Estimation du nombre d'exceptions à ce qu'un ensemble de base privé d'un point reste un ensemble de base.

Bruno DESCHAMPS et Georges GREKOS

Université de Saint-Etienne

Abstract.— In this article, we show that if A denotes a basis set of order $h \geq 2$ and if A^* denotes the set of elements $a \in A$ such that $A - \{a\}$ remains a basis set, then $\sharp(A - A^*) \leq 5.7\sqrt{\frac{h}{\log h}}$. Moreover, thanks to an example, we show that this estimate in $O\left(\sqrt{\frac{h}{\log h}}\right)$ is best possible.

Résumé.— On montre dans cet article que si A désigne un ensemble de base d'ordre $h \geq 2$ et si A^* désigne l'ensemble des éléments $a \in A$ tels que $A - \{a\}$ reste un ensemble de base, alors $\sharp(A - A^*) \leq 5.7\sqrt{\frac{h}{\log h}}$. On montre de plus, grâce à un exemple, que cette estimation en $O\left(\sqrt{\frac{h}{\log h}}\right)$ est la meilleure possible.

1.— Introduction et résultats.

Si A désigne une partie de $\mathbb{N}$ et $h \geq 1$ un entier, on note hA l'ensemble $\{x_1 + \cdots + x_h \ / \ x_1, \cdots, x_h \in A\}$. Si A et B sont deux parties de $\mathbb{N}$, on note $A \sim B$, si la différence symétrique $A \Delta B$ est finie. On dit qu'une partie A de $\mathbb{N}$ est un *ensemble de base*, s'il existe $h \in \mathbb{N}^*$ tel que $hA \sim \mathbb{N}$. Le plus petit $h \in \mathbb{N}^*$ vérifiant $hA \sim \mathbb{N}$ est alors appelé *ordre* de A. Si A est un ensemble de base, on note A^* l'ensemble des éléments $a \in A$ tel que $A - \{a\}$ soit un ensemble de base.

Pour un ensemble A de base d'ordre h, l'étude de l'ordre de $A - \{a\}$ lorsque $a \in A^*$ a été entreprise dans une série de travaux, notamment [Nas] et [Gre1] où il est démontré que l'ordre de $A - \{a\}$ ne dépasse pas $\dfrac{h^2 + 3h}{2}$ et que pour tout h, il existe un ensemble de base A_h d'ordre h et un élément $a \in A_h^*$ tel que l'ordre de $A_h - \{a\}$ dépasse $\dfrac{h^2 - 3h}{3}$. L'étude de $A - A^*$ a été abordé dans [Gre2], où il est montré que pour un ensemble de base A d'ordre h, le cardinal de $A - A^*$ est majoré par $h - 1$. L'objet de cet article est de montrer le théorème suivant:

Théorème 1.— *Si A est un ensemble de base d'ordre $h \geq 2$, alors*

$$\sharp(A - A^*) \leq C\sqrt{\frac{h}{\log h}}, \ \textit{avec}\ C = \sqrt{4e^{2.0769} + e^{-1}} \simeq 5.6822$$

Le cardinal de $(A - A^*)$ est donc un $O\left(\sqrt{\frac{h}{\log h}}\right)$. Cette estimation est en fait la meilleure possible comme le montre le

Théorème 2.— *Il existe une constante $K > 0$ et une suite d'ensembles de base $(A_n)_n$ d'ordre $h_n \geq 2$ telle que:*

- $\lim_n h_n = +\infty$,
- $\sharp(A_n - A_n^*) \geq K\sqrt{\frac{h_n}{\log h_n}}$.

que nous montrons dans la dernière partie de cet article.

2.— Preuves des théorèmes.

2.1.— Preuve du théorème 1.

Si d désigne un entier non nul, on note ϕ_d la surjection canonique de $\mathbb{N}$ dans $\mathbb{Z}/d\mathbb{Z}$. Pour $n \in \mathbb{N}^*$, on note p_n le n-ième nombre premier. Dans ce qui suit, A désigne un ensemble de base d'ordre h.

