ANNALES

DE

L'INSTITUT FOURIER

Alain PLAGNE

A propos de la fonction X d'Erdös et Graham

Tome 54, n° 6 (2004), p. 1717-1767.

<http://aif.cedram.org/item?id=AIF_2004__54_6_1717_0>

Ann. Inst. Fourier, Grenoble
54, 6 (2004), 1717–1767

À PROPOS DE LA FONCTION X D'ERDŐS ET GRAHAM

par Alain PLAGNE

1. Introduction.

1.1. Le contexte.

D'un ensemble $\mathcal{A}$ d'entiers bornés inférieurement (on admet donc un nombre *fini* d'entiers négatifs), on dira qu'il est une *base* (sous-entendu *additive, exacte et asymptotique*) s'il existe un entier $h \geqslant 1$ tel que tout entier assez grand s'écrive comme somme d'exactement h éléments de $\mathcal{A}$, ce que l'on notera

$$h\mathcal{A} \sim \mathbb{N}.$$

L'*ordre* de la base $\mathcal{A}$ est le plus petit entier h que l'on puisse prendre dans cette définition. On le notera $\mathrm{ord}^*\mathcal{A}$.

Étant donnée une base $\mathcal{A}$, on définit $\mathcal{A}^*$ comme le sous-ensemble de $\mathcal{A}$ composé des éléments $a \in \mathcal{A}$ tels que $\mathcal{A} \setminus \{a\}$ soit encore une base (d'ordre éventuellement supérieur à h). L'ensemble $\mathcal{A}^*$ défini ci-dessus a donné lieu à plusieurs travaux plus ou moins récents (*cf.* [5, 7, 4]) montrant, au final,

Mots-clés : Base additive – Base asymptotique – Base exacte – Ordre – Méthode isopérimétrique – Théorème des trois distances.
Classification math. : 11B13.

que

$$\max_{h\mathcal{A}\sim\mathbb{N}} |\mathcal{A}\setminus\mathcal{A}^*| \asymp \sqrt{\frac{h}{\log h}},$$

et en particulier que l'ensemble $\mathcal{A}\setminus\mathcal{A}^*$ est fini.

Dans cet article, on s'intéresse à l'augmentation de l'ordre d'une base lorsqu'on la prive d'un élément ne lui ôtant pas sa qualité de base. Cette problématique a été initiée par Erdős et Graham [5] qui ont ainsi défini la quantité

$$X(h) = \max_{h\mathcal{A}\sim\mathbb{N}} \max_{a\in\mathcal{A}^*} \operatorname{ord}^*(\mathcal{A}\setminus\{a\})$$

dont ils ont pu prouver que la croissance était quadratique en h et plus précisément que l'on avait

$$\frac{h^2}{4} \lesssim X(h) \lesssim \frac{5h^2}{4}. \tag{1.1}$$

Ils calculaient également $X(2)=4$ et précisaient dans [6, Chapitre 5] qu'ils n'avaient aucune idée de quel pouvait être le bon coefficient de h^2 dans ces bornes, sous-entendant qu'une formule du type $X(h)\sim\alpha h^2$ était probable. Notons que la minoration

$$\left[\frac{h^2+6h+1}{4}\right] \leqslant X(h) \tag{1.2}$$

résultait en fait de travaux antérieurs de Stöhr [24, 25]. Grekos [7] s'est ensuite attaqué au problème et il a pu prouver que la formule (1.1) pouvait être améliorée en

$$\frac{h^2-3h}{3} \leqslant X(h) \lesssim h^2.$$

La borne inférieure provient d'une construction à base d'intervalles modulaires tandis que la borne supérieure utilise le théorème de Kneser pour les suites entières. Plus tard, Nash [20] a démontré, d'une part, que $X(3)=7$ et, d'autre part, que

$$X(h) \leqslant \frac{h^2+3h}{2}.$$

En résumé et au meilleur de nos connaissances, on sait aujourd'hui que $X(1)=1$, $X(2)=4$, $X(3)=7$ et que, si h vaut au moins 4, on a

$$\max\left(\frac{h^2-3h}{3}, \left[\frac{h^2+6h+1}{4}\right]\right) \leqslant X(h) \leqslant \frac{h^2+3h}{2}. \tag{1.3}$$

Remarquons que la minoration due à Stöhr reste intéressante pour les petites valeurs de h. En particulier, on a d'après (1.3)

$$(1.4) \qquad 10 \leqslant X(4) \leqslant 14, \qquad 14 \leqslant X(5) \leqslant 20, \qquad 18 \leqslant X(6) \leqslant 27.$$

Notre connaissance de la fonction X reste donc encore grossière puisque même son asymptotique n'est pas connue. Un premier pas vers la compréhension de cette asymptotique consistera probablement en le calcul de nouvelles valeurs de la fonction X : que valent, par exemple, $X(4)$, $X(5)$ ou $X(6)$? Certains spécialistes conjecturent que le bon ordre de grandeur dans la formule (1.3) se trouverait du côté de la minoration. En particulier, une preuve de $X(4) = 10$ aurait été annoncée par Li il y a une quinzaine d'années (voir [7]), mais elle n'a jamais été publiée. En fait, seule la minoration de $X(4)$ par cette quantité est connue (*cf.* la formule (1.2)). Elle résulte tout simplement de l'exemple suivant

$$(1.5) \qquad \mathcal{B} = \{0\} \cup (\{2, 5\} + \{11n, \text{ où } n \in \mathbb{N}\}).$$

Notons que $\mathcal{B}$ est la réunion de deux progressions arithmétiques de même raison et de zéro, qui sera l'élément à enlever pour atteindre l'ordre 10. On croisera ce type de constructions de façon essentielle tout au long de cet article. Ajoutons que la forme de l'exemple (1.5) a poussé Grekos à conjecturer que, quelle que soit la base $\mathcal{A}$ d'ordre au plus h considérée, seul un nombre *fini* d'éléments a de $\mathcal{A}^*$ vérifiaient $\operatorname{ord}^*(\mathcal{A} \setminus \{a\}) = X(h)$. C'est l'origine de l'introduction de la fonction S définie par la formule

$$S(h) = \max_{h\mathcal{A} \sim \mathbb{N}} \limsup_{a \in \mathcal{A}^*} \operatorname{ord}^*(\mathcal{A} \setminus \{a\}).$$

On sait désormais [1, 21] que l'on a en effet $S(2) = 3$ et, pour $h \geqslant 3$,

$$h + 1 \leqslant S(h) \leqslant 2h,$$

ce qui implique en particulier la conjecture de Grekos ($S(h) < X(h)$ pour $h \geqslant 2$).

1.2. Nouveaux résultats et organisation de l'article.

Le principal objectif de cet article est l'amélioration des bornes sur $X(h)$ fournies par (1.3). Dans la partie 5, nous démontrerons le résultat suivant.

THÉORÈME 1. — *Pour tout entier $h \geqslant 1$, on dispose des inégalités*

$$\left[\frac{h(h+4)}{3}\right] \leqslant X(h) \leqslant \frac{h(h+1)}{2} + \left[\frac{h-1}{3}\right].$$

Ce résultat est plus précis, et dans tous les cas, que tous les résultats précédemment cités sur $X(h)$. Notons que ces bornes sont définitives pour $h \leqslant 3$ puisque, dans ces cas, bornes inférieure et supérieure coïncident pour fournir $X(1) = 1$, $X(2) = 4$, $X(3) = 7$ (mais ces résultats étaient déjà connus). Pour des valeurs de $h \geqslant 4$, nos bornes permettent d'obtenir une réponse partielle à la question des valeurs que prend la fonction X lorsque l'entier h est petit. On améliore par exemple (1.4) en

$$(1.6) \qquad 10 \leqslant X(4) \leqslant 11, \qquad 15 \leqslant X(5) \leqslant 17, \qquad 20 \leqslant X(6) \leqslant 23.$$

Dans le chapitre 5.3, on verra qu'au prix de calculs fastidieux, la méthode est encore susceptible d'amélioration dans certains cas. Par exemple, et pour illustrer cette possibilité, on améliorera deux des encadrements de (1.6) en

$$(1.7) \qquad 15 \leqslant X(5) \leqslant 16, \qquad 20 \leqslant X(6) \leqslant 22.$$

On peut ainsi observer que, pour $2 \leqslant h \leqslant 6$, la meilleure borne supérieure connue (et pour $h = 2$ et 3, la valeur) de $X(h)$ coïncide avec $h(h+1)/2 + 1$. Cette quantité apparaît d'ailleurs comme limite de la méthode à plusieurs endroits dans notre démonstration. Cela conduit naturellement à la conjecture suivante.

CONJECTURE 2. — *Pour tout entier $h \geqslant 2$, on a*

$$X(h) \leqslant \frac{h(h+1)}{2} + 1.$$

Cela nous renforce aussi dans l'idée que le calcul de X pour les petites valeurs de h pourrait déjà contenir toute la difficulté du problème : si $X(4)$ vaut effectivement 10, il est bien possible que la preuve de ce résultat (qui devrait «casser» la borne $h(h+1)/2+1$ pour $h = 4$) puisse servir à améliorer notre borne supérieure pour toute valeur de h.

La preuve du théorème 1 sera exposée à la fin de cet article. Au préalable, dans la partie 2, nous aurons présenté les résultats additifs nécessaires à notre étude puis développé un nouveau résultat additif général (théorème 12) qui pourrait se révéler utile dans d'autres contextes. Dans la partie 3, on évoquera tout d'abord le théorème des trois distances, puis on présentera trois problèmes combinatoires (dans les groupes cycliques) liés à notre étude : pour le premier problème (recouvrement intervallaire), nous évoquerons un article de Deléglise [3] dont nous reprendrons la méthode générale pour l'adapter à notre propos ; tandis que nous devrons effectuer une étude originale pour les second (foncière génération maximale) et troisième (recouvrement économique). La partie 4 est le cœur de cet article. Elle contient un lemme (lemme 25) qui est la pierre angulaire de la majoration dans le théorème 1. Ce résultat nécessitera l'utilisation récursive de la méthode isopérimétrique d'ould Hamidoune sous la forme du théorème 12 prouvé précédemment et le résultat du chapitre 3.2 sur le recouvrement intervallaire. Au passage, nous déduirons du lemme 25 le théorème 3 ci-dessous. Ce résultat n'est pas nécessaire à notre étude mais sa portée plus générale en fait un outil potentiel dans d'autres situations.

THÉORÈME 3. — *Soient h et n deux entiers strictement positifs. Soit $\mathcal{E}$ un sous-ensemble de $\mathbb{Z}/n\mathbb{Z}$ possédant au moins deux éléments et tel que*

$$\mathcal{E} \cup 2\mathcal{E} \cup \ldots \cup h\mathcal{E} = \mathbb{Z}/n\mathbb{Z}.$$

Dans ces conditions, $\left(\frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil\right)\mathcal{E}$ est dégénéré *: cet ensemble peut s'écrire comme une réunion de classes modulo un certain sous-groupe non nul de G.*

Enfin, la partie 5 fera la synthèse de ce qui précède : la preuve de la borne inférieure du théorème 1 (présentée en 5.1) découlera de nos résultats sur la foncière génération maximale (chapitre 3.3), tandis que la preuve de la borne supérieure (présentée en 5.2), qui se fondera sur les acquis – développés sous la forme du lemme 27 – de celles de Grekos et Nash, fera appel de façon cruciale au lemme isopérimétrique (lemme 25) démontré dans la partie 4 ; enfin, la preuve des inégalités (1.7) sera exposée dans le chapitre 5.3 ; elle reposera sur l'étude du problème du recouvrement économique (chapitre 3.4).

