A_{(m_0)}) = \max\{N(A_{(m)}),\ A_{(m)} \in \mathcal{M}\}$.

Cette fois-ci $\sum_{\gamma=0}^{g-1} N(A_{(\gamma m_0)}) \leq gN(A_{(m_0)})$ et $(*)$ donne $N(A_{(\gamma m_0)}) = 0$ puis $\mathcal{M} = \{0\}$ ce qui est absurde.

iii) Cette fois ci on doit avoir l'égalité $N(A_{(\gamma m_0)}) = N(A_{(m_0)})$ pour $\gamma = 0, 1, \ldots, g-1$. D'où le résultat de proche en proche.

COROLLAIRE. *Si $g >$ Card C, il existe des nombres arbitrairement grands ne s'écrivant pas sous la forme $\sum c_k g^k$ et si $g <$ Card C, alors C n'est pas g-libre.*

Ce sont des conséquences claires de *i)* et *ii)*. On peut aussi retrouver facilement ces résultats par une attaque directe du problème.

II. Opérateurs polynomiaux associés à $\mathcal{M}$.

1. Définition

On note $\mathcal{E}$ la $\mathbb{R}$-algèbre engendrée par X et $\frac{1}{X}$. Elle admet $\{X^i,\ i \in \mathbb{Z}\}$ pour base vectorielle. On note E le sous-espace vectoriel de dimension $N+1$ engendré par les X^i avec $i = 0, \ldots, N$. On définit les opérateurs B et T par :

$$B(X^i) = X^{i'}.\delta_{r,0} \quad \text{où } i = gi' + r,\ 0 \leq r \leq g-1,\ i \in \mathbb{Z},\ i' \in \mathbb{Z},$$
$$T(H) = XH \quad \text{pour } H \in \mathcal{E}.$$

On a évidemment $T^{-1}(H) = \dfrac{H}{X}$. On a d'autre part les relations :

$$TB = BT^g \quad \text{et} \quad T^{-1}B = BT^{-g} \tag{1}$$

On pose $P_n(X) = P(X)P(X^g)\ldots P(X^{g^{n-1}})$ où $P = \sum_{c \in C} X^c$.

3. Condition nécessaire et suffisante lorsque $g =$ Card C pour que C soit g-libre

Etablissons tout d'abord quelques résultats préliminaires.

PROPOSITION 2. *Soit (m) le mot $(\gamma_{n-1} \ldots \gamma_0)$ et $m = \sum_{i=0}^{n-1} \gamma_i g^i$. L'opérateur $B^n P_n(T) T^{-m}$ laisse E stable et la matrice de sa restriction à E relativement à la base canonique est $A_{(m)}$ (on suppose $n \geq 1$).*

Démonstration. On raisonne par récurrence sur $n \geq 1$.

• Pour $n = 1$. Soit $\gamma \in \{0, \ldots, g-1\}$

$$P(T)T^{-\gamma} = \sum_{c \in C} T^{c-\gamma} \quad \text{et} \quad BP(T)T^{-\gamma}(X^j) = \sum_{c \in C} B(X^{j+c-\gamma}) = \sum_{i \in D_{(\gamma)}(j)} X^i.$$

•• Supposons que ce soit vrai pour les mots de longueur $n-1$, $n \geq 2$. Soit $(m) = (\gamma m')$ avec $|(m')| = n-1$. On a $m = \gamma g^{n-1} + m'$.

$A_{(m)} = A_{(\gamma)}A_{(m')}$ c'est la matrice de la restriction

de $BP(T)T^{-\gamma}.B^{n-1}P_{n-1}(T)T^{-m'}$.

En itérant (1) $n-1$ fois on en déduit le résultat.

