JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Jean-Marc DESHOUILLERS

Quand seule la sous-somme vide est nulle modulo p

Tome 19, n° 1 (2007), p. 71-79.

<http://jtnb.cedram.org/item?id=JTNB_2007__19_1_71_0>

Journal de Théorie des Nombres
de Bordeaux **19** (2007), 71-79

Quand seule la sous-somme vide est nulle modulo p

par Jean-Marc DESHOUILLERS

Résumé. Soit $c > 1$, p un nombre premier et $\mathcal{A}$ une partie de $\mathbb{Z}/p\mathbb{Z}$ de cardinal supérieur à $c\sqrt{p}$ telle que pour tout sous-ensemble non vide $\mathcal{B}$ de $\mathcal{A}$, on a $\sum_{b\in\mathcal{B}} b \neq 0$. On montre qu'il existe s premier à p tel que l'ensemble $s.\mathcal{A}$ est très concentré autour de l'origine et qu'il est presque entièrement composé d'éléments de partie fractionnaire positive. Plus précisément, on a

$$\sum_{a\in\mathcal{A}} \|\frac{sa}{p}\| < 1 + O(p^{-1/4}\ln p) \quad \text{et} \quad \sum_{\substack{a\in\mathcal{A},\\ \{sa/p\}\geq 1/2}} \|\frac{sa}{p}\| = O(p^{-1/4}\ln p).$$

On montre également que les termes d'erreurs ne peuvent être remplacés par $o(p^{-1/2})$.

Abstract. Let $c > 1$, p be a prime number and $\mathcal{A}$ a subset of $\mathbb{Z}/p\mathbb{Z}$ with cardinality larger than $c\sqrt{p}$ and such that for any non empty subset $\mathcal{B}$ of $\mathcal{A}$, one has $\sum_{b\in\mathcal{B}} b \neq 0$. We show that there exists s coprime with p such that the set $s.\mathcal{A}$ is very concentrated around the origin, and that it is almost exclusively composed of elements with a positive fractional part. More precisely, one has

$$\sum_{a\in\mathcal{A}} \|\frac{sa}{p}\| < 1 + O(p^{-1/4}\ln p) \quad \text{and} \quad \sum_{\substack{a\in\mathcal{A},\\ \{sa/p\}\geq 1/2}} \|\frac{sa}{p}\| = O(p^{-1/4}\ln p).$$

We also show that the error terms cannot be replaced by $o(p^{-1/2})$.

1. Introduction

1.1 Soit p un nombre premier et $\mathcal{A}$ un sous-ensemble de $\mathbb{Z}/p\mathbb{Z}$. P. Erdős et H. Heilbronn [3] ont posé en 1964 la question de trouver une constante c telle que si $\operatorname{card}\mathcal{A} \geq c\sqrt{p}$, alors $\mathcal{A}$ contient un sous-ensemble non vide dont la somme des termes est égale à 0. Ils ont fourni une construction d'un ensemble $\mathcal{A}$ de cardinal $\lfloor\sqrt{2p}-1\rfloor$ tel que la somme des termes de tout sous-ensemble non vide de $\mathcal{A}$ est non nulle. L'existence d'une telle constante c a

Manuscrit reçu le 15 janvier 2006.
Supported by Université Victor Segalen Bordeaux 2 (EA 2961), Université Bordeaux1 and CNRS (UMR 5465).

été obtenue en 1968 par Olson [4] avec la valeur admissible $c = 2$, comme conséquence d'un résultat plus général. En 1996, Y. Ould Hamidoune et G. Zémor [5] ont montré que la condition $\operatorname{card} \mathcal{A} \geq \sqrt{2p} + 5 \ln p$ implique que $\mathcal{A}$ contient un sous-ensemble non vide dont la somme des termes est égale à 0.