1.3. Notations et définitions.

Dans tout cet article, nous utiliserons les notations additives usuelles (voir par exemple [18, 19]) que nous rappelons ici. Soient h un entier positif et $\mathcal{A}_1, \ldots, \mathcal{A}_h$ des sous-ensembles d'un certain groupe dont l'opération sera notée additivement. On notera

$$\mathcal{A}_1 + \cdots + \mathcal{A}_h = \{a_1 + \cdots + a_h, \text{ où } a_1 \in \mathcal{A}_1, \ldots, a_h \in \mathcal{A}_h\}.$$

Dans le cas où l'on additionne un ensemble $\mathcal{A}$ avec un ensemble à un élément a (cela correspond à une translation de $\mathcal{A}$), on s'autorisera l'écriture $\mathcal{A}+a$ au lieu de $\mathcal{A}+\{a\}$. Si $x \in \mathcal{A}_1 + \cdots + \mathcal{A}_h$, le *nombre de représentations* de x (sous-entendu comme élément de $\mathcal{A}_1 + \cdots + \mathcal{A}_h$) est le nombre de h-uplets $(a_1, \ldots, a_h)$ avec $a_1 \in \mathcal{A}_1, \ldots, a_h \in \mathcal{A}_h$ tels que $x = a_1 + \cdots + a_h$. Si $\mathcal{A}_1 = \cdots = \mathcal{A}_h$, on notera $h\mathcal{A}$ la somme $\mathcal{A}_1 + \cdots + \mathcal{A}_h$ qu'on ne confondra pas avec l'ensemble des h-multiples de $\mathcal{A}$,

$$h.\mathcal{A} = \{ha, \text{ où } a \in \mathcal{A}\}.$$

Par convention $0\mathcal{A} = \{0\}$. Soulignons qu'on notera cependant comme à l'accoutumée le groupe quotient $\mathbb{Z}/n\mathbb{Z}$ (alors qu'on devrait le noter, pour être cohérent, $\mathbb{Z}/n.\mathbb{Z}$).

On appelle *densité inférieure* d'un certain ensemble d'entiers $\mathcal{A}$, et l'on note $\underline{d}\mathcal{A}$, la quantité

$$\underline{d}\mathcal{A} = \liminf_{m \to +\infty} \frac{|\mathcal{A} \cap \{0, 1, \ldots, m\}|}{m}.$$

La fonction apparaissant au numérateur de cette expression, qui associe à l'entier m, le cardinal de l'ensemble $\mathcal{A} \cap \{0, 1, \ldots, m\}$ sera couramment appelée *fonction de comptage* de l'ensemble $\mathcal{A}$ (et souvent notée A).

Si $\mathcal{B}$ et $\mathcal{C}$ sont deux ensembles d'entiers, l'expression $\mathcal{B} \sim \mathcal{C}$ signifie que la différence symétrique des ensembles $\mathcal{B}$ et $\mathcal{C}$ est finie.

Classiquement, les notations $[x]$ et $\lceil x \rceil$ désigneront les parties entières par défaut et par excès d'un réel x tandis que la notation $\{x\}$ désignera sa partie fractionnaire. Enfin, étant données deux fonctions f et g, la notation $f \lesssim g$ est équivalente à $f \leqslant (1 + o(1))g$.

Soit maintenant G un groupe fini (abélien pour simplifier) quelconque. Nous dirons qu'un sous-ensemble de G est *dégénéré* (ou *périodique*) s'il peut

être écrit comme une réunion de classes modulo un certain sous-groupe non nul de G (en particulier, G tout entier *est* dégénéré car il est la réunion d'une classe modulo G).

Nous dirons qu'un sous ensemble $\mathcal{A}$ de G est *foncièrement générateur* s'il existe un entier i tel que $i\mathcal{A}$ soit égal à G tout entier. Dans le vocabulaire de la théorie additive, cette notion coïncide avec celle de *base exacte de* $\mathbb{Z}/n\mathbb{Z}$. Toutefois, afin d'éviter les confusions, nous réserverons ici la notion de base aux ensembles d'entiers relatifs. Notons qu'un ensemble foncièrement générateur d'un groupe non réduit à un élément, possède au minimum deux éléments. Remarquons aussi qu'un ensemble foncièrement générateur est générateur.

Si H et $\mathcal{A}$ sont respectivement un sous-groupe et un sous-ensemble de G, la notation $\mathcal{A}/H$ désignera la projection canonique de $\mathcal{A}$ dans G/H.

Introduisons maintenant le vocabulaire de la méthode isopérimétrique nécessaire à cet article. On suppose que $\mathcal{A}$ est un sous-ensemble de G de cardinal au moins égal à 2 et contenant 0. Si k est un entier positif, nous dirons que $\mathcal{A}$ est *k-séparable* s'il existe un sous-ensemble $\mathcal{X}_0$ de G tel que $|\mathcal{X}_0| \geqslant k$ et $|\mathcal{X}_0 + \mathcal{A}| \leqslant |G| - k$. Si $\mathcal{A}$ est k-séparable, on définit le *k-ième nombre isopérimétrique* par la formule

$$\kappa_k(G,\mathcal{A}) = \min\{|\mathcal{X}+\mathcal{A}| - |\mathcal{X}| \text{ où } \mathcal{X} \subset G \text{ est tel que } |\mathcal{X}| \geqslant k \text{ et } |\mathcal{X}+\mathcal{A}| \leqslant |G| - k\}.$$

Un ensemble $\mathcal{X}$ en lequel ce minimum est atteint sera appelé dans la suite un ensemble *k-critique*.

En référence au célèbre théorème de Vosper [28, 29] (régissant les paires critiques dans le cas des groupes cycliques d'ordre premier), nous dirons qu'un ensemble $\mathcal{A}$ est *vospérien* si, pour tout ensemble $\mathcal{X} \subset G$ de cardinal $|\mathcal{X}| \geqslant 2$, on a

$$|\mathcal{A} + \mathcal{X}| \geqslant \min(|G| - 1, |\mathcal{A}| + |\mathcal{X}|).$$

On constate qu'un ensemble $\mathcal{A}$ n'est pas vospérien si et seulement si il est 2-séparable et $\kappa_2(G,\mathcal{A}) \leqslant |\mathcal{A}| - 1$.

Un mot, maintenant, sur la notion centrale dans cet article de *progression arithmétique*. Dans tout ce qui suit, les progressions arithmétiques dans $\mathbb{N}$ seront obligatoirement *infinies*, donc du type $\{a+bk,\ \text{où } k \in \mathbb{N}\}$. À l'inverse, dans un groupe fini, nous ne demanderons évidemment pas aux

progressions arithmétiques d'être infinies; qui plus est, nous n'exigerons même pas des progressions arithmétiques qu'elles soient égales à une classe modulo un sous-groupe. Ainsi, par exemple, deux éléments quelconques d'un groupe fini quelconque formeront toujours une progression arithmétique.

On notera que le cardinal des multiples d'une progression arithmétique dans un groupe cyclique est aisé à calculer : ainsi si I est une progression arithmétique dans $\mathbb{Z}/n\mathbb{Z}$ et si j un entier positif ou nul quelconque, on a

$$|jI| = \min\big(j(|I|-1)+1, d\big),$$

où d est l'ordre du groupe engendré par une raison de I. En particulier, on a toujours

$$|jI| \leqslant \min\big(j(|I|-1)+1, n\big). \tag{1.8}$$

On s'intéressera tout particulièrement aux *intervalles d'entiers* dans les groupes cycliques, c'est-à-dire aux progressions arithmétiques de raison 1 modulo un certain entier n (dans ce cas, (1.8) est toujours une égalité, propriété que nous utiliserons plus tard – sous le nom de (1.8) également – à plusieurs reprises). Un tel intervalle I dans $\mathbb{Z}/n\mathbb{Z}$ sera dit *strict* s'il diffère de $\mathbb{Z}/n\mathbb{Z}$ tout entier. Dans ce cas, il n'y a qu'une façon d'écrire I sous la forme (qu'on qualifiera plus loin de *standard*) $\{a, a+1, a+2, \ldots, a+k\}$. Les éléments a et $a+k$ seront appelés respectivement *début* et *fin* de l'intervalle I et notés $d(I)$ et $f(I)$.

2. Quelques outils et un nouveau théorème additifs.

Commençons par rappeler le théorème de Kneser pour les suites entières (voir [8], [7] ou [20]).

THÉORÈME 4. — *Soient $(\mathcal{A}_i)_{1\leqslant i\leqslant n}$ des ensembles d'entiers dont les fonctions de comptage associées sont notées $(A_i)_{1\leqslant i\leqslant n}$. Si*

$$\underline{\mathrm{d}}(\mathcal{A}_1+\cdots+\mathcal{A}_n) < \liminf_{m\to+\infty} \frac{1}{m}\left(\sum_{i=1}^{n} A_i(m)\right),$$

l'ensemble $\mathcal{A}_1+\cdots+\mathcal{A}_n$ coïncide, à partir d'un certain entier, avec une réunion de progressions arithmétiques de même raison. Plus précisément, il existe un entier g tel que $\mathcal{A}_1+\cdots+\mathcal{A}_n \sim (\mathcal{A}_1+\cdots+\mathcal{A}_n)+g.\mathbb{N}$.

On en déduit immédiatement le corollaire suivant.

COROLLAIRE 5. — *Soient $(\mathcal{A}_i)_{1\leqslant i\leqslant n}$ des ensembles d'entiers dont les fonctions de comptage associées sont notées $(A_i)_{1\leqslant i\leqslant n}$. Si*

$$\liminf_{m\to+\infty} \frac{1}{m}\left(\sum_{i=1}^{n} A_i(m)\right) > 1,$$

il existe un entier g tel que l'ensemble $\mathcal{A}_1+\cdots+\mathcal{A}_n$ coïncide, à partir d'un certain entier, avec la réunion de progressions arithmétiques de raison g, $(\mathcal{A}_1+\cdots+\mathcal{A}_n)+g.\mathbb{N}$.

Passons maintenant à des résultats nécessités par le «versant groupe» de notre démonstration. Citons d'abord le lemme préhistorique qui résulte d'une application banale du principe des tiroirs.

LEMME 6 (Lemme préhistorique). — *Soit G un groupe abélien fini. Soient $\mathcal{A}$ et $\mathcal{B}$ deux sous-ensembles de G satisfaisant l'inégalité $|\mathcal{A}|+|\mathcal{B}|>|G|$. On a $\mathcal{A}+\mathcal{B}=G$.*

Le théorème de Kneser pour les suites entières admet un analogue pour les groupes abéliens [16, 17]. C'est une généralisation du fameux théorème de Cauchy-Davenport [2] (le lecteur pourra également se reporter au livre [19]).