LEMME 3. *On suppose $g = \mathrm{Card}\, C$ alors :*

i) *C g-libre est équivalent à $N(A_{(m)})$ borné.*

ii) *C g-libre entraîne $0 \notin \mathcal{M}$.*

Démonstration.

i) Si C est g-libre alors $a_{i,j}^{(m)} \leq 1$ d'où $N(A_{(m)}) \leq (N+1)^2$. Réciproquement si C n'est pas g-libre alors pour un certain (m_1) on a $a_{0,0}^{(m_1)} \geq 2$ et si on note $(m_n) = \underbrace{(m_1 m_1 \cdots m_1)}_{n \text{ fois}}$ on a $a_{0,0}^{(m_n)} = \sum_{i_1, \ldots, i_{n-1}} a_{0,i_1}^{(m_1)} a_{i_1,i_2}^{(m_1)} \ldots a_{i_{n-1},0}^{(m_1)} \geq \left[a_{0,0}^{(m_1)}\right]^n$ non borné.

ii) D'après le lemme 2 :

$$\sum_{|(m)|=n} N(A_{(m)}) = \sum_j \sum_{i, |(m)|=n} a_{i,j}^{(m)} = (N+1)g^n.$$

Si $0 \in \mathcal{M}$, soit (m_0) tel que $A_{(m_0)} = 0$. Puisque C est g-libre, on sait d'après i) qu'il existe M tel que $N(A_{(m)}) \leq M$ pour tout mot (m). D'où

$$\sum_{|(m)|=nn_0} N(A_{(m)}) = \sum_{\substack{(m)=(m_1 \ldots m_n) \\ (m_i) \neq (m_0) \\ 0 \leq i \leq n, |(m_i)|=n_0}} N(A_{(m)}) \leq M(g^{n_0}-1)^n,$$

ce qui est absurde car $M(g^{n_0}-1)^n = o(g^{n_0 n})$.

LEMME 4. *Soit Q un polynôme. On a pour tout entier $n \geq 1$*

$$B^n(Q)(1) = \frac{1}{g^n} \sum_{\theta \in U_{g^n}} Q(\theta).$$

Démonstration.

Si $Q = \alpha_0 + \cdots + \alpha_l X^l$ alors $B(Q) = \sum_{g|i} \alpha_i X^i$; en itérant cette relation on obtient $B^n(Q)(1) = \sum_{g^n|i} \alpha_i$. Posons $S_k = \sum_{\theta \in U_h} \theta^k$. En multipliant par ω^k où ω est une racine primitive h-ième de l'unité

$$\omega^k S_k = \sum_{\theta \in U_h} (\omega\theta)^k = S_k.$$

On en déduit $S_k = 0$ si h ne divise pas k et $S_k = h$ si h divise k. Le lemme en résulte par la linéarité de B^n et le choix $h = g^n$.

Nous sommes maintenant en mesure d'établir le

TÉORÈME. *Soit C une partie de $\mathbb{N}$, contenant 0, de cardinal g. On définit les polynômes*

$$P = \sum_{c \in C} X^c \qquad et \qquad P_n = \prod_{h=0}^{n-1} P(X^{g^h}) \quad (n \geq 1).$$

On note Z_n l'ensemble des racines de P_n et U_{g^n} l'ensembles des racines g^n-ièmes de l'unité.

Pour que C soit g-libre il faut et il suffit que $Card\,(U_{g^n} \setminus Z_n)$ soit majoré indépendament de n.

Démonstration. Pour tout mot (m)

$$A_{(m)} \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \qquad \alpha_i = \sum_{j=0}^{N} a_{i,j}^{(m)} \quad (0 \leq i \leq N).$$

On en déduit en posant $R = \sum_{i=0}^{N} X^i$ que :

$$N(A_{(m)}) = B^n P_n(T) T^{-m}(R)(1). \tag{2}$$

Supposons maintenant C g-libre et soit (m_0) tel que $N(A_{(m_0)})$ soit le minimum des $N(A_{(m)})$. On sait qu'alors $N(A_{(mm_0)}) = N(A_{(m_0)})$ pour tout mot (m) (voir Proposition 1). Or

$$N(A_{(m)}) = B^n P_n(T) T^{-m}(R)(1)$$

et $$N(A_{(m)}A_{(m_0)}) = B^n P_n(T) T^{-m} B^{n_0} P_{n_0}(T) T^{-m_0}(R)(1).$$