Nous donnons ici une information sur la structure des sous-ensembles $\mathcal{A}$ de $\mathbb{Z}/p\mathbb{Z}$ dont le cardinal est sensiblement supérieur à $\sqrt{p}$ et dont seule la sous-somme vide est nulle. Nous montrons comment la méthode introduite en collaboration avec G. A. Freiman [2] permet de montrer le résultat suivant :

Théorème 1. *Soit $c > 1$, p un nombre premier et $\mathcal{A}$ une partie de $\mathbb{Z}/p\mathbb{Z}$ de cardinal supérieur à $c\sqrt{p}$ telle que pour tout sous-ensemble non vide $\mathcal{B}$ de $\mathcal{A}$, on a $\sum_{b\in\mathcal{B}} b \neq 0$. Il existe un entier s premier à p tel que l'on a*

$$(1) \quad \sum_{a\in\mathcal{A}} \|\frac{sa}{p}\| < 1 + O(p^{-1/4}\ln p) \quad \textit{et} \quad \sum_{\substack{a\in\mathcal{A},\\ \{sa/p\}\geq 1/2}} \|\frac{sa}{p}\| = O(p^{-1/4}\ln p).$$

Nous conjecturons que les termes d'erreur peuvent être réduits à $O(p^{-1/2})$; ce résultat serait optimal, car la construction donnée en [1] s'adapte facilement pour démontrer le résultat suivant

Théorème 2. *Soit $0 < c < \sqrt{2}$. Il existe un nombre réel strictement positif K tel que pour tout nombre premier p suffisamment grand, il existe un sous-ensemble $\mathcal{A}$ of $\mathbb{Z}/p\mathbb{Z}$ de cardinal supérieur à $c\sqrt{p}$, tel que pour tout entier s premier à p on a*

$$(2) \quad \sum_{a\in\mathcal{A}} \|\frac{as}{p}\| > 1 + Kp^{-1/2} \quad \textit{et} \quad \sum_{a\in\mathcal{A},\{sa/p\}\geq 1/2} \|\frac{sa}{p}\| > Kp^{-1/2}$$

et tel que la somme des éléments de tout sous-ensemble non vide de $\mathcal{A}$ est non nulle.

Gyan Prakash et l'auteur ont utilisé le Théorème 1 pour démontrer que le cardinal d'un sous-ensemble maximal $\mathcal{A}$ de $\mathbb{Z}/p\mathbb{Z}$ dont seule la sous-somme vide est nulle est le plus grand entier k tel que $\sum_{1\leq n\leq k} \leq p+1$. *Note ajoutée lors de la révision de l'article.*

1.2 Notations. Pour un nombre réel u, on note $e_p(u) = \exp(\frac{2\pi i u}{p})$, $\|u\| = \min_{z\in\mathbb{Z}} |u - z|$ et $\{u\}$ la partie fractionnaire de u ; quand $b \in \mathbb{Z}/p\mathbb{Z}$, l'expression $e_p(b)$ (resp. $\|b/p\|$, resp. $\{b/p\}$) représente la valeur commune de toutes les quantités $e_p(\tilde{b})$ (resp. $\|\tilde{b}/p\|$, resp. $\{\tilde{b}/p\}$) où $\tilde{b}$ est n'importe quel entier représentant la classe de b ; on dénote par $|b|$ le minimum de $|\tilde{b}|$ pris sur tous les représentants $\tilde{b}$ de b, ou, de façon équivalente $|b| = p\|b/p\|$ et par $\langle b\rangle$ le reste de la division euclidienne de n'importe quel représentant $\tilde{b}$ de b par p, ou, de façon équivalente $\langle b\rangle = p\{\tilde{b}/p\}$.

La lettre p dénote un nombre premier suffisamment grand pour satisfaire à toutes les inégalités explicites ou implicites dans lesquelles il est impliqué (pour l'essentiel, des comparaisons de constantes et de puissances de logarithmes).

Quand une *famille*, c'est-à-dire une collection d'éléments où les répétitions sont permises (*multiset* en anglais), est décrite par ses éléments, on les indique entre double accolade, par exemple $\mathcal{A} = \{\{0, 1, 1\}\} = \{\{a_1, a_2, a_3\}\}$. Pour une telle famille $\mathcal{A}$ dont les éléments appartiennent à un groupe abélien, on note $\mathcal{A}^*$ l'ensemble (sic) des sommes de ses parties, c'est-à-dire $\mathcal{A}^* = \{\sum_{b\in\mathcal{B}} b,\, \mathcal{B} \subset \mathcal{A}\}$, où la somme prise sur l'ensemble vide est 0, et de même on note $\mathcal{A}^\sharp = \{\sum_{b\in\mathcal{B}} b,\, \emptyset \neq \mathcal{B} \subset \mathcal{A}\}$; on a donc $\mathcal{A}^* = \mathcal{A}^\sharp \cup \{0\}$. Pour une sous-famille, ou un sous-ensemble, $\mathcal{A}$ d'un groupe abélien et un entier positif s, on note $s \cdot \mathcal{A}$ la famille, ou l'ensemble, constituée des multiples par s de ses éléments ; dans le cas où $\mathcal{A}$ est constitué d'entiers multiples de s, on note $(1/s) \cdot \mathcal{A}$ la famille, ou l'ensemble, des éléments de $\mathcal{A}$ divisés par s. Enfin, le cardinal d'un ensemble, ou d'une famille, $\mathcal{A}$ est noté indifféremment $\mathrm{Card}(\mathcal{A})$ ou $|\mathcal{A}|$.