THÉORÈME 7 (Théorème de Kneser). — *Soit G un groupe abélien quelconque. Soient $\mathcal{A}$ et $\mathcal{B}$ deux sous-ensembles finis de G satisfaisant l'inégalité*

$$|\mathcal{A}+\mathcal{B}| \leqslant |\mathcal{A}|+|\mathcal{B}|-1.$$

Si H désigne le stabilisateur de $\mathcal{A}+\mathcal{B}$, on dispose de l'égalité suivante

$$|\mathcal{A}+\mathcal{B}| = |\mathcal{A}+H|+|\mathcal{B}+H|-|H|.$$

Nous utiliserons ce théorème sous la forme de l'immédiat corollaire suivant.

COROLLAIRE 8. — *Soit G un groupe abélien fini. Soient $\mathcal{A}$ et $\mathcal{B}$ deux sous-ensembles de G tels que $\mathcal{A}+\mathcal{B}$ ne soit pas dégénéré. On a*

$$|\mathcal{A}+\mathcal{B}| \geqslant |\mathcal{A}|+|\mathcal{B}|-1.$$

Un pas supplémentaire par rapport au théorème de Kneser a été fait par ould Hamidoune grâce à la méthode isopérimétrique [9, 10, 11]. L'énoncé suivant (obtenu dans [13], comme Lemma 3.2) étend très légèrement un résultat présent implicitement dans [11] et explicitement dans [12]. Il nous sera particulièrement utile.

THÉORÈME 9. — *Soit $\mathcal{A}$ un sous-ensemble, contenant 0 et générateur, d'un certain groupe abélien G. On est dans l'une des quatre situations suivantes :*

- $|\mathcal{A}| > (|G|+1)/2$,
- *$\mathcal{A}$ est une progression arithmétique,*
- *$\mathcal{A}$ est un ensemble vospérien,*
- *$\mathcal{A}$ admet un sous-groupe comme ensemble 2-critique.*

On aura aussi besoin d'un autre résultat additif dû originellement à Scherk [22]. Historiquement, ce résultat a été d'abord donné sur le tore $\mathbb{R}/\mathbb{Z}$. Ce n'est que par la suite qu'il a été traduit, utilisé et généralisé (par Kemperman [15]) dans sa version groupe cyclique.

THÉORÈME 10 (Théorème de Scherk). — *Soient G un groupe abélien fini et $\mathcal{A}$ et $\mathcal{B}$ deux sous-ensembles de G. Si l'inégalité*

$$|\mathcal{A}+\mathcal{B}| \leqslant |\mathcal{A}| + |\mathcal{B}| - 2$$

est satisfaite, tout élément de $\mathcal{A}+\mathcal{B}$ possède au moins deux représentations.

Ce théorème est suffisamment utile et peu connu à la fois pour qu'il nous semble valoir la peine d'en donner une preuve courte, due à ould Hamidoune.

Démonstration. — Supposons le résultat faux et considérons deux ensembles $\mathcal{A}$ et $\mathcal{B}$ satisfaisant

$$|\mathcal{A}+\mathcal{B}| \leqslant |\mathcal{A}| + |\mathcal{B}| - 2 \tag{2.1}$$

et tels qu'il existe un élément de $\mathcal{A}+\mathcal{B}$ avec une seule représentation. Par translations, on supposera que 0 est cet élément et que son unique représentation est $0+0$. Soient H le stabilisateur de $\mathcal{A}+\mathcal{B}$ et $\mathcal{A}_0$ (resp.

$\mathcal{B}_0$) l'intersection $\mathcal{A} \cap H$ (resp. $\mathcal{B} \cap H$). Le lemme préhistorique implique $|\mathcal{A}_0 \setminus \{0\}| + |\mathcal{B}_0| \leqslant |H|$ car dans le cas contraire

$$0 \in H = (\mathcal{A}_0 \setminus \{0\}) + \mathcal{B}_0 \subset \big(\mathcal{A} \setminus \{0\}\big) + \mathcal{B}$$

et 0 aurait au moins deux représentations. On a donc $|\mathcal{A}_0| + |\mathcal{B}_0| \leqslant |H| + 1$ d'où

$$\begin{aligned} |\mathcal{A}+H| + |\mathcal{B}+H| - |H| &\geqslant \big(|\mathcal{A}| + (|H| - |\mathcal{A}_0|)\big) + \big(|\mathcal{B}| + (|H| - |\mathcal{B}_0|)\big) - |H| \\ &\geqslant |\mathcal{A}| + |\mathcal{B}| - 1. \end{aligned}$$

Or, le théorème de Kneser implique que le membre de gauche dans cette inégalité vaut $|\mathcal{A} + \mathcal{B}|$, en contradiction avec (2.1). □

Du lemme préhistorique et du théorème de Scherk, on déduit aisément le corollaire suivant.

COROLLAIRE 11. — *Soient G un groupe abélien fini et $\mathcal{A}$ et $\mathcal{B}$ deux sous-ensembles de G. Si l'inégalité*

$$|\mathcal{A}| + |\mathcal{B}| \geqslant |G| + 2$$

est satisfaite, tout élément de G possède au moins deux représentations sous la forme $a + b$ ($a \in \mathcal{A}$, $b \in \mathcal{B}$).

Pour la suite de cet article, nous aurons besoin d'un peu plus que ces rappels. Nous allons maintenant démontrer un nouveau résultat additif utile à la preuve du lemme isopérimétrique de la partie 4. Ce résultat, d'intérêt général, devrait pouvoir servir dans d'autres contextes.

THÉORÈME 12. — *Soit $\mathcal{A}$ un sous-ensemble contenant 0, générateur et 2-séparable d'un certain groupe abélien fini G. On suppose, de plus, que $|\mathcal{A}| \leqslant |G|/2$ et $\kappa_2(G, \mathcal{A}) \leqslant |\mathcal{A}| - 1$.*

Dans ces conditions, si $\mathcal{A}$ n'est pas une progression arithmétique, il existe un sous-groupe H de G, 2-critique pour $\mathcal{A}$, tel que $\mathcal{A}/H$ est soit une progression arithmétique, soit un ensemble vospérien dans G/H.

Démonstration. — Considérons un sous-ensemble $\mathcal{A}$ contenant 0, générateur et 2-séparable de G; et supposons que $|\mathcal{A}| \leqslant |G|/2$, $\kappa_2(G, \mathcal{A}) \leqslant |\mathcal{A}| - 1$ et que $\mathcal{A}$ n'est pas une progression arithmétique.

Appliquons d'abord le théorème 9 à $\mathcal{A}$. Les hypothèses faites sur $\mathcal{A}$ montrent qu'aucune des deux premières conclusions ne peut se produire. La troisième non plus car la 2-séparabilité de $\mathcal{A}$ et $\kappa_2(G,\mathcal{A}) \leqslant |\mathcal{A}| - 1$ montrent qu'il existe un ensemble $\mathcal{X}$ dans G de cardinal au moins 2 vérifiant $|\mathcal{A}+\mathcal{X}| \leqslant \min(|G|-2, |\mathcal{A}|+|\mathcal{X}|-1)$, ce qui exclut que $\mathcal{A}$ soit vospérien. C'est donc que $\mathcal{A}$ admet un sous-groupe comme ensemble 2-critique. Soit H un tel sous-groupe que l'on choisit, parmi les sous-groupes solutions, maximal pour l'inclusion.

Par définition, H vérifie entre autres

$$|\mathcal{A}+H| - |H| = \kappa_2(G,\mathcal{A}) \leqslant |\mathcal{A}| - 1,$$

on a donc

$$|\mathcal{A}/H| = \frac{|\mathcal{A}+H|}{|H|} \leqslant \frac{|\mathcal{A}|+|H|-1}{|H|} \leqslant \frac{|G|/2+|H|-1}{|H|}$$

d'où, par intégralité de $|\mathcal{A}/H|$,

$$|\mathcal{A}/H| \leqslant \frac{|G|}{2|H|} + \frac{1}{2} = \frac{|G/H|+1}{2}. \tag{2.2}$$

De plus, pour tout sur-groupe K strict ($|K/H| \geqslant 2$) de H, on a

$$|\mathcal{A}/H + K/H| \geqslant \min(|G/H|-1, |\mathcal{A}/H| + |K/H|) \tag{2.3}$$

car sinon

$$\begin{aligned} |\mathcal{A}+K| &= |(\mathcal{A}+K)/H|\ |H| \\ &\leqslant \min(|G/H|-2, |\mathcal{A}/H|+|K/H|-1)\ |H| \\ &= \min(|G|-2|H|, |\mathcal{A}/H| \times |H| + |K| - |H|) \\ &= \min(|G|-2|H|, |\mathcal{A}+H| - |H| + |K|) \\ &\leqslant \min(|G|-2, \kappa_2(G,\mathcal{A}) + |K|), \end{aligned}$$

ce qui contredirait la maximalité de H.

Cela dit, supposons que $\mathcal{A}/H$ ne soit pas vospérien et démontrons qu'il s'agit alors forcément d'une progression arithmétique. Puisque $\mathcal{A}/H$ n'est pas vospérien, il est 2-séparable et

$$\kappa_2(G/H, \mathcal{A}/H) \leqslant |\mathcal{A}/H| - 1. \tag{2.4}$$

Appliquons alors à nouveau le théorème 9 mais cette fois-ci à $\mathcal{A}/H \subset G/H$ (l'ensemble $\mathcal{A}/H$ contient évidemment 0 et engendre G/H). La première conclusion possible est exclue en vertu de la majoration (2.2) ; la troisième également par hypothèse. L'inégalité (2.3) montre que $\mathcal{A}/H$ ne peut admettre un sous-groupe comme ensemble 2-critique sans contredire (2.4), et la quatrième conclusion du théorème 9 ne peut pas non plus se produire. Ne reste que la deuxième : $\mathcal{A}/H$ est bien une progression arithmétique. □

3. Quelques outils combinatoires.

Dans cette partie, nous commençons par des rappels sur le théorème des trois distances. Ensuite, trois problèmes combinatoires modulaires qui rentrent en jeu naturellement dans l'étude de la fonction X sont présentés. Le premier a déjà été partiellement abordé par la littérature cependant que, pour les deux autres, nous devons développer une étude originale.

3.1. Le théorème des trois distances.

Dans ce chapitre, on présente quelques faits simples à propos du théorème des trois distances.

Une *suite circulaire* est une suite finie d'éléments distincts du tore $\mathbb{T} = \mathbb{R}/\mathbb{Z}$, $(x_i)_{0\leqslant i\leqslant m-1}$, telle que la différence $x_{i+1} - x_i$ ne dépende pas de i. Le terme traditionnel de suite circulaire ne cache donc rien d'autre qu'une progression arithmétique sans répétition. Pour une telle suite, on définit l'application *successeur géométrique* j qui est donnée par l'application successeur naturelle (au sens de l'ordre – croissant – sur $\mathbb{R}$) après projection sur $[0,1[$. On finit de caractériser j en précisant que le successeur géométrique du plus grand élément (dans $[0,1[$) est le plus petit. En fait, on fera plutôt porter la fonction j sur les indices i que sur les x_i eux-mêmes : ce sera donc une bijection de $\{0,\dots,m-1\}$ sur lui-même.