Lemme 1.— *Soit $a \in A$. Les propositions suivantes sont équivalentes:*

i) $A - \{a\}$ est un ensemble de base,

ii) p.g.c.d.$\{b - b^{'} / \ b, b^{'} \in A - \{a\}\} = 1$.

Preuve: *non ii)* $\Rightarrow$ *non i)* Si $p.g.c.d.\{b - b^{'} / \ b, b^{'} \in A - \{a\}\} = d > 1$, alors $\phi_d(A - \{a\}) = \{\alpha\}$ et par suite, pour tout $h \in \mathbb{N}$, $\phi_d(h(A - \{a\})) = h\phi_d(A - \{a\}) = \{h\alpha\} \neq \mathbb{Z}/d\mathbb{Z}$, ce qui prouve que l'on n'a pas $h(A - \{a\}) \sim \mathbb{N}$.

ii) $\Rightarrow$ *i)* (Les idées essentielles de cette preuve viennent de l'article [EG] d'Erdös et Graham.)

Posons $A = \{a_0 < a_1 < \cdots\}$ et notons $A_1 = A - a$ (translaté de A par l'entier a). On a donc

$$A_1 = \{x - a / \ x \in A\}$$

L'ensemble A_1 est alors un sous-ensemble de $\mathbb{Z}$ qui contient 0. Comme $hA \sim \mathbb{N}$, on a $hA_1 \sim \mathbb{N}$ car $hA_1 = hA - ha$ (translaté de hA par l'entier ha). Posons $B = A - \{a\}$ et $B_1 = A_1 - \{0\}$. On a alors $B_1 = B - a$, il s'ensuit que B est un ensemble de base si et seulement si B_1 en est un. Nous allons montrer que B_1 est bien un ensemble de base.

Puisque B_1 est le translaté de B, on a

$$p.g.c.d.\{b - b^{'} / \ b, b^{'} \in B_1\} = p.g.c.d.\{b - b^{'} / \ b, b^{'} \in B\} = 1$$

Si l'on pose $B_1 = \{b_0 < b_1 < \cdots\}$, on remarque alors que

$$p.g.c.d.\{b - b^{'} / \ b, b^{'} \in B_1\} = p.g.c.d.\{b_{k+1} - b_k / \ k \in \mathbb{N}\}$$

Comme $p.g.c.d.\{b_{k+1} - b_k / \ k \in \mathbb{N}\} = 1$, il existe un entier $t \in \mathbb{N}$ tel que $p.g.c.d.\{b_{k+1} - b_k / \ k \leq t\} = 1$. En effet, la fonction

$$f(n) = p.g.c.d.\{b_{k+1} - b_k / \ k \leq n\}$$

est une suite d'entiers décroissante et de limite 1. Elle est donc stationnaire. Par application du théorème de Bézout, il existe des entiers $c_0, \cdots, c_t \in \mathbb{Z}$ tels que:

$$\sum_{k=0}^{t} c_k(b_{k+1} - b_k) = 1$$

Posons alors

$$\begin{aligned} p_k &= \begin{cases} b_{k+1} & si\ c_k \geq 0 \\ b_k & si\ c_k < 0 \end{cases} \\ q_k &= \begin{cases} b_k & si\ c_k \geq 0 \\ b_{k+1} & si\ c_k < 0 \end{cases} \end{aligned}$$

on a alors

$$\sum_{k=0}^{t} |c_k|(p_k - q_k) = 1$$

c'est-à-dire $\sum_{k=0}^{t} |c_k| p_k = 1 + \sum_{k=0}^{t} |c_k| q_k$. Prenons un élément $q \in B_1 \cap \mathbb{N}$ et posons

$$M = \sum_{k=0}^{t} q|c_k|p_k = q + \sum_{k=0}^{t} q|c_k|q_k$$

On a alors $M \in nB_1 \cap (n+1)B_1$ avec $n = q\sum_{k=0}^{t} |c_k|$. On en déduit donc que $2M \in 2nB_1 \cap (2n+1)B_1 \cap (2n+2)B_1$ et par récurrence que pour tout $w \in \mathbb{N}^*$,