1.3 Remerciements. Une partie de ce travail a été effectuée lorsque l'auteur séjournait à l'**I**nstitute for **M**athematical **Sc**iences de Chennai ; il remercie cette institution ainsi que l'**I**nstitut **F**ranco-**I**ndien de **M**athématiques et le **CE**ntre **F**ranco-**I**ndien pour la **P**romotion de la **R**echerche **A**vancée pour leur soutien.

2. Résultats préliminaires

Lemme 1. *Soit $\mathcal{G}$ un groupe abélien fini avec $q \geq 2$ éléments et $\mathcal{A}$ une famille de m éléments non nuls de $\mathcal{G}$ avec $m \geq q - 1$. Alors, ou bien il existe une sous-famille $\mathcal{B}$ de $\mathcal{A}$ avec $q - 1$ éléments telle que $\mathcal{B}^* = \mathcal{G}$, ou bien il existe un sous-groupe $\mathcal{H}$ de $\mathcal{G}$ différent de $\{0\}$ et $\mathcal{G}$ tel que moins de $\mathrm{Card}(\mathcal{G}/\mathcal{H}) - 1$ éléments de $\mathcal{A}$ ne sont pas dans $\mathcal{H}$.*

C'est le second lemme de [2].

Lemme 2. *Soit d un entier positif et $\mathcal{L}$ une famille d'entiers de cardinal supérieur ou égal à d. Il existe $\mathcal{D} \subset \mathcal{L}$ avec $|\mathcal{D}| \leq d - 1$ tel que pour tout y de $(\mathcal{L}\backslash\mathcal{D})^\sharp$, il existe z dans $\mathcal{D}^*$ congru à $-y$ modulo d.*

Démonstration du Lemme 2. On procède par récurrence sur d. Le lemme est clairement valide pour $d = 1$, car $\emptyset^* = \{0\}$. On le suppose établi pour tout $d < \delta$, où δ est un entier supérieur à 1 donné. Si $\mathcal{L}$ contient moins de $\delta - 1$ éléments qui ne sont pas congrus à 0 modulo δ, on note $\mathcal{D}$ cette famille et on remarque que tout élément de $(\mathcal{L}\backslash\mathcal{D})^\sharp$ est congru à 0 modulo δ, tandis que $\mathcal{D}^*$ contient 0. Dans le cas contraire, on note $\mathcal{L}_1$ la famille des éléments de $\mathcal{L}$ qui ne sont pas congrus à 0 modulo δ, et on

applique le Lemme 1, ce qui conduit à distinguer deux cas :
– ou bien $\mathcal{L}_1$ contient une famille $\mathcal{D}$ avec $\delta-1$ éléments telle que $\mathcal{D}^*$ couvre tous les résidus modulo δ, auquel cas le lemme est vérifié pour $d=\delta$;
– ou bien il existe un diviseur δ_1 de δ, avec $2\le\delta_1<\delta$, tel qu'au plus (δ/δ_1-1) éléments de $\mathcal{L}_1$ ne sont pas divisibles par δ_1. Dans ce cas, il y a également au plus (δ/δ_1-1) éléments de $\mathcal{L}$ qui ne sont pas divisibles par δ_1 ; on note alors $\mathcal{D}_1$ cette famille et on considère $\mathcal{L}_2=(1/\delta 1)\cdot(\mathcal{L}\backslash\mathcal{D}_1)$; le cardinal de $\mathcal{L}_2$ est au moins $\delta-(\delta/\delta_1-1)\ge\delta/\delta_1$; par l'hypothèse de récurrence, on peut trouver $\mathcal{D}_2$ dans $\mathcal{L}_2$ avec $|\mathcal{D}_2|\le\delta/\delta_1-1$ et tel que pour tout y_2 de $(\mathcal{L}_2\backslash\mathcal{D}_2)^\sharp$ il existe z_2 dans $\mathcal{D}_2^*$ congru à $-y_2$ modulo δ/δ_1. On pose alors $\mathcal{D}=\mathcal{D}_1\cup(\delta_1\cdot\delta_2)$ et on a bien $\mathcal{D}\subset\mathcal{L}$, $|\mathcal{D}|\le\delta-1$ et $\mathcal{D}$ satisfait aux conditions requises dans l'énoncé du lemme pour $d=\delta$. □