On définit ensuite les *paramètres* d'une suite circulaire comme étant les entiers s et q tels que $j(s) = 0$ et $j(0) = q$. On montre facilement (c'est la proposition 1.3 de [3]) que

$$s + q \geqslant m.$$

Le théorème des trois distances, d'abord conjecturé par Steinhaus, puis démontré par Sós [23], Świerczkowski [27] et Surányi [26], énonce que l'application j est affine par morceaux avec au plus *trois* morceaux.

THÉORÈME 13 (Théorème des trois distances). — *Soit* $(x_i)_{0\leqslant i\leqslant m-1}$ *une suite circulaire de paramètres* s *et* q. *On a*

$$j(i) = \begin{cases} i+q & \text{si } 0 \leqslant i \leqslant m-q-1, \\ i+q-s & \text{si } m-q \leqslant i \leqslant s-1, \\ i-s & \text{si } s \leqslant i \leqslant m-1. \end{cases}$$

Dans le cas où l'on a $m = s+q$, on dit que la suite circulaire est *à deux distances*. En effet, la portion linéaire intermédiaire de la fonction j est alors inexistante.

Le théorème des trois distances est lié à la théorie de l'approximation et à la notion de réduite de Farey (voir par exemple le très classique [14] pour une introduction à cette notion). Rappelons seulement qu'une fraction *irréductible* a/b est une *réduite de Farey* d'un réel α si aucune autre fraction de dénominateur inférieur ou égal à b n'appartient à l'intervalle délimité par α et a/b.

Nous utiliserons le résultat suivant dont on trouvera une démonstration dans [3].

LEMME 14 (Corollaire 2.6 de [3]). — *Si* t *est le dénominateur d'une réduite de Farey d'un réel* α *quelconque, toute suite circulaire d'incrément* α *et de cardinal* t *est une suite circulaire à deux distances.*

Dans la partie suivante, nous utiliserons ce lemme pour obtenir un résultat sur le recouvrement des groupes cycliques par des intervalles.

3.2. Recouvrement intervallaire.

Deléglise a étudié le problème du recouvrement du tore $\mathbb{T}$ par les multiples d'un intervalle réel. Le résultat principal de son article [3] (on notera que les cas $h = 1$ et 2 sont évidents et que ce sont les seuls cas de recouvrement parfait) est le suivant :

LEMME 15 (Théorème A de [3]). — *Soit* h *un entier strictement positif. Soit* I *un intervalle fermé du tore, de longueur minimale* $L(h)$,

tel que $I \cup 2I \cup \cdots \cup hI = \mathbb{T}$. *On a*

$$L(h) = \begin{cases} 1 & \text{si } h = 1, \\ 1/3 & \text{si } h = 2, \\ 3/\big(h(h+2)\big) & \text{si } h \geqslant 3 \text{ et } h \equiv 0 \text{ ou } 1 \pmod 3, \\ 3/\big(h(h+2)-2\big) & \text{si } h \geqslant 3 \text{ et } h \equiv 2 \pmod 3. \end{cases}$$

Ici, on s'intéresse plutôt au recouvrement de groupes cycliques par un intervalle d'entiers (au sens donné dans le chapitre 1.3). Définissons avec Deléglise la quantité $L(n,h)$ comme la longueur du plus court intervalle d'entiers J modulo n tel que

$$J \cup 2J \cup \cdots \cup hJ = \mathbb{Z}/n\mathbb{Z}. \tag{3.1}$$

Notons enfin, ce qui nous sera plus utile, $C(n,h)$ le cardinal du plus court intervalle d'entiers J modulo n vérifiant (3.1). Évidemment, on a

$$C(n,h) = L(n,h) + 1.$$

Remarquons qu'au besoin on pourra supposer que $h < n$ à défaut de quoi $C(n,h) = 1$ (il suffit de prendre l'intervalle réduit à l'élément unité). Dans le cas $n > h$, on aura évidemment toujours $C(n,h) \geqslant 2$.

Si l'on veut obtenir une borne inférieure pour $C(n,h)$, on peut toujours utiliser la relation de recouvrement (3.1) et la borne (1.8). On en déduit par un calcul simple (voir la preuve du lemme 16 ci-après) que

$$\frac{h(h+1)}{2}\,(C(n,h)-1) \geqslant n - h. \tag{3.2}$$

Cette borne est a priori grossière puisqu'on ne tient pas compte de ce que les multiples des intervalles considérés ne sont pas toujours deux à deux disjoints.

Une autre idée pour établir une borne inférieure pour $L(n,h)$ (et donc pour $C(n,h)$), ainsi qu'il est signalé dans [3], est de se servir du lemme 15.

LEMME 16. — *Soient n et h deux entiers strictement positifs. On a, pour toute valeur de l'entier n,*

$$C(n,1) = n \qquad \text{et} \qquad C(n,2) = \left\lceil \frac{n+1}{3} \right\rceil$$

et si $h \geqslant 3$,

$$C(n,h) \geqslant \left\lceil nL(h) + \frac{1}{3} \right\rceil .$$

Ce résultat est souvent meilleur que (3.2). C'est en particulier le cas lorsque n est grand par rapport à h. Inversement, si n est petit, il arrive que ce lemme fournisse de moins bons résultats que l'inégalité (3.2) : par exemple si h est divisible par 9 et $n = 5h(h+2)/9$, le lemme 16 donne seulement $C(n,h) \geqslant 2$ tandis que (3.2) fournit

$$C(n,h) \geqslant 1 + \left\lceil \frac{10h+2}{9(h+1)} \right\rceil \geqslant 3,$$

si $h \geqslant 9$.

Démonstration du lemme 16. — Si $h = 1$, le résultat est évident. Si h vaut 2, et si un intervalle d'entiers J vérifie $J \cup 2J = \mathbb{Z}/n\mathbb{Z}$, on a forcément $|J| + |2J| \geqslant n$ puis comme, par (1.8), $|2J| \leqslant 2|J| - 1$, il vient $|J| \geqslant (n+1)/3$ (c'est en fait l'inégalité (3.2)). Le résultat découle alors de ce que l'intervalle $\{\lceil \frac{n+1}{3} \rceil, \ldots, 2\lceil \frac{n+1}{3} \rceil - 1\}$ vérifie $J \cup 2J = \mathbb{Z}/n\mathbb{Z}$.

Supposons maintenant $h \geqslant 3$. Soit $J = \{a, \ldots, b\}$ un intervalle d'entiers de cardinal minimal $C(n,h)$ vérifiant $J \cup 2J \cup \cdots \cup hJ = \mathbb{Z}/n\mathbb{Z}$. On considère I l'intervalle du tore $\left[\frac{a-1/3}{n}, \frac{b+1/3}{n} \right]$. On vérifie alors que l'on a bien $I \cup 2I \cup \cdots \cup hI = \mathbb{T}$, d'où

$$C(n,h) = b - a + 1 = n\left(\frac{b+1/3}{n} - \frac{a-1/3}{n} \right) + \frac{1}{3} \geqslant nL(h) + \frac{1}{3},$$

et le résultat suit. □

Ce résultat est moins fort que celui qui est annoncé dans [3], à savoir $L(n,h) = [nL(h)] + \epsilon(n,h)$ où la fonction $\epsilon(n,h)$ vaut 0 si $nL(h)$ est entier, et 1 ou 2 sinon. Cependant, comme nous l'a aimablement fait savoir son auteur, cet énoncé de [3] est sujet à caution. Il est en particulier faux pour $h = 2$, cas dans lequel il fournirait, si n n'est pas divisible par 3, $C(n,2) = 1 + [n/3] + \epsilon(n,2) \geqslant 2 + [n/3] = 1 + \lceil \frac{n+1}{3} \rceil$, ce qui est contraire à la formule donnée dans le lemme 16. Dans le cas $h = 3$, pour donner un autre exemple, cette formule fournirait $C(n,3) = 1 + [n/5] + \epsilon(n,3) \geqslant 2 + [n/5]$ si 5 ne divise pas n, soit par exemple $C(6,3) \geqslant 3$ alors que l'intervalle $\{2,3\}$ suffit à voir que $C(6,3) = 2$.

Dans cet article, nous aurons besoin d'un résultat légèrement (mais strictement) plus fort que la formule (3.2) pour *toutes* les valeurs de n, et en particulier pour les petites (par rapport à h, toujours). Ne pouvant utiliser le lemme 16, nous allons donc devoir établir un résultat indépendant de celui de [3], dont nous reprendrons cependant la technique. Le résultat suivant (lemme 17) sera le cœur de cette partie. Il est visiblement meilleur que la formule (3.2) et ne découle donc pas non plus en général du lemme 16.

LEMME 17. — *Soient n et h deux entiers vérifiant $n > h \geqslant 2$. Si $h = 2$ et $n \equiv 2 \pmod 3$ ou si $h = 3$ et $n = 8$, on a*

$$\frac{h(h+1)}{2}(C(n,h)-1) = n-2\,;$$

dans tous les autres cas,

$$\frac{h(h+1)}{2}(C(n,h)-1) \geqslant n-1.$$

Avant de passer à la preuve de ce lemme proprement dite, commençons par une définition et quelques résultats faciles. Soient I et J deux intervalles stricts de $\mathbb{Z}/n\mathbb{Z}$ tels que J ne soit pas inclus dans I. Le *recouvrement* de I par J, noté $\mathrm{Rec}\,(I,J)$ est l'intervalle vide si $d(J) \notin I$ et l'intervalle strict $\{d(J), d(J)+1, \ldots, f(I)\}$ dans le cas contraire (les notations utilisées ici ont été introduites dans le chapitre 1.3). C'est un sous-ensemble de $I \cap J$ qui peut bien sûr être différent de $I \cap J$ (considérer par exemple dans $\mathbb{Z}/4\mathbb{Z}$, $I = \{2,3,0\}$ et $J = \{0,1,2\}$).

LEMME 18. — *Soient I un intervalle de $\mathbb{Z}/n\mathbb{Z}$ et p et q deux entiers strictement positifs tels que qI soit inclus dans pI. Alors, si pI est un intervalle strict, $(q-1)I$ est inclus dans $(p-1)I$.*

L'hypothèse exigeant que pI soit strict est nécessaire comme le montre l'exemple $p = 2$, $q = 1$ et I quelconque de cardinal $> n/2$ et ne contenant pas 0.