$$wM \in \bigcap_{k=0}^{w} (wn + k)B_1$$

On prend $w = h - 1$, on a alors $wM \in \bigcap_{k=0}^{h-1}((h-1)n + k)B_1$. Pour tout $r = 1, \cdots, h$, on a $0 \leq h - r \leq h - 1$ et donc $(h-1)M \in [(h-1)n + (h-r)]B_1$. Ainsi,

$$(h-1)M + rB_1 \subset [(h-1)n + (h-r) + r]B_1 = [(h-1)n + h]B_1$$

et par suite

$$\bigcup_{r=1}^{h} [(h-1)M + rB_1] \subset [(h-1)n + h]B_1$$

Maintenant, $hA_1 \sim \mathbb{N}$ et puisque $0 \in A_1$, on a

$$hA_1 = \bigcup_{r=1}^{h} rB_1 \sim \mathbb{N}$$

Mais comme $rB_1 \sim (h-1)M + rB_1$, on en déduit que $\bigcup_{r=1}^{h}[(h-1)M + rB_1] \sim \mathbb{N}$ et par suite que B_1 est un ensemble de base d'ordre $\leq (h-1)n + h$.

Lemme 2.— *L'ensemble $A - A^*$ est fini.*

Preuve: Enumérons les éléments de A en une suite $(x_n)_n$ strictement croissante. Considérons la fonction $f : \mathbb{N} \longrightarrow \mathbb{N}$ définie par:

$$f(n) = p.g.c.d.\{x_i - x_j \ / \ i, j \leq n\}$$

La fonction f est décroissante et vérifie $\lim_n f(n) = 1$. Donc il existe $n_0 \in \mathbb{N}$ tel que $f(n_0) = 1$. Soit $A_1 = \{x_0, \cdots, x_{n_0}\}$. Il est clair que pour tout $a \in A - A_1$, $p.g.c.d.\{b - b^{'}; \ b, b^{'} \in A - \{a\}\} = 1$ (puisque $A_1 \subset A - \{a\}$). Donc d'après le lemme 1, $A - A^* \subset A_1$.

Notons alors $A - A^* = \{x_1, \cdots, x_s\}$ et pour tout $i = 1, \cdots, s$ posons

$$d_i = p.g.c.d.\{b - b^{'} / \ b, b^{'} \in A - \{x_i\}\}$$

Lemme 3.— *On a pour tout $i = 1, \cdots, s$, $2 \leq d_i \leq h$.*

Preuve: Le fait que $d_i \geq 2$ provient directement du lemme 1. Puisque $d_i = p.g.c.d.\{b - b^{'} / \ b, b^{'} \in A - \{x_i\}\}$, on en déduit que $\phi_{d_i}(A - \{x_i\})$ n'a qu'un seul élément. Soit a_i un représentant dans $\mathbb{N}$ de cet élément. On a $\phi_{d_i}(a_i) \neq \phi_{d_i}(x_i)$ car sinon $\phi_{d_i}(A)$ ne contient qu'un seul élément et par suite A n'est plus de base. Il est clair que $\phi_{d_i}(hA) = h\phi_{d_i}(A)$ et par suite, comme h est l'ordre de A, on a

$$h\phi_{d_i}(A) = \mathbb{Z}/d_i\mathbb{Z}$$

Posons $\omega_1 = \phi_{d_i}(a_i)$ et $\omega_2 = \phi_{d_i}(x_i)$. On a:

$$h\phi_{d_i}(A) = \{i\omega_1 + j\omega_2 / \ i + j = h\} = \mathbb{Z}/d_i\mathbb{Z}$$