Théorème 3. *Soit $I>L>100$ et $B>2C\ln L$ des entiers positifs tels que*

$$C^2>500L(\ln L)^2+2000I\ln L.$$

Soit $\mathcal{B}$ un ensemble de B entiers inclus dans $[-L\,,\,L]$. Alors, il existe $d>0$ et un sous-ensemble $\mathcal{C}$ de $\mathcal{B}$ de cardinal C tel que
(i) tous les éléments de $\mathcal{C}$ sont divisibles par d,
(ii) $\mathcal{C}^*$ contient une progression arithmétique avec I termes et de raison d,
(iii) au plus $C\ln L$ éléments de $\mathcal{B}$ ne sont pas divisibles par d.

C'est le second théorème de [2].

Théorème 4. *Soit x un entier suffisamment grand et $\mathcal{K}$, et $\mathcal{L}$ deux ensembles d'entiers inclus dans $]0\,,\,x]$ tels que l'on ait*

(i) $\quad|\mathcal{K}|\ge 50x^{1/2}\ln^2 x,$

(ii) $\quad\sum_{\ell\in\mathcal{L}}\ell\ge 27x^{3/2}\ln x.$

Alors, on a $\mathcal{K}^\sharp\cap\mathcal{L}^\sharp\ne\emptyset$.

Démonstration du Théorème 4. On applique le Théorème 3 pour l'ensemble $\mathcal{B}=\mathcal{K}$, avec $I=\lfloor 0,04\,x\ln x\rfloor$, $L=x$ et $C=\lfloor 24\,x^{1/2}\ln x\rfloor$; soit alors d et $\mathcal{C}$ le nombre réel et l'ensemble introduits par le Théorème 3. Puisque d divise au moins la moitié des éléments de $\mathcal{K}$, on a $d\le 0,04\,x^{1/2}\ln^{-2}x$. Notons $\mathcal{I}$ la progression arithmétique de I termes et de raison d dont l'existence est affirmée par le Théorème 3. Son plus grand terme, qui est élément de $\mathcal{C}^*$, est inférieur ou égal à $|\mathcal{C}|x$ et donc à $25\,x^{3/2}\ln x$; par ailleurs, il est supérieur ou égal à $(I-1)d$ et donc à $0,03\,dx\ln x$.

Puisque les éléments de $\mathcal{L}$ sont au plus égaux à x, il y en a au moins $27\,x^{1/2}\ln x$, et donc $|\mathcal{L}|>d$: on peut donc appliquer le Lemme 2 à l'ensemble $\mathcal{L}$ avec le nombre d que nous venons d'introduire ; on note que l'ensemble $\mathcal{D}$ obtenu a au plus $0,04\,x^{1/2}\ln^{-2}x$ éléments et $\mathcal{L}\backslash\mathcal{D}$ en a au moins $26,5\,x^{1/2}\ln x$. Soit t un entier compris entre $0,02\,dx\ln x$ et $25\,x^{3/2}\ln x$;

puisque tous les éléments de $\mathcal{L}\backslash\mathcal{D}$ sont au plus égaux à x et que leur somme est supérieure à $27\,x^{3/2}\ln x\,-\,d\,x\geq 26\,x^{3/2}\ln x$, il existe un élément y de $(\mathcal{L}\backslash\mathcal{D})^\sharp$ compris entre t et $t+x$. Par le Lemme 2, il existe z dans $\mathcal{D}^*$ congru à $-y$ modulo d. L'élément $y+z$ est dans $\mathcal{D}^*+(\mathcal{L}\backslash\mathcal{D})^\sharp\subset\mathcal{L}^\sharp$: nous venons de montrer que tout entier congru à 0 modulo d compris entre $0,02\,d\,x\ln x+d\,x$ et $25\,x^{3/2}\ln x\,+\,d\,x$ est dans $\mathcal{L}^\sharp$. Mais l'un de ces éléments est un élément non nul de $\mathcal{C}^*$; il est donc dans $\mathcal{C}^\sharp$ et *a fortiori* dans $\mathcal{K}^\sharp$. □