Démonstration. — Soit $I = \{a, \ldots, b\}$. Les hypothèses montrent que l'intervalle pI, dans sa forme standard, se présente comme ceci :

$$pI = \{pa, pa+1, \ldots, \underbrace{qa, qa+1, \ldots, qb}_{=qI}, qb+1, \ldots, pb\}.$$

En effet, si les éléments pa, qa, qb et pb ne se présentaient pas dans cet ordre dans l'écriture standard de pI, cet intervalle ne pourrait être strict. Il suffit alors de constater que

$$(p-1)I = \{(p-1)a, (p-1)a+1, \dots, \underbrace{(q-1)a, (q-1)a+1, \dots, (q-1)b}_{=(q-1)I}, (q-1)b+1, \dots, (p-1)b\}.$$

□

LEMME 19. — *Soient I un intervalle de $\mathbb{Z}/n\mathbb{Z}$ et p et q deux entiers positifs. On suppose que qI n'est pas inclus dans pI et que $(p+1)I$ et $(q+1)I$ sont stricts.*

Si $d(qI) \in pI$ ou si $d(qI) = f(pI)+1$, on a

$$\big|\mathrm{Rec}\,\big((p+1)I, (q+1)I\big)\big| = |\mathrm{Rec}\,(pI, qI)| + |I| - 1.$$

Démonstration. — Remarquons tout d'abord que le lemme 18 implique que l'intervalle $(q+1)I$ n'est pas inclus dans $(p+1)I$.

Soit $I = \{a, \dots, b\}$. On a $pI = \{pa, \dots, pb\}$ et $qI = \{qa, \dots, qb\}$.

Nous n'examinerons que le cas où $d(qI) \in pI$ (le second cas d'application du lemme, i.e. $d(qI) = f(pI)+1$, se démontrerait de manière analogue).

On a alors $qa \in pI$ et $qb \notin pI$ (sinon $qI \subset pI$). On observe que

$$\mathrm{Rec}\,(pI, qI) = \{qa, \dots, pb\}.$$

On a

$$\mathrm{Rec}\,\big((p+1)I, (q+1)I\big) = \{(q+1)a, \dots, (p+1)b\},$$

de sorte que, de Rec (pI, qI) à Rec $\big((p+1)I, (q+1)I\big)$, l'augmentation de cardinal vaut $(p+1)b - (q+1)a - (pb - qa) = b - a = |I| - 1$. □

Démonstration du lemme 17. — Tout d'abord, on vérifie sans peine grâce au lemme 16 que si $h = 2$ et $n \equiv 2 \pmod 3$, on a bien

$$\frac{h(h+1)}{2}(C(n,h) - 1) = n - 2. \tag{3.3}$$

Il en est de même si $h = 3$ et $n = 8$ puisqu'alors $C(n, h) = 2$.

Démontrons maintenant que l'inégalité

$$\frac{h(h+1)}{2}(C(n,h)-1) \geqslant n-1 \tag{3.4}$$

vaut pour tous les autres cas. Avant de commencer, on notera que le membre de gauche de (3.4) étant toujours entier, il suffit de montrer qu'il est minoré strictement par $n-2$.

Soit $I = \{a, a+1, \ldots, a+c-1\}$ un intervalle de $c = C(n,h) \geqslant 2$ (car $n > h$) entiers vérifiant

$$I \cup 2I \cup \ldots \cup hI = \mathbb{Z}/n\mathbb{Z}. \tag{3.5}$$

Dans toute cette démonstration, afin de pouvoir appliquer le lemme 19, on supposera que $h(c-1) \leqslant n-2$ de sorte que tous les intervalles jI considérés ci-après ($j \leqslant h$) seront stricts. Si tel n'était pas le cas, la conclusion serait immédiate.

Soit t l'entier minimal tel que $0 \in tI$. On pose

$$r = h - t.$$

On a clairement

$$I \subset (t+1)I,\ 2I \subset (t+2)I,\ \ldots,\ rI \subset hI.$$

Cela montre que

$$(r+1)I \cup (r+2)I \cup \cdots \cup hI = \mathbb{Z}/n\mathbb{Z}. \tag{3.6}$$

Notons aussi, par minimalité de t et le lemme 18, qu'aucun intervalle $(r+i)I$ (avec $1 \leqslant i \leqslant t$) n'est inclus dans un autre.

Soit maintenant la suite $(x_i)_{0 \leqslant i \leqslant t-1}$ du tore définie par

$$x_i = \{(r+1+i)a/n\}.$$

Elle est circulaire d'après les hypothèses (c'est bien une progression arithmétique à termes distincts par définition de t). Soient alors s et q ses paramètres : ils sont compris entre 0 et $t-1$.

Posons $\alpha = a/n$ et $\beta = (a+c-1)/n$. Par définition, t est le plus petit des entiers u tels qu'il existe un entier m vérifiant

$$u\frac{a}{n} \leqslant m \leqslant u\frac{a+c-1}{n}.$$

Autrement dit, t est le plus petit entier tel qu'il existe un entier m tel que

$$\alpha \leqslant \frac{m}{t} \leqslant \alpha + \frac{c-1}{n}.$$

Cela signifie que t *est* le dénominateur d'une réduite de Farey (d'ailleurs par excès) de α. Dans ces conditions, le lemme 14 permet d'affirmer que la suite $(x_i)_{0\leqslant i\leqslant t-1}$ est une suite circulaire à *deux* paramètres. En particulier, on a $s+q=t$ ou encore

$$s+q+r=h \tag{3.7}$$

et l'application successeur géométrique est donnée par

$$j(i) = \begin{cases} i+q & \text{si } 0 \leqslant i \leqslant s-1 \\ i-s & \text{si } s \leqslant i \leqslant t-1. \end{cases}$$

En particulier, le successeur géométrique du début de $(r+1)I$ est celui de $(r+q+1)I$. Par (3.6), on en déduit que soit le recouvrement de $(r+1)I$ par $(r+q+1)I$ n'est pas vide, soit la fin de $(r+1)I$ vaut (modulo n) un de moins que le début de $(r+q+1)I$. Dans les deux cas, le recouvrement de $(r+2)I$ par $(r+q+2)I$ ne peut être vide et contient en fait (par le lemme 19) au moins $c-1$ éléments. De proche en proche, on observe alors que

$$\begin{aligned} &|\mathrm{Rec}\,\big((r+2)I,(r+q+2)I\big)| \geqslant (c-1) \\ &|\mathrm{Rec}\,\big((r+3)I,(r+q+3)I\big)| \geqslant 2(c-1) \\ &\qquad\vdots \\ &|\mathrm{Rec}\,\big((h-q)I,hI\big)| \geqslant (h-q-r-1)(c-1) = (s-1)(c-1). \end{aligned} \tag{3.8}$$

De façon analogue, mais en considérant cette fois-ci le prédécesseur géométrique, on trouve

$$\begin{aligned} &|\mathrm{Rec}\,\big((r+s+2)I,(r+2)I\big)| \geqslant (c-1) \\ &|\mathrm{Rec}\,\big((r+s+3)I,(r+3)I\big)| \geqslant 2(c-1) \\ &\qquad\vdots \\ &|\mathrm{Rec}\,\big(hI,(h-s)I\big)| \geqslant (h-s-r-1)(c-1) = (q-1)(c-1). \end{aligned} \tag{3.9}$$

Or, on a

$$(3.10)\quad |(r+1)I| + |(r+2)I| + \cdots + |hI| \geqslant |(r+1)I \cup (r+2)I \cup \cdots \cup hI| + \sum_{i=0}^{t-1} |\mathrm{Rec}\,\big((r+1+i)I, (r+1+j(i))I\big)|,$$

ainsi qu'on l'observe en partitionnant chaque intervalle $(r+1+i)I$ (pour $0 \leqslant i \leqslant t-1$) en deux sous-intervalles : celui allant de $d\big((r+1+i)I\big)$ à $d\big((r+1+j(i))I\big) - 1$ puis celui (éventuellement vide) allant de $d\big((r+1+j(i))I\big)$ à $f\big((r+1+i)I\big)$. Cette partition nécessite évidemment que $d\big((r+1+j(i))I\big)$ appartienne à $(r+1+i)I$ ou soit égal à $f\big((r+1+i)I\big)+1$ et que $(r+1+j(i))I \not\subset (r+1+i)I$, deux propriétés qui sont bien vérifiées. Notons que l'équation analogue de (3.10) où les recouvrements seraient remplacés par des intersections serait en général fausse.

D'après (3.10), (3.6), (3.8) et (3.9), on a alors

$$(3.11)\quad \begin{aligned} &|(r+1)I| + |(r+2)I| + \cdots + |hI| \\ &\geqslant n + \big((c-1) + \cdots + (s-1)(c-1)\big) + \big((c-1) + \cdots + (q-1)(c-1)\big) \\ &= n + (c-1)\left(\frac{s(s-1)+q(q-1)}{2}\right). \end{aligned}$$

Or, en utilisant (1.8), on trouve que pour toute valeur de $k \leqslant h$

$$|I| + |2I| + \cdots + |kI| = \frac{k(k+1)}{2}(c-1) + k.$$

De l'application de cette formule pour $k = h$ puis r ainsi que de (3.11), on déduit alors que

$$\frac{h(h+1)}{2}(c-1) \geqslant n + \frac{1}{2}(c-1)\big(s(s-1) + q(q-1) + r(r+1)\big) + r - h.$$

Pour démontrer le lemme, il suffit donc de démontrer que

$$(3.12)\qquad \frac{1}{2}(c-1)\big(s(s-1) + q(q-1) + r(r+1)\big) + r - h > -2$$

puis, c étant au moins égal à 2,

$$(3.13)\qquad \frac{1}{2}\big(s(s-1) + q(q-1) + r(r+1)\big) + r - h > -2.$$

Supposons d'abord que r est différent de 0. La minoration (3.13) découlerait alors de

$$\frac{1}{2}\big(s(s-1)+q(q-1)+r(r+1)\big)-h>-3.$$

Or le minimum de la fonction du membre de gauche sujet à la contrainte (3.7) est atteint en $s=q=(h+1)/3$, $r=(h-2)/3$ et vaut $(h+1)(h-2)/6$. Le résultat découle alors de ce qu'effectivement

$$\frac{1}{6}(h+1)(h-2)-h>-3,$$

pour toute valeur de $h\geqslant 2$.

On suppose désormais que r vaut 0. Un calcul analogue à celui présenté plus haut montre que (3.13) découle de

$$\frac{1}{2}\big(s(s-1)+q(q-1)\big)-h\geqslant h\left(\frac{h}{4}-\frac{3}{2}\right)>-2,$$

pour toutes les valeurs de h au moins égales à 5. Restent les cas $h\in\{2,3,4\}$.

Dans le cas $h=2$, on calcule facilement grâce au lemme 16 que si $n\not\equiv 2 \pmod 3$,

$$\begin{aligned}\frac{h(h+1)}{2}(C(n,h)-1)&=\frac{h(h+1)}{2}\left(\left\lceil\frac{n+1}{3}\right\rceil-1\right)\\&>3\left(\frac{n+1}{3}-1\right)=n-2.\end{aligned}$$

Considérons maintenant les cas $h\in\{3,4\}$.