Cet ensemble a $h + 1$ éléments (non nécessairement distincts), on en déduit donc que $d_i \leq h + 1$. Si $d_i = h + 1$, alors quel que soit $k = 1, \cdots, h$, on a $k\omega_1 + (h - k)\omega_2 \neq h\omega_2$. Prenons un entier n assez grand tel que $n \in hA$ et $n \equiv hx_i(d_i)$, alors il existe un entier $k \leq h$ tel que $n = kx_i + \alpha_{k+1} + \cdots + \alpha_h$ avec $\alpha_{k+1}, \cdots, \alpha_h \in A - \{x_i\}$. On a alors $\phi_{d_i}(n) = h\omega_2 = (h - k)\omega_1 + k\omega_2$ ce qui n'est possible que si $k = h$. En prenant $n > hx_i$, on obtient alors une absurdité. Ainsi, $d_i \leq h$.

Lemme 4.— *Pour tout i et tout j distincts, on a $p.g.c.d.(d_i, d_j) = 1$.*

Preuve: Soit $i \neq j$ et $d > 1$ un diviseur commun de d_i et d_j. D'après le lemme 1, on a $\sharp\phi_{d_i}(A - \{x_i\}) = 1$ et $\sharp\phi_{d_j}(A - \{x_j\}) = 1$. On a, puisque $d|d_i$ et $d|d_j$, $\sharp\phi_d(A - \{x_i\}) = 1$ et $\sharp\phi_d(A - \{x_j\}) = 1$. Comme A est infini, on en déduit que $\phi_d(A - \{x_i\}) = \phi_d(A - \{x_j\})$ et par suite $\sharp\phi_d(A) = 1$, ce qui est en contradiction avec le fait que A est un ensemble de base.

Lemme 5.— *Pour tout entier $n \geq 2$, on a $n! \geq n^n e^{-n}$.*

Preuve: Pour $n = 2$, on a bien $\dfrac{2!}{2^2 e^{-2}} \geq 1$. Posons pour tout $n \geq 2$,

$$u_n = \log\left(\frac{n!}{n^n e^{-n}}\right)$$

On veut montrer que $u_n \geq 0$. C'est vrai pour $n = 2$. Calculons $u_{n+1} - u_n$:

$$\begin{array}{rcl} u_{n+1} - u_n & = & \log(n+1) + 1 + n\log(n) - (n+1)\log(n+1) \\ & = & 1 - n\log(1 + 1/n) \end{array}$$

Par ailleurs, on a toujours $\log(1+x) \leq x$ pour $x \geq 0$, donc $1 - n\log(1+1/n) \geq 0$. La suite $(u_n)_n$ est donc croissante, ce qui prouve le lemme.

Lemme 6.— *Soient n et k deux entiers de $\mathbb{N}^*$. Le nombre $A_n(k)$ de n-uplets $(\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n$ tels que $\sum_{i=1}^{n} \alpha_i = k$ vaut*

$$A_n(k) = C_{k+n-1}^{k} = \frac{(k+1)(k+2)\cdots(k+n-1)}{(n-1)!}$$

Preuve: On a $A_1(k) = 1$, $A_2(k) = k+1$. Supposons qu'au rang $n \geq 2$, on ait $A_n(k) = C_{k+n-1}^{k}$. Alors, au rang $n+1$:

$$A_{n+1}(k) = \sum_{i=0}^{k} A_n(i) = C_{n-1}^{0} + C_{n}^{1} + C_{n+1}^{2} + \cdots + C_{k+n-1}^{k} = C_{k+n}^{k}$$

Lemme 7.— *Pour tout $n \geq 2$, on a:*

$$p_1 \cdots p_n \geq n^n \left(\log^n n\right) \alpha^{-n}$$

avec $\alpha = e^{1.0769}$.

Preuve: Voir [Rob].