3. Démonstration du Théorème 1

3.1 La démonstration de la deuxième proposition de [2] n'est valable que lorsqu'il existe x différent de zéro qui n'appartient pas à $\mathcal{A}^*$. Dans le cas considéré en [2], cette hypothèse était justifiée par le fait que 0, somme sur la partie vide, est bien un élément de $\mathcal{A}^*$. La proposition suivante traite du cas $x=0$, qui nous intéresse ici ; la démonstration est très proche de celle de la deuxième proposition de [2].

Proposition 1. *Soit p un nombre premier et $\mathcal{A}$ un sous-ensemble de $\mathbb{Z}/p\mathbb{Z}$ tel que $0\notin\mathcal{A}^\sharp$ et $|\mathcal{A}|>\frac{2\ln p}{\ln 2}$. Il existe $t\neq 0$ dans $\mathbb{Z}/p\mathbb{Z}$ tel que*

$$\exp(-\pi\sum_{a\in\mathcal{A}}\|\frac{at}{p}\|^2)>\frac{1}{p} \tag{3}$$

et, pour tout $u>0$, on a

$$\mathrm{Card}\{a\in\mathcal{A}\,;\|\frac{at}{p}\|\geq u^{-1}\}\leq u^2\ln p. \tag{4}$$

Démonstration de la Proposition 1. Pour toute famille non vide $\{a_i\}_{i\leq r}$ d'éléments deux à deux distincts de $\mathcal{A}$, la somme $a_1+\cdots+a_r$ est non nulle et on a

$$\sum_{t\mod p}e_p(t(a_1+\cdots+a_r))=0\,;$$

pour la famille vide, dont la somme est nulle, la même expression vaut p. En sommant sur tous les sous-ensembles de $\mathcal{A}$ et en utilisant la multiplicativité de l'exponentielle, on obtient

$$\sum_{t\mod p}\prod_{a\in\mathcal{A}}(1+e_p(ta))=p.$$

On sépare alors la contribution de $t=0$, d'où l'on déduit

$$2^{|\mathcal{A}|}+\sum_{t\neq 0}\prod_{a\in\mathcal{A}}(1+e_p(ta))=p.$$

Cela implique qu'il existe $t\neq 0$ tel que

$$\prod_{a\in\mathcal{A}}|1+e_p(ta)|\geq\frac{2^{|\mathcal{A}|}-p}{p-1}>\frac{2^{|\mathcal{A}|}}{p}. \tag{5}$$

Par la formule de Taylor, on établit aisément (cf. [2]) l'inégalité

$$|1+\exp(2\pi iy)| \le 2\exp(-\pi\|y\|^2). \tag{6}$$

La Relation (3) provient de (5) et (6). Si l'on suppose que (4) n'a pas lieu, on a

$$\exp(-\pi\sum_{a\in\mathcal{A}}\|\frac{at}{p}\|^2) \le \exp(-\pi.\log p) = p^{-\pi} < p^{-1},$$

en contradiction avec (3). □

3.2 Nous omettons la preuve du résultat suivant, qui est identique à celle de la Proposition 3 de [2].

Proposition 2. *Soit p un nombre premier suffisamment grand. Soit $\mathcal{A}$ une partie de $\mathbb{Z}/p\mathbb{Z}$ telle que $|\mathcal{A}| \ge 0,1\sqrt{p}$ et $0 \notin \mathcal{A}^\sharp$, et soit $I = \lfloor p^{0.9}\rfloor$. Il existe s, premier à p, tel que*

$$|\{a\in\mathcal{A}, \|as/p\| \ge I^{-1/4}\}| \le 2I^{1/2}\ln^2 p$$

et $s\cdot\mathcal{A}$ contient un sous-ensemble $\mathcal{C}$ avec au plus $I^{1/2}\ln^2 p$ éléments tel que $\mathcal{C}^*$ contient un intervalle avec au moins I éléments.