Supposons d'abord que c soit différent de 2. Alors $c\geqslant 3$ et, revenant à l'équation (3.12), pour démontrer le lemme il suffit de démontrer que

$$\big(s(s-1)+q(q-1)\big)-h>-2,$$

ce qui découle effectivement de

$$\big(s(s-1)+q(q-1)\big)-h\geqslant h\left(\frac{h}{2}-2\right)>-2,$$

pour $h=3$ et 4. On se ramène donc au seul cas $C(n,h)=c=2$.

Dans le cas $h = 4$, la borne (3.2) montre que $n \leqslant 14$. Il n'y a alors plus qu'un nombre fini (et petit) de situations à examiner. On constate alors qu'en fait un recouvrement (3.5) avec $|I| = 2$ implique $n \leqslant 11$ et donc l'inégalité (3.4).

Dans le cas $h = 3$, la borne (3.2) montre que $n \leqslant 9$. De même, on constate que (3.5) avec $|I| = 2$ implique $n \leqslant 7$ et donc (3.4), à l'unique exception près $n = 8$ et $I = \{2, 3\}$ ou $\{5, 6\}$.

Cela achève la preuve de ce lemme. □

3.3. Foncière génération maximale.

Soient $h \geqslant 1$ et $c \geqslant 2$ deux entiers. On notera $K_2(h, c)$ le plus grand entier k tel qu'il existe un entier g et un sous-ensemble foncièrement générateur $\mathcal{A}$, de cardinal c, dans $\mathbb{Z}/g\mathbb{Z}$ vérifiant les deux propriétés suivantes :

(i) $\mathcal{A} \cup 2\mathcal{A} \cup \ldots \cup h\mathcal{A} = \mathbb{Z}/g\mathbb{Z}$,

(ii) $(k-1)\mathcal{A} \neq \mathbb{Z}/g\mathbb{Z}$.

Bien évidemment, cet entier k vérifie $k\mathcal{A} = \mathbb{Z}/g\mathbb{Z}$. On définit ensuite

$$K(h) = \max_{c \geqslant 2} K_2(h, c).$$

Notre premier résultat concerne le cas $c = 2$.

THÉORÈME 20. — *Pour toute valeur strictement positive de h, on a*

$$K_2(h, 2) \geqslant \left[\frac{h(h+4)}{3} \right].$$

Démonstration. — La preuve de ce résultat suivra, pour toute valeur de l'entier h, de l'exhibition d'un module g, en l'occurrence

$$g = \left[\frac{h(h+4)}{3} \right] + 1,$$

et d'un entier x_0 tel que $x_0 - 1$ soit premier avec g (de sorte que $\mathcal{A} = \{1, x_0\}$ soit foncièrement générateur) tel que

$$\mathcal{U} = \mathcal{A} \cup 2\mathcal{A} \cup \ldots \cup h\mathcal{A} = \mathbb{Z}/g\mathbb{Z}. \tag{3.14}$$

Pour ce faire, nous allons distinguer trois cas.

(a) Si $h \equiv 0 \pmod 3$: on a $g = (h^2+4h+3)/3$ et l'on pose $x_0 = h+3$. On vérifie aisément que $x_0 - 1 = h+2$ est premier à $g = ((h+2)^2-1)/3$. Passons à la validation de (3.14) et fixons un entier x entre 1 et g. Sa division euclidienne par x_0 s'exprime sous la forme $x = qx_0 + r$, où $0 \leqslant r \leqslant h+2$ et $(q,r) \neq (0,0)$. On vérifie aussi que

$$q \leqslant \left[\frac{h^2+4h+3}{3(h+3)}\right] = \left[\frac{h+1}{3}\right] = \frac{h}{3}.$$

Ainsi $q + r \leqslant 4h/3 + 2$. En fait, on a même

$$q + r \leqslant 4h/3 + 1 \tag{3.15}$$

car, dans le cas contraire, on aurait $q = h/3$ et $r = h+2$ ce qui impliquerait l'impossible

$$x = \frac{h}{3}(h+3) + h + 2 = \frac{h^2+6h+6}{3} > g.$$

Maintenant, si $q+r \leqslant h$, on a $x \in (q+r)\mathcal{A} \subset \mathcal{U}$ (puisque évidemment $q+r \geqslant 1$). Nous supposons donc désormais que l'on a $q+r \geqslant h+1$. On va séparer deux sous-cas selon la valeur de r :

- Si l'on a $2h/3+2 \leqslant r \leqslant h+1$, il vient (ceci est légitimé par la positivité des coefficients apparaissant ci-dessous)

$$\begin{aligned} x + g &= qx_0 + r + \frac{h^2+4h+3}{3} \\ &= \left(q + \frac{h+3}{3}\right)(h+3) + \left(r - \frac{2(h+3)}{3}\right) \\ &\in \left(q + \frac{h+3}{3} + r - \frac{2(h+3)}{3}\right)\mathcal{A} \\ &= \left(q + r - \frac{h+3}{3}\right)\mathcal{A} \\ &\in \mathcal{U}, \end{aligned}$$

puisque, d'entre autres (3.15), on tire

$$1 \leqslant q + r - \frac{h+3}{3} \leqslant \frac{4h}{3} + 1 - \frac{h+3}{3} = h.$$

– Passons au cas où $r \leqslant 2h/3+1$. On a $q \leqslant h/3$ et donc $q+r \leqslant h+1$. Ainsi, la seule possibilité est que $r = 2h/3+1$ et $q = h/3$. Mais ceci correspond à une valeur de x valant

$$x = \frac{h}{3}(h+3) + \frac{2h}{3} + 1 = \frac{h^2+5h+3}{3} > g,$$

ce qui exclut ce cas et achève notre preuve dans le cas $h \equiv 0 \pmod 3$.

Les deux autres cas conduisent à des calculs du même acabit laissés au lecteur :

(b) Si $h \equiv 1 \pmod 3$: on a $g = (h^2+4h+1)/3$ et l'on peut prendre $x_0 = h+1$.

(c) Si $h \equiv 2 \pmod 3$: on a $g = (h^2+h)/3$ et l'on peut prendre $x_0 = (h^2+h)/3$. □

Il est tentant de conjecturer le résultat suivant.

CONJECTURE 21. — *Pour tout entier strictement positif h,*

$$K_2(h,2) = \left[\frac{h(h+4)}{3}\right].$$

En fait, l'étude spécifique de la fonction $K_2(\,.\,,2)$ se justifie d'abord par sa simplicité. Il n'y a aucune bonne raison de négliger les fonctions $K_2(\,.\,,c)$ pour c supérieur à trois. Au contraire, il est facile de voir que, quels que soient les entiers positifs c, h et q, on a $K_2(h,qc) \geqslant K_2(h,c)$: en effet, si l'ensemble, de cardinal c, $\mathcal{A} \subset \mathbb{Z}/g\mathbb{Z}$ permet d'atteindre une valeur de k égale à $K_2(h,c)$, il en est de même de l'ensemble $\mathcal{A} + \{0, g, \ldots, (q-1)g\} \subset \mathbb{Z}/qg\mathbb{Z}$ (qui est de cardinal qc). Étonnamment, un certain nombre de manipulations expérimentales (*cf.* la table 1 ci-dessous) montrent que cette remarque ne permet pas facilement d'amélioration pratique pour la minoration de la fonction K. En effet, $K_2(h,c)$ n'est jamais supérieur à $K_2(h,2)$ pour les petites valeurs de h et de c (au sens de la table 1). Remarquons que pour calculer $K_2(h,c)$ il n'y jamais qu'un nombre fini de possibilités à tester, de sorte qu'une recherche exhaustive est toujours possible (c'est ce que nous avons fait en l'occurrence) quoique parfois longue : dans la table 1 ci-dessous, les cases où l'on a porté un signe « – » correspondent aux cas où l'on n'a pas pu obtenir le résultat recherché en temps raisonnable.

Table 1. Premières valeurs de $K_2(h,c)$

c \ h	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	4	7	10	15	20	25	32	39	46	55	64	73	84	95	106
3	4	6	9	13	18	23	29	36	–	–	–	–	–	–	–
4	4	7	10	15	20	25	32	–	–	–	–	–	–	–	–
5	4	6	10	14	18	–	–	–	–	–	–	–	–	–	–
6	4	7	10	–	–	–	–	–	–	–	–	–	–	–	–

3.4. Recouvrement économique.

Il s'agit du problème dual de celui de la foncière génération maximale. L'intérêt de ce problème dans le cadre de notre étude provient notamment de ce que sa résolution pourrait permettre d'améliorer l'inégalité (4.8) et donc le résultat des lemmes 24 puis 25 (voir plus loin, chapitre 4). On utilisera et illustrera cette remarque dans le chapitre 5.3.

Soient g, h et c des entiers strictement positifs. On définit $\mathcal{M}_{h,c,g}$ comme l'ensemble des sous-ensembles de $\mathbb{Z}/g\mathbb{Z}$ suivants :

$$\mathcal{M}_{h,c,g} = \{\mathcal{A} \subset \mathbb{Z}/g\mathbb{Z},\ \text{foncièrement générateur,}\\ \text{vérifiant } \mathcal{A} \cup 2\mathcal{A} \cup \ldots \cup h\mathcal{A} = \mathbb{Z}/g\mathbb{Z} \text{ et } |\mathcal{A}| = c\}.$$

On définit ensuite

$$M_3(h,c,g) = \begin{cases} +\infty & \text{si } \mathcal{M}_{h,c,g} \text{ est vide,} \\ \min_{\mathcal{A} \in \mathcal{M}_{h,c,g}} (|\mathcal{A}| + \cdots + |h\mathcal{A}| - g) & \text{sinon,} \end{cases}$$

une quantité qui reste évidemment toujours positive ou nulle. On pose ensuite

$$M_2(h,c) = \min_{g \in \mathbb{N}} M_3(h,c,g)$$

et enfin

$$M(h) = \min_{c \in \mathbb{N}} M_2(h,c).$$

Nous ne pouvons que proposer le résultat suivant.

THÉORÈME 22. — *Pour tout entier strictement positif h, on a*

$$M(h) \leqslant \left[\frac{h^2+h-2}{6}\right].$$

Démonstration. — Il suffit de vérifier que $M_2(h,2)$ est bien majoré par la borne supérieure proposée dans l'énoncé. Or, pour h donné, il suffit de prendre

$$g = \left[\frac{h(h+4)}{3}\right] + 1$$

et $\mathcal{A}$ l'ensemble associé lors de la démonstration du théorème 20. Comme $|j\mathcal{A}| = j+1$, il vient

$$|\mathcal{A}| + \cdots + |h\mathcal{A}| - g = \frac{h(h+3)}{2} - \left[\frac{h(h+4)}{3}\right] - 1 = \left[\frac{h^2+h-2}{6}\right].$$

□

L'unique intérêt de ce résultat est qu'il pourrait bien être optimal, ce que traduit la conjecture suivante.