Lemme 8.— *On a $s^2 \log s \leq 2e\alpha h$.*

Preuve: D'après le lemme 1, on $\sharp\phi_{d_i}(A - \{x_1, \cdots, x_s\}) = 1$ pour tout $i = 1, \cdots, s$. Le lemme 4 affirme que les d_i sont premiers deux à deux, donc par le théorème des restes chinois, on en déduit que $\sharp\phi_q(A - \{x_1, \cdots, x_s\}) = 1$ pour $q = d_1 \cdots d_s$. Soit $\lambda = \phi_q(A - \{x_1, \cdots, x_s\})$, $\lambda_1 = \phi_q(x_1), \cdots, \lambda_s = \phi_q(x_s)$. Comme $hA \sim \mathbb{N}$, on en déduit que

$$\mathbb{Z}/q\mathbb{Z} = \left\{\alpha_0\lambda + \alpha_1\lambda_1 + \cdots + \alpha_s\lambda_s / \ (\alpha_0, \cdots, \alpha_s) \in \mathbb{N}^{s+1},\ \sum_{k=0}^{s} \alpha_k = h\right\}$$

Ce dernier ensemble compte au plus $C_{h+s}^{h} = \dfrac{(h+1)\cdots(h+s)}{s!}$ éléments (lemme 6). On en déduit donc que:

$$d_1 \cdots d_s \leq \frac{(h+1)\cdots(h+s)}{s!}$$

Par ailleurs, le lemme 4 permet d'affirmer que $p_1 \cdots p_s \leq d_1 \cdots d_s$ et comme $s \leq h$ (lemme 3 et 4), on en déduit que:

$$s! s^s (\log^s s) \alpha^{-s} \leq (2h)^s$$

Par le lemme 5, on a $s! \geq s^s e^{-s}$ et par suite:

$$s^2 \log s \leq 2e\alpha h$$

Preuve du théorème 1: Supposons que $s > C\sqrt{\frac{h}{\log h}}$, on a alors:

$$\begin{cases} s^2 & > \quad C^2 \frac{h}{\log h} \\ \log s & > \quad \log C + \frac{1}{2}\log h - \frac{1}{2}\log\log h \end{cases}$$

et par suite

$$s^2 \log s > \frac{C^2}{2} h - \frac{C^2}{2} h \frac{\log\log h}{\log h} + C^2 \log C \frac{h}{\log h}$$

On en déduit, par le lemme 8, que:

$$2e\alpha h > \frac{C^2}{2} h - \frac{C^2}{2} h \frac{\log\log h}{\log h} + C^2 \log C \frac{h}{\log h}$$

c'est-à-dire, après simplification, que:

$$\left(\frac{4e\alpha}{C^2} - 1\right)\log h + \log\log h - 2\log C > 0$$

Considérons la fonction $f :]1, +\infty[\to \mathbb{R}$ définie par:

$$f(x) = \left(\frac{4e\alpha}{C^2} - 1\right)\log x + \log\log x - 2\log C$$

On a

$$f^{'}(x) = \left(\frac{4e\alpha - C^2}{C^2}\right)\frac{1}{x} + \frac{1}{x\log x}$$

La fonction $f^{'}$ s'annule en $x_0 = exp\left(\frac{C^2}{C^2 - 4e\alpha}\right)$. La fonction f est croissante sur $]1, x_0]$ et décroissante sur $[x_0, +\infty[$, elle présente donc un maximum absolu en x_0, mais comme $f\left(exp\left(\frac{C^2}{C^2-4e\alpha}\right)\right) = 0$, on obtient alors une absurdité.

2.2.— Preuve du théorème 2.

Soit $n \geq 2$ un entier. On considère l'ensemble

$$A_n = p_1 \cdots p_n \mathbb{N} \cup \{q_i = \prod_{j \neq i} p_j / i = 1, \cdots, n\}$$

($A_2 = 6\mathbb{N} \cup \{2,3\}$, $A_3 = 30\mathbb{N} \cup \{6,10,15\}$, $A_4 = 210\mathbb{N} \cup \{30,42,70,105\}$, etc.)