3.3 Jusqu'à la fin de cet article, $\mathcal{A}$ désigne un sous-ensemble de $\mathbb{Z}/p\mathbb{Z}$ satisfaisant aux hypothèses du Théorème 1. On peut appliquer à $\mathcal{A}$ la Proposition 2 ; on note $\mathcal{B} = \{sa, a\in\mathcal{A}, |sa| < p^{0,8}\}$ et on écrit $\mathcal{E} = \mathcal{B}\backslash\mathcal{C}$; puisque la différence entre deux éléments de $\mathcal{E}$ est au plus $2p^{0,8} < \lfloor p^{0,9}\rfloor = I$, l'ensemble $\mathcal{E}^\sharp + \mathcal{C}^*$ contient un intervalle, et puisqu'il est inclus dans $(s\cdot\mathcal{A})^\sharp$, qui ne contient pas 0, sa longueur est au plus égale à p. Cela implique la majoration $\sum_{e\in\mathcal{E}}|e| < p$, d'où l'on déduit que pour tout $\lambda > 0$ on a $|\{e\in\mathcal{E}, |e| \ge \lambda\sqrt{p}\}| \le \lambda^{-1}\sqrt{p}$.

Soit $\lambda = 2(c-1)^{-1}$, $\mathcal{D} = \{e\in\mathcal{E}, |e| < \lambda\sqrt{p}\}$, $\mathcal{D}_1$ l'image naturelle de $\mathcal{D}$ dans $[-\lambda\sqrt{p}\,,\,\lambda\sqrt{p}]$, $\mathcal{D}_1^+ = \mathcal{D}_1\cap]0\,,\,\lambda\sqrt{p}]$ et $\mathcal{D}_1^- = \mathcal{D}_1\cap[-\lambda\sqrt{p}\,,\,0[$. Quitte à changer s en $-s$, on peut supposer sans perte de généralité que $|\mathcal{D}_1^+| \ge |\mathcal{D}_1^-|$, et on a donc $|\mathcal{D}_1^+| \ge 0,5\sqrt{p}$. Si on a $\sum_{d\in\mathcal{D}_1^-}|d| > 27\,(\lambda\sqrt{p})^{3/2}\ln(\lambda\sqrt{p})$, le Théorème 4 implique que $(\mathcal{D}_1^+)^\sharp$ et $((-1)\cdot\mathcal{D}_1^-)^\sharp$ ont un élément en commun, ce qui contredit le fait que 0 n'est pas dans $\mathcal{A}^\sharp$ et donc pas dans $(s\cdot\mathcal{A})^\sharp$. On a donc montré que $\sum_{d\in\mathcal{D}_1^-}|d| = O(p^{3/4}\ln p)$. Il en résulte que $|\mathcal{D}_1^-| = O(p^{3/8}\ln p)$, et donc $|\mathcal{D}_1^+| \ge (c+2)/3\,\sqrt{p}$.

On applique le Théorème 3 à $\mathcal{D}_1^+$, avec $L = \lfloor\lambda\sqrt{p}\rfloor$, $I = L+1$ et $C = \lfloor 25\,L^{1/2}\ln L\rfloor$; puisque $\mathcal{D}_1^+$, inclus dans $]0\,,\,\lambda\sqrt{p}]$, contient au moins $(c+2)/3\,\sqrt{p}$ éléments, l'élément d dont le Théorème 3 affirme l'existence est $O(1)$. On prend pour d le plus grand tel élément. Au moins $(c+3)/4\,\sqrt{p}$ termes de $\mathcal{D}_1^+$ sont divisibles par d. On note $\bar{d}$ l'inverse de d modulo p et

$u \equiv \bar{d}s \mod p$. Considérons l'ensemble $\mathcal{B} = u \cdot \mathcal{A}$ et notons $\bar{\mathcal{B}}$ son image naturelle dans $]-p/2\,,\,p/2]$, $\mathcal{B}_1^+ = \bar{\mathcal{B}} \cap]0\,,\,\lambda\sqrt{p}]$ et $\mathcal{B}_1^- = \bar{\mathcal{B}} \cap [-\lambda\sqrt{p}\,,\,0[$. Par construction, on a