CONJECTURE 23. — *Pour tout entier strictement positif h, on a*

$$M(h) = \left[\frac{h^2+h-2}{6}\right].$$

Pour essayer d'étayer cette conjecture «naturelle», nous proposons maintenant quelques résultats expérimentaux obtenus par vérification exhaustive. Dans le cas $c = 2$, les résultats numériques sont sous-entendus par la conjecture 21. Dans le cas $c = 3$, nous avons obtenu :

Table 2. Quelques valeurs de $M_2(h,3)$

h	3	4	5	6	7
$M_2(h,3)$	2	4	7	11	15

Pour finir, citons les résultats numériques trouvés dans le cas $c = 4$.

Table 3. Quelques valeurs de $M_2(h,4)$

h	3	4	5	6
$M_2(h,4)$	2	6	8	12

Ce sont ces tables qui nous seront utiles dans le chapitre 5.3.

4. Un lemme isopérimétrique.

Le cœur de la démonstration de la borne supérieure dans le théorème 1 découlera du lemme 25 ci-dessous. Le lemme 24, que nous présentons d'abord, est un premier pas en direction du résultat du lemme 25.

LEMME 24. — *Soient h et n deux entiers strictement positifs et $\mathcal{E}$ un sous-ensemble foncièrement générateur de $\mathbb{Z}/n\mathbb{Z}$, tels que*

$$\mathcal{E} \cup 2\mathcal{E} \cup \ldots \cup h\mathcal{E} = \mathbb{Z}/n\mathbb{Z}.$$

On suppose que l'une des conditions suivantes est remplie :

- $|\mathcal{E}| > n/2$,
- *$\mathcal{E}$ est une progression arithmétique,*
- *$\mathcal{E}$ est un ensemble vospérien ;*

alors l'ensemble $\left(\frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil\right)\mathcal{E}$ est un ensemble dégénéré.

De plus, dans tous les cas sauf :

- *$n = 1$ (et h quelconque),*
- *$h = 1$ (et n quelconque),*
- *$h = 2$, $n = 5$ et $\mathcal{E} = \{2,3\}$ ou $\{1,4\}$,*
- *$h = 3$, $n = 8$ et $\mathcal{E} = \{2,3\}$ ou $\{1,6\}$ ou $\{2,7\}$ ou $\{5,6\}$,*

tout élément de $\left(\frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil\right)\mathcal{E}$ admet au moins deux représentations différentes.

Avant de passer à la preuve de ce lemme, notons que son résultat est optimal au sens où, dans les cas exclus pour la seconde conclusion, cette conclusion est fausse.

Démonstration. — Le cas $n = 1$ est évident (on a alors $|\mathcal{E}| = 1$ et il n'y a jamais qu'une seule somme dans $\left(\frac{h(h+1)}{2} + \lceil \frac{h-1}{3} \rceil\right)\mathcal{E}$, quelle que soit la valeur de h). Il est également facile de traiter les (autres) cas pour lesquels la seconde conclusion ne tient pas (et de comprendre pourquoi elle ne tient pas). Le cas $h = 1$ est immédiat puisqu'alors $\left(\frac{h(h+1)}{2} + \lceil \frac{h-1}{3} \rceil\right) = 1$ (et tout élément de $\mathcal{E} = \mathbb{Z}/n\mathbb{Z}$ a bien une unique représentation). Dans le cas $h = 2$, $n = 5$ et $\mathcal{E} = \{2,3\}$, on observe que $\left(\frac{h(h+1)}{2} + \lceil \frac{h-1}{3} \rceil\right) = 4$, puis que $4\mathcal{E} = \mathbb{Z}/5\mathbb{Z}$ (noter que 3 n'admet bien que l'unique représentation $2+2+2+2$). Le cas $\mathcal{E} = \{1,4\}$ s'en déduit car, modulo 5, $\{1,4\} = 2.\{2,3\}$. Il en est de même dans le cas $h = 3$, $n = 8$ et $\mathcal{E} = \{2,3\}$ car alors $\left(\frac{h(h+1)}{2} + \lceil \frac{h-1}{3} \rceil\right) = 7$ et $7\mathcal{E} = \mathbb{Z}/8\mathbb{Z}$ (ici également, 6 ne peut s'écrire autrement que sous la forme $2 + 2 + 2 + 2 + 2 + 2 + 2$). Les autres cas correspondent également à la multiplication par un élément inversible (modulo 8, cette fois).

Donnons-nous maintenant des entiers strictement positifs h et n, et un sous-ensemble $\mathcal{E}$ de $\mathbb{Z}/n\mathbb{Z}$ foncièrement générateur tel que

$$\mathcal{E} \cup 2\mathcal{E} \cup \ldots \cup h\mathcal{E} = \mathbb{Z}/n\mathbb{Z}. \tag{4.1}$$

On exclut les cas traités ci-dessus, en particulier on peut supposer

$$h \geqslant 2, \qquad n \geqslant 2 \qquad \text{et} \qquad |\mathcal{E}| \geqslant 2$$

(cette dernière minoration puisque $n \geqslant 2$ et que $\mathcal{E}$ est foncièrement générateur) et l'on cherche à démontrer que, sous l'une des trois conditions énoncées dans le lemme, $\left(\frac{h(h+1)}{2} + \lceil \frac{h-1}{3} \rceil\right)\mathcal{E}$ est un ensemble dégénéré dont tout élément admet au moins deux représentations différentes.

(i) Supposons tout d'abord que $|\mathcal{E}| > n/2$. Le lemme préhistorique montre alors que $2\mathcal{E} = \mathbb{Z}/n\mathbb{Z}$. Ainsi $|2\mathcal{E}| + |\mathcal{E}| \geqslant n + 2$ et l'application du corollaire 11 montre que $3\mathcal{E} = \mathbb{Z}/n\mathbb{Z}$ et que chaque élément admet au moins deux représentations. Il en est de même des multiples suivants de $\mathcal{E}$ et en particulier de $\left(\frac{h(h+1)}{2} + \lceil \frac{h-1}{3} \rceil\right)\mathcal{E}$ puisque $h \geqslant 2$ implique $\frac{h(h+1)}{2} + \lceil \frac{h-1}{3} \rceil \geqslant 4$. La conclusion s'ensuit (rappelons que $\mathbb{Z}/n\mathbb{Z}$ est bel et bien dégénéré).

(ii) Supposons maintenant que $\mathcal{E}$ est une progression arithmétique (finie) foncièrement génératrice dans $\mathbb{Z}/n\mathbb{Z}$. Sa raison est donc génératrice

(et donc inversible) dans $\mathbb{Z}/n\mathbb{Z}$. Multipliant par l'inverse de cette raison, on se ramène au cas où cette raison est égale à 1 et donc au cas d'un *intervalle* d'entiers.

Remarquons tout d'abord que l'on a, d'après (1.8), pour tout $i \geqslant 1$,

$$|i\mathcal{E}| = \min\big(i(|\mathcal{E}| - 1) + 1, n\big). \tag{4.2}$$

On peut supposer que

$$n > h.$$

En effet, dans le cas contraire, (4.2) impliquerait $(h-1)\mathcal{E} = \mathbb{Z}/n\mathbb{Z}$. Ainsi on aurait $h\mathcal{E} = \mathbb{Z}/n\mathbb{Z}$ et chaque élément admettrait au moins deux représentations. Il en serait de même des multiples suivants de $\mathcal{E}$ et en particulier de $\left(\frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil\right)\mathcal{E}$.

Si l'on n'est ni dans le cas $h = 2$ et $n \equiv 2 \pmod 3$, ni dans le cas $h = 3$, $n = 8$, il vient alors, d'après le lemme 17,

$$\frac{h(h+1)}{2}\,(|\mathcal{E}| - 1) \geqslant n - 1. \tag{4.3}$$

Grâce à (4.2) et (4.3), on obtient lorsque $i = h(h+1)/2$,

$$\left|\frac{h(h+1)}{2}\mathcal{E}\right| \geqslant n$$

ou encore

$$\frac{h(h+1)}{2}\mathcal{E} = \mathbb{Z}/n\mathbb{Z}.$$

La conclusion s'ensuit, comme dans le cas (i), par une application du corollaire 11 puisqu'alors

$$\left|\frac{h(h+1)}{2}\mathcal{E}\right| + |\mathcal{E}| \geqslant n + 2. \tag{4.4}$$

Supposons maintenant que $h = 2$ et $n \equiv 2 \pmod 3$ ou bien que $h = 3$ et $n = 8$. Grâce à la première partie du lemme 17 et (4.2), on observe que l'on a tout de même

$$\left|\frac{h(h+1)}{2}\mathcal{E}\right| \geqslant n - 1$$

ce qui donne la conclusion souhaitée par le même raisonnement que plus haut dès que $|\mathcal{E}| \geqslant 3$ (puisque (4.4) est encore valable).

Ne reste plus à étudier que les deux cas $h = 2$, $n \equiv 2 \pmod 3$ et $h = 3$, $n = 8$ sous l'hypothèse $|\mathcal{E}| = 2$, et en particulier $C(n,h) = 2$. Si $h = 2$ et $n \equiv 2 \pmod 3$, on trouve l'unique solution $n = 5$ (d'après le lemme 16). Or, dans les deux cas $h = 2$, $n = 5$ et $h = 3$, $n = 8$, les ensembles foncièrement générateurs $\mathcal{E}$ de cardinal 2 vérifiant $\mathcal{E} \cup 2\mathcal{E} \cup \ldots \cup h\mathcal{E} = \mathbb{Z}/n\mathbb{Z}$ sont exactement ceux qui sont exclus dans l'énoncé du lemme.

(iii) Supposons maintenant que $\mathcal{E}$ est vospérien : il vérifie l'inégalité

$$|\mathcal{E} + \mathcal{E}'| \geqslant \min(|\mathcal{E}| + |\mathcal{E}'|, n-1) \tag{4.5}$$

pour *tout* ensemble $\mathcal{E}' \subset \mathbb{Z}/n\mathbb{Z}$ de cardinal au moins égal à 2.

Nous pouvons évidemment supposer que

$$|\mathcal{E}| \geqslant 3$$

car tout ensemble à deux éléments est une progression arithmétique, un cas réglé par (ii).

On peut aussi supposer que pour tout $i \leqslant \frac{h(h+1)}{2} + \lceil \frac{h-1}{3} \rceil - 1$, on a

$$|i\mathcal{E}| \leqslant n-2. \tag{4.6}$$

En effet, dans le cas contraire, on aurait en particulier

$$\left| \left(\frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil - 1 \right) \mathcal{E} \right| \geqslant n-1,$$

puis

$$|\mathcal{E}| + \left| \left(\frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil - 1 \right) \mathcal{E} \right| \geqslant n+2,$$

d'où la conclusion encore une fois d'après le corollaire 11.

De là, on déduit que si i est inférieur ou égal à $\frac{h(h+1)}{2} + \lceil \frac{h-1}{3} \rceil - 2$, on a

$$|(i+1)\mathcal{E}| \geqslant |\mathcal{E}| + |i\mathcal{E}|. \tag{4.7}$$

En effet, on a $i+1 \leqslant \frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil - 1$ et l'on trouve alors, par (4.5) et (4.6),

$$n-2 \geqslant |(i+1)\mathcal{E}| = |\mathcal{E} + i\mathcal{E}| \geqslant \min(|\mathcal{E}| + |i\mathcal{E}|, n-1)$$

ce qui implique l'inégalité (4.7).