Proposition 1.— *L'ensemble A_n est de base d'ordre $1 - n + \sum_{k=1}^{n} p_k$ et*

$$A_n - A_n^* = \{q_1, \cdots, q_n\}$$

Preuve: Soit $q = q_1 + \cdots + q_n$. L'entier q est premier avec $p_1 \cdots p_n$, sinon il existerait un indice i tel que p_i divise q. Comme p_i divise q_j pour tout $j \neq i$, p_i diviserait q_i ce qui est absurde. L'entier q engendre donc $\mathbb{Z}/p_1 \cdots p_n\mathbb{Z}$ ce qui justifie que A_n est de base et que son ordre est $\leq n.p_1 \cdots p_n + 1$.
Soit maintenant un indice $i_0 \in \{1, \cdots, n\}$. Pour tout $i \neq i_0$, q_i est divisible par p_{i_0} donc pour tout h, les éléments de $h(A_n - \{q_{i_0}\})$ sont divisibles par p_{i_0} ce qui prouve que $A_n - \{q_{i_0}\}$ n'est pas un ensemble de base. Reste maintenant à calculer l'ordre de A_n.
Pour tout entier h, posons

$$\Omega_h = \phi_{p_1 \cdots p_n} \left\{ \sum_{k=1}^{n} \alpha_k q_k / \ (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n \ et \ \sum_{k=1}^{n} \alpha_k \leq h \right\}$$

Si h_n désigne l'ordre de A_n, il est alors clair que $h_n = h + 1$ avec h le plus petit entier tel que $\Omega_h = \mathbb{Z}/p_1 \cdots p_n\mathbb{Z}$, c'est-à-dire tel que $\sharp\Omega_h = p_1 \cdots p_n$. Considérons alors l'ensemble

$$E = \left\{ (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n \ / \sum_{k=1}^{n} \alpha_k \leq h \right\}$$

et sur E définissons la relation d'équivalence $\sim$ suivante:

$$(\alpha_1, \cdots, \alpha_n) \sim (\beta_1, \cdots, \beta_n) \Longleftrightarrow \sum_{k=1}^{n} \alpha_k q_k \equiv \sum_{k=1}^{n} \beta_k q_k \ mod(p_1 \cdots p_n)$$

Il est alors clair que $\sharp\Omega_h = \sharp E/\sim$.

Lemme.— *Soient $(\alpha_1, \cdots, \alpha_n)$ et $(\beta_1, \cdots, \beta_n)$ deux éléments de E. Les propositions suivantes sont équivalentes:*

i) $(\alpha_1, \cdots, \alpha_n) \sim (\beta_1, \cdots, \beta_n)$,

ii) $\forall i = 1, \cdots, n$, $\alpha_i \equiv \beta_i \ mod(p_i)$.

Preuve du lemme: *ii)* $\Rightarrow$ *i)*: si $\alpha_i - \beta_i$ est divisible par p_i, alors $(\alpha_i - \beta_i)q_i$ est divisible par $p_1 \cdots p_n$ et par suite $\sum_{k=1}^{n} (\alpha_k - \beta_k)q_k \equiv 0 \ mod(p_1 \cdots p_n)$.
i) $\Rightarrow$ *ii)*: Supposons que $\sum_{k=1}^{n} (\alpha_k - \beta_k)q_k \equiv 0 \ mod(p_1 \cdots p_n)$, on a donc

$\sum_{k=1}^{n}(\alpha_k - \beta_k)q_k \equiv 0 \; mod(p_i)$ pour tout $i = 1, \cdots, n$. Mais comme q_k est divisible par p_i pour tout $k \neq i$, on en déduit que $(\alpha_i - \beta_i)q_i \equiv 0 \; mod(p_i)$. Maintenant q_i est premier avec p_i donc $(\alpha_i - \beta_i) \equiv 0 \; mod(p_i)$.