En posant $S = B^{n_0} P_{n_0}(T) T^{-m_0} R$, on a

$$B^n[P_n(T)T^{-m}(S)](1) = N(A_{(m_0)}) = S(1).$$

En appliquant (2) on en déduit :

$$\frac{1}{g^n} \sum_{\theta \in U_{g^n}} P_n(\theta)\theta^{-m} S(\theta) = S(1).$$

et, si θ_n désigne une racine g^n-ième primitive de l'unité :

$$\frac{1}{g^n} \sum_{k=0}^{g^n-1} P_n(\theta_n^k)\theta_n^{-km} S(\theta_n^k) = S(1).$$

Pour $k = 0$, $P_n(\theta_n^k)\theta_n^{-mk} S(\theta_n^k) = g^n S(1)$. On en déduit que le polynôme :

$$\sum_{k=1}^{g^n-1} P_n(\theta_n^k) S(\theta_n^k) X^k,$$

qui est au plus de degré $g^n - 1$, admet tous les θ_n^{-m} avec $|(m)| = n$ pour racines. Cela donne g^n racines et donc le polynôme est nul. Or, d'après le lemme 2, $S \neq 0$ et par conséquent si W désigne l'ensemble des racines de S de module 1 union $\{1\}$, on a $U_{g^n} \subset (Z_n \cup W)$ et $\mathrm{Card}(U_{g^n} \setminus Z_n)$ est majoré.

Réciproquement supposons que $U_{g^n} \setminus Z_n$ soit de cardinal majoré par M indépendant de n. D'après (2)

$$\begin{aligned} N(A_{(m)}) &= \frac{1}{g^n} \sum_{\theta \in R_{g^n}} P_n(\theta) R(\theta) \theta^{-m} \\ &\leq \frac{1}{g^n} \sum_{\theta \in U_{g^n}} |P_n(\theta) R(\theta)| \\ &\leq \frac{1}{g^n} \sum_{\substack{\theta \notin Z_n \\ \theta \in U_{g^n}}} P_n(1)(N+1) \leq \frac{g^n(N+1)}{g^n} M, \end{aligned}$$

et le lemme 3 permet de conclure.

COROLLAIRE. *Prenons $g = 4$ et écrivons les entiers à l'aide des chiffres $\{-1, 0, 1, 2\}$. Tout nombre entier, $\neq 0$, dont le premier chiffre non nul, en partant de la droite, n'est pas 2 dans sa décomposition en base 4, est le quotient de deux nombres s'écrivant uniquement avec des 0, 1 et -1.(Loxton et Van der Poorten [1]).*

Démonstration. L'entier k s'écrit sous la forme voulue si et seulement s'il existe des entiers s_1, s_1', s_2, s_2' s'écrivant uniquement à l'aide de 0 et 1 tels que $k = \frac{s_1' - s_1}{s_2' - s_2}$ ce qui équivaut à $s_2 k + s_1 = s_2' k + s_1'$ avec $(s_1, s_2) \neq (s_1', s_2')$, ce qui équivaut à $\{0, 1, k, k+1\}$ n'est pas 4-libre.

Le polynôme associé est $P = (1+X)(1+X^k)$. Si $k = 4^\alpha k'$ avec k' impair, alors tous les éléments θ de U_{g^n} d'ordre 4^h avec $0 \leq h \leq n$ ne sont pas dans Z_n. Il s'ensuit que Card $(U_{g^n} \setminus Z_n)$ est non borné et $\{0, 1, k, k+1\}$ n'est pas 4-libre. Par contre, si $k \equiv 2.4^\alpha \bmod 4^{\alpha+1}$ pour un certain entier α, alors $U_{g^n} \subset Z_n \cup U_{g^\alpha}$.

BIBLIOGRAPHIE

[1] J. H. LOXTON et A. J. van der POORTEN, *An awful problem about integers in base 4*, Acta Arith. 49 (1987), 193-203.

[2] G. RAUZY, *Systèmes de numération*, Journées de théorie élémentaire et analytique des nombres, 1982, Valenciennes.

P. GONZALEZ
204, rue d'Endoume,
13007 MARSEILLE
France