Ces préliminaires étant établis, on peut revenir au cœur de la démonstration. De la relation (4.1) vérifiée par hypothèse, on tire immédiatement

$$|\mathcal{E}| + |2\mathcal{E}| + \cdots + |h\mathcal{E}| \geqslant n \tag{4.8}$$

puis

$$\begin{aligned} \left(\left\lceil \frac{h-1}{3} \right\rceil + 1\right) |\mathcal{E}| + |2\mathcal{E}| + \ldots + |h\mathcal{E}| &\geqslant n + \left\lceil \frac{h-1}{3} \right\rceil |\mathcal{E}| \\ &\geqslant n + 3\left\lceil \frac{h-1}{3} \right\rceil \\ &\geqslant n + h - 1. \end{aligned} \tag{4.9}$$

Pour simplifier la présentation des calculs ci-dessous, on distinguera les cas $h \geqslant 4$, $h = 3$ et $h = 2$.

On supposera dans un premier temps que h est supérieur ou égal à 4, ce qui implique en particulier l'inégalité $3 + \left\lceil \frac{h-1}{3} \right\rceil \leqslant h$.

Regroupons d'abord les sommants du membre de gauche de (4.9)

(4.10)

$$\begin{aligned} &\left(\left\lceil \frac{h-1}{3} \right\rceil + 1\right) |\mathcal{E}| + |2\mathcal{E}| + \ldots + |h\mathcal{E}| \\ &\quad = \left((|\mathcal{E}| + |2\mathcal{E}|) + (|\mathcal{E}| + |3\mathcal{E}|) + \cdots + \left(|\mathcal{E}| + \left|\left(2 + \left\lceil \frac{h-1}{3} \right\rceil\right)\mathcal{E}\right|\right)\right) \\ &\qquad + \left(\left|\left(3 + \left\lceil \frac{h-1}{3} \right\rceil\right)\mathcal{E}\right| + \cdots + |h\mathcal{E}|\right). \end{aligned}$$

Maintenant, appliquons à chacun des regroupements du type $|\mathcal{E}| + |i\mathcal{E}|$ (on a bien $i \leqslant 2 + \left\lceil \frac{h-1}{3} \right\rceil \leqslant \frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil - 2$) apparaissant dans le membre

de droite de cette formule l'inégalité (4.7). La formule (4.10) fournit alors

$$\left(\left\lceil\frac{h-1}{3}\right\rceil+1\right)|\mathcal{E}|+|2\mathcal{E}|+\ldots+|h\mathcal{E}| \leqslant \left(|3\mathcal{E}|+|4\mathcal{E}|+\cdots+\left|\left(3+\left\lceil\frac{h-1}{3}\right\rceil\right)\mathcal{E}\right|\right) + \left(\left|\left(3+\left\lceil\frac{h-1}{3}\right\rceil\right)\mathcal{E}\right|+\cdots+|h\mathcal{E}|\right).$$

Pour simplifier la suite de la présentation de l'argument, notons $(c_i)_{1\leqslant i\leqslant h-1}$ la suite des coefficients de $\mathcal{E}$ apparaissant dans le membre de droite de cette inégalité :

$$c_1=3,\ c_2=4,\ \ldots,\ c_{1+\lceil\frac{h-1}{3}\rceil}=3+\left\lceil\frac{h-1}{3}\right\rceil,$$
$$c_{2+\lceil\frac{h-1}{3}\rceil}=3+\left\lceil\frac{h-1}{3}\right\rceil,\ \ldots,\ c_{h-1}=h.$$

Maintenant de deux choses l'une :

– Ou bien pour tout entier $3\leqslant i\leqslant h-1$, on a

$$|(c_2+\ldots+c_i)\mathcal{E}|\geqslant|(c_2+\ldots+c_{i-1})\mathcal{E}|+|c_i\mathcal{E}|-1 \tag{4.11}$$

et il vient, par une récurrence immédiate,

$$\left(\left\lceil\frac{h-1}{3}\right\rceil+1\right)|\mathcal{E}|+|2\mathcal{E}|+\ldots+|h\mathcal{E}| \leqslant\left|\left(\frac{h(h+1)}{2}+\left\lceil\frac{h-1}{3}\right\rceil-3\right)\mathcal{E}\right|+|3\mathcal{E}|+h-3,$$

ce qui, rapproché de (4.9), fournit

$$\left|\left(\frac{h(h+1)}{2}+\left\lceil\frac{h-1}{3}\right\rceil-3\right)\mathcal{E}\right|+|3\mathcal{E}|+h-3\geqslant n+h-1$$

et donc

$$\left|\left(\frac{h(h+1)}{2}+\left\lceil\frac{h-1}{3}\right\rceil-3\right)\mathcal{E}\right|+|3\mathcal{E}|\geqslant n+2.$$

L'application du corollaire 11 donne alors le résultat et clôt ce cas.

– Ou bien il existe une valeur de l'entier i (vérifiant $3 \leqslant i \leqslant h-1$) pour laquelle (4.11) n'est pas vraie :

$$|(c_2 + \ldots + c_i)\mathcal{E}| \leqslant |(c_2 + \ldots + c_{i-1})\mathcal{E}| + |c_i\mathcal{E}| - 2.$$

Dans ce cas, l'ensemble $(c_2 + \ldots + c_i)\mathcal{E}$ est dégénéré d'après le corollaire au théorème de Kneser et chacun de ses éléments admet au moins deux représentations d'après le théorème de Scherk. Il en sera de même pour les multiples suivants et en particulier pour $\left(\frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil\right)\mathcal{E}$. Cela clôt le cas $h \geqslant 4$.

Restent à traiter les cas $h \in \{2, 3\}$.

Si $h = 3$, on tire de (4.9)

$$(|\mathcal{E}| + |2\mathcal{E}|) + (|\mathcal{E}| + |3\mathcal{E}|) \geqslant n + 2$$

puis, grâce à deux applications de (4.7),

$$|3\mathcal{E}| + |4\mathcal{E}| \geqslant n + 2,$$

ce qui implique que $7\mathcal{E} = \mathbb{Z}/n\mathbb{Z}$ et que tout élément admet au moins deux représentations différentes, à nouveau d'après le corollaire 11, et clôt le cas $h = 3$.

Si $h = 2$, on tire de (4.8)

$$|\mathcal{E}| + |2\mathcal{E}| \geqslant n,$$

puis, par (4.6) et (4.7),

$$n - 2 \geqslant |3\mathcal{E}| \geqslant |\mathcal{E}| + |2\mathcal{E}| \geqslant n,$$

une contradiction qui clôt la preuve du lemme 24. □

Avant de passer au lemme suivant, qui est le résultat fondamental de cette partie, formulons une remarque essentielle pour la suite. Les deux premiers cas envisagés dans le lemme 24 ne nécessiteraient qu'un coefficient de $\mathcal{E}$ dans la conclusion égal à $h(h+1)/2+1$. Par ailleurs, l'étape limitante du lemme précédent est le cas où $\mathcal{E}$ est vospérien et de cardinal 3.

Passons maintenant au résultat fondamental de cette partie.

LEMME 25. — *Soient h et n deux entiers strictement positifs. Soit $\mathcal{E}$ un sous-ensemble foncièrement générateur de $\mathbb{Z}/n\mathbb{Z}$ tel que*

$$\mathcal{E} \cup 2\mathcal{E} \cup \ldots \cup h\mathcal{E} = \mathbb{Z}/n\mathbb{Z}.$$

Dans ces conditions, $\left(\frac{h(h+1)}{2} + \lceil \frac{h-1}{3} \rceil\right)\mathcal{E}$ est dégénéré.

Démonstration. — Si $h = 1$ le résultat est immédiat. Nous supposerons par la suite

$$h \geqslant 2.$$

On peut également supposer que $|\mathcal{E}| \leqslant n/2$, que $\mathcal{E}$ n'est pas une progression arithmétique dans $\mathbb{Z}/n\mathbb{Z}$ (en particulier $|\mathcal{E}| \geqslant 3$) et que $\mathcal{E}$ n'est pas vospérien. En effet, si l'une de ces trois conditions n'était pas remplie, les hypothèses du lemme permettraient d'appliquer le lemme précédent 24 et de conclure tout de suite que la somme $\left(\frac{h(h+1)}{2} + \lceil \frac{h-1}{3} \rceil\right)\mathcal{E}$ est dégénérée.

Ainsi, puisque $\mathcal{E}$ n'est pas vospérien, il existe un certain sous-ensemble $\mathcal{E}'$ de $\mathbb{Z}/n\mathbb{Z}$ vérifiant $|\mathcal{E}'| \geqslant 2$ et

$$|\mathcal{E} + \mathcal{E}'| \leqslant \min(|\mathcal{E}| + |\mathcal{E}'| - 1, n-2). \tag{4.12}$$

Soit e un élément arbitraire de $\mathcal{E}$, considérons $\mathcal{S}$ le translaté $\mathcal{E} - e = \{x - e \text{ pour } x \in \mathcal{E}\}$ de sorte que $0 \in \mathcal{S}$ et que $|\mathcal{S}| \geqslant 2$. Par (4.12), il vient

$$|\mathcal{S} + \mathcal{E}'| = |\mathcal{E} + \mathcal{E}'| \leqslant \min(|\mathcal{E}| + |\mathcal{E}'| - 1, n-2) = \min(|\mathcal{S}| + |\mathcal{E}'| - 1, n-2).$$

Cela montre que $\mathcal{S}$ est 2-séparable et que

$$\kappa_2(\mathbb{Z}/n\mathbb{Z}, \mathcal{S}) \leqslant |\mathcal{S}| - 1. \tag{4.13}$$

Également, pour toute valeur de l'entier s, on a $s\mathcal{S} = s\mathcal{E} - se$; de sorte que, puisque $\mathcal{E}$ est foncièrement générateur, $\mathcal{S}$ l'est aussi.

Ainsi $\mathcal{S}$ contient 0 et est 2-séparable et générateur. Cet ensemble vérifie aussi (4.13) et $|\mathcal{S}| \leqslant n/2$. Comme $\mathcal{S}$ n'est pas une progression

arithmétique, l'application du théorème 12 montre que $\mathcal{S}$ admet un sous-groupe, que l'on désignera par la lettre H, comme ensemble 2-critique (en particulier, le groupe H n'est ni réduit à $\{0\}$ ni égal à $\mathbb{Z}/n\mathbb{Z}$ tout entier) tel que $\overline{\mathcal{S}} = \mathcal{S}/H$ est soit une progression arithmétique, soit un ensemble vospérien dans $(\mathbb{Z}/n\mathbb{Z})/H$. Notons aussi, avant de poursuivre, que $\overline{\mathcal{E}} = \mathcal{E}/H$ étant un translaté de $\overline{\mathcal{S}}$, il en est de même pour lui car la qualité de progression arithmétique et la vospérianité sont conservées par translation.

On a, d'après (4.13),

$$|\mathcal{S