Par conséquent une classe de représentants de $E/\sim$ est donnée par les n-uplets $(\alpha_1, \cdots, \alpha_n)$ vérifiants

$$0 \leq \alpha_i \leq p_i - 1 \; \forall i = 1, \cdots, n; \; \sum_{k=1}^{n} \alpha_k \leq h$$

On en déduit donc que si

$$\mathcal{E}_h = \left\{ (\alpha_1, \cdots, \alpha_n) / \; \sum_{k=1}^{n} \alpha_k \leq h \; et \; 0 \leq \alpha_i \leq p_i - 1 \; \forall i = 1, \cdots, n \right\}$$

alors $\sharp\Omega_h = \sharp\mathcal{E}_h$. Notons $N_n(h)$ le cardinal de $\mathcal{E}_h$. Si $h \geq \sum_{k=1}^{n} p_k - n$ alors

$$N_n(h) = \sharp \left\{ (\alpha_1, \cdots, \alpha_n) / \; 0 \leq \alpha_i \leq p_i - 1 \forall i = 1, \cdots, n \right\} = p_1 \cdots p_n$$

Maintenant si $h < \sum_{k=1}^{n} p_k - n$, au moins un des n-uplets $(\alpha_1, \cdots, \alpha_n)$ assujetis aux conditions $0 \leq \alpha_i \leq p_i - 1 \; \forall i = 1, \cdots, n$ ne figure pas dans $\mathcal{E}_h$, c'est-à-dire que $N_n(h) < p_1 \cdots p_n$. On en déduit donc que le plus petit entier h tel que $\sharp\Omega_h = p_1 \cdots p_n$ vaut $\sum_{k=1}^{n} p_k - n$ et ainsi $h_n = \sum_{k=1}^{n} p_k - n + 1$.

Le théorème des nombres premiers a comme conséquence l'équivalence suivante:

$$p_n \simeq_n n \log n$$

Il existe donc une constante $\omega > 1$ telle que:

$$\forall n \geq 2, \; p_n \leq \omega n \log n$$

et par suite on a la majoration

$$h_n \leq \sum_{k=1}^{n} p_k \leq \omega n^2 \log n$$

Si l'on note $s_n = \sharp(A_n - A_n^*)$ on a alors $s_n = n$ et ce qui précède assure alors que

$$h_n \leq \omega s_n^2 \log s_n$$

On choisit la constante ω telle que $\omega > \frac{2}{\log 2}$ et on pose $K = \sqrt{\frac{2}{\omega}}$. Supposons qu'il existe un $n \geq 1$ tel que $s_n < K\sqrt{\frac{h_n}{\log h_n}}$, alors on a

$$s_n^2 \log s_n < \frac{K^2}{2} h_n - \frac{K^2}{2} h_n \frac{\log \log h_n}{\log h_n} + K^2 \log K \frac{h_n}{\log h_n}$$

Compte tenu du fait que $\frac{1}{\omega}h_n \leq s_n^2 \log s_n$, on en déduit que

$$-\log\log h_n + \log K^2 > 0$$

ce qui implique que $h_n < e^{K^2} \leq 2$, ce qui, étant absurde, montre le théorème 2.

Références

[EG] P. Erdös and R.L. Graham, *On bases with an exact order*, Acta Arithmetica XXXVII, p. 201-207 (1980).

[Gre1] G. Grekos, *Sur l'ordre d'une base additive*, Séminaire de théorie des nombres de Bordeaux 1987-1988, exp. 31.

[Gre2] G. Grekos, *Quelques aspects de la théorie additive des nombres*, Thèse de doctorat, Université de Bordeaux I (1982).

[Nas] J.C.M. Nash, *Some applications of a theorem of M. Kneser*, Journal of Number Theory, Vol. 44, p. 1-8 (1993).

[Rob] G. Robin, *Estimation de la fonction de Tchebychev*, Acta Arithmetica XLII, p. 367-389 (1983).

Bruno Deschamps, Georges Grekos, Equipe de théorie des nombres, Faculté des sciences et techniques, Université Jean Monnet, 23 rue du docteur Paul Michelon, 42023 Saint-Etienne, Cedex 2, France.
E-mail: Bruno.Deschamps@univ-st-etienne.fr, grekos@univ-st-etienne.fr