$$|\mathcal{B}_1^+| \geq (c+3)/4\,\sqrt{p}. \tag{7}$$

On applique – c'est la dernière fois ! – le Théorème 3 à $\mathcal{B}_1^+$, avec $L = \lfloor \lambda\sqrt{p} \rfloor$, $I = L+1$ et $C = \lfloor 25\,L^{1/2} \ln L \rfloor$; le caractère maximal du nombre d choisi à l'étape précédente implique que le nouveau d obtenu vaut 1 : il existe donc un sous-ensemble $\mathcal{C}$ de $\mathcal{B}_1^+$, de cardinal au plus C, tel que $\mathcal{C}^\sharp$ contient un intervalle avec au moins L termes ; il est en outre clair que le plus petit de ses termes est inférieur à $CL = O(p^{3/4} \ln p)$. Il en résulte que $(\mathcal{B}_1^+)^\sharp$ contient un intervalle de longueur au moins $\sum_{b \in \mathcal{B}_1^+ \setminus \mathcal{C}} b$ et dont le plus petit élément est $O(p^{3/4} \ln p)$. Par la Relation 7, cet intervalle est de longueur supérieure à $p/2$. On considère alors l'ensemble $\mathcal{B}^+ = \bar{\mathcal{B}} \cap]0\,,\,p/2[$: l'ensemble $(\mathcal{B}^+)^\sharp$ contient un intervalle de longueur au moins $\sum_{b \in \mathcal{B}+ \setminus \mathcal{C}} b$; puisque cette longueur est au plus p, et que $\sum_{c \in \mathcal{C}} c = O(p^{3/4} \ln p)$, on a

$$\sum_{b \in \mathcal{B}^+} b \leq p + O(p^{3/4} \ln p). \tag{8}$$

Considérons maintenant $\mathcal{B}^- = \bar{\mathcal{B}} \cap]-p/2\,,\,0[$: aucun élément de $(\mathcal{B}^-)^\sharp$ ne peut être l'opposé d'un élément de $(\mathcal{B}^+)^\sharp$: cela implique que tous les éléments b^- de $\mathcal{B}^-$ vérifient $|b^-| = O(p^{3/4} \ln p)$, et qu'on a

$$\sum_{b \in \mathcal{B}^-} |b| = O(p^{3/4} \ln p). \tag{9}$$

Le Théorème 1 résulte de la construction des ensembles $(\mathcal{B}^+)$ et $(\mathcal{B}^-)$ et des Relations (8) et (9). □

4. Démonstration du Théorème 2

Cette partie suit de près l'argument de l'article [1] en le simplifiant en partie, et nous n'en indiquons les détails que pour cette partie. En revanche, nous profitons de cet article pour redonner l'énoncé du Lemme 1, pollué par une coquille, qui doit se lire ainsi :

Lemme 3. *Soit $k \geq 3$ un entier naturel. Tout entier de l'intervalle $[k+2, 4k^2-3k]$ peut être écrit comme somme d'éléments deux à deux distincts de l'intervalle $[k+2, 5k]$.*

Pour démontrer le Théorème 2 on commence par construire un ensemble auxiliaire d'entiers $\mathcal{E}$. On rappelle que l'on a $0 < c < \sqrt{2}$. On pose

$$\epsilon = \min\{1/10\,,\,(\sqrt{2}-c)/5\} \quad \text{et} \quad k = \lfloor \epsilon\sqrt{p} \rfloor$$

et on définit $\mathcal{E}$ comme l'ensemble des entiers de l'intervalle

$$[k+1\,,\ \lfloor(\sqrt{2}+\epsilon^2/2,2)\sqrt{p}+1\rfloor\,].$$

Quand p est suffisamment grand, on a

$$(\sqrt{2}+\epsilon^2/2,2)\sqrt{p} \le \lfloor(\sqrt{2}+\epsilon^2/2.2)\sqrt{p}+1\rfloor \le (\sqrt{2}+\epsilon^2/2,1)\sqrt{p},$$

d'où l'on déduit aisément, toujours pour p suffisamment grand

$$p+0,1k^2 \le \sum_{e\in\mathcal{E}} e \le p+k^2. \tag{10}$$

D'après le Lemme 3, on peut trouver un ensemble $\mathcal{C}$ d'entiers de l'intervalle $[k+2\,,\ 5k]$, deux à deux distincts, tel qu'en notant $\mathcal{D}=\mathcal{E}\backslash\mathcal{C}$ on ait

$$\sum_{d\in\mathcal{D}} d = p+k. \tag{11}$$

Puisque $\mathcal{D}$ contient les entiers de l'intervalle $[5k+1\,,\ \lfloor(\sqrt{2}+\epsilon^2/2,2)\sqrt{p}+1\rfloor\,]$ et donc ceux de l'intervalle $[5\epsilon\sqrt{p}+1\,,\ \sqrt{2}\sqrt{p}+3]$, le choix de ϵ assure que l'on a

$$\operatorname{card}\mathcal{D} > c\sqrt{p}. \tag{12}$$

Soit alors $\mathcal{B}$ l'ensemble des entiers de l'intervalle $[-\lfloor\sqrt{k}\rfloor\,,\ -1]$ et $\mathcal{F}=\mathcal{D}\cup\mathcal{B}$. On a $\mathcal{B}^*\subset[-k+1\,,\ -1]$, d'où $\mathcal{F}^*\subset[-k+1\,,\ p+k]$. Montrons que ni p ni 0 ne sont dans $\mathcal{F}^\sharp$. Soit $\mathcal{G}$ un sous-ensemble non vide de $\mathcal{F}$; s'il contient $\mathcal{D}$, on a $\sum_{g\in\mathcal{G}} g \ge p+1$; s'il ne contient pas tout $\mathcal{D}$ mais en contient un élément, on a $0<\sum_{g\in\mathcal{G}} g<p$; enfin, s'il ne contient aucun élément de $\mathcal{D}$, puisqu'il est non vide, on a $\sum_{g\in\mathcal{G}} g<0$. Cela implique que l'image canonique $\mathcal{A}$ de $\mathcal{F}$ dans $\mathbb{Z}/p\mathbb{Z}$ satisfait à la relation souhaitée $0\notin\mathcal{A}^\sharp$; en outre la relation (12) implique que $\operatorname{card}\mathcal{A}>c\sqrt{p}$; puisque k est de l'ordre de grandeur de $\sqrt{p}$, la relation (11) et la définition de $\mathcal{B}$ impliquent les inégalités de (2) pour $s=1$.

La validité des inégalités (2) pour $0<|s|<p/2$ se démontre comme dans [1] ; rappelons-en le principe. Tant que $|s|\le 0,35\sqrt{p}$, on a bien sûr $\sum_{x\in s\cdot\mathcal{D}}|x| = |s|\sum_{d\in\mathcal{D}} d$, mais l'ensemble d'entiers $s\cdot\mathcal{D}$ est dans $[0\,,\ p/2]$ ou $[-p/2\,,\ 0]$, d'où $\|sd/p\| = |s|\|d/p\|$, et la relation (11) implique la première partie de la relation (2) ; quant à la seconde inégalité, l'argument précédent la fournit si s est négatif ; si s est positif, on applique l'argument précédent à $\mathcal{B}$. Lorsque $0,35\sqrt{p}\le|s|<p/2$, le même argument qu'en [1] (étude directe lorsque s n'est pas trop grand et sinon, utilisation de sommes trigonométriques) implique la relation $\sum_{x\in s\cdot\mathcal{D}}|x|\ge 2$. Si s est négatif, l'argument précédent implique également la seconde inégalité de (2). Enfin, si s est positif, on applique la technique précédente à $s\cdot\mathcal{B}$ pour terminer la démonstration du Théorème 2. □

Bibliographie

[1] Deshouillers J-M., *A lower bound concerning subset sums which do not cover all the residues modulo p.* Hardy-Ramanujan J. **28** (2005), 30–34.

[2] Deshouillers J-M., Freiman G. A., *When subset-sums do not cover all the residues modulo p.* J. Number Theory **104** (2004), 255–262.

[3] Erdős P., Heilbronn H., *On the addition of the residue classes mod p.* Acta Arith. **IX** (1964), 149–159.

[4] Olson J. E., *An addition theorem modulo p.* J. Combin. Theory **5** (1968), 45–52.

[5] Ould Hamidoune Y., Zémor G., *On zero sum-free sets.* Acta Arith. **LXXVIII** (1996), 143–152.

Jean-Marc Deshouillers
Institut de Cognitique
Université Victor Segalen Bordeaux 2
33076 BORDEAUX Cedex (France)
et
A2X, UMR 5465
Université Bordeaux 1 et CNRS
33405 TALENCE Cedex (France)
E-mail: jean-marc.deshouillers@math.u-bordeaux1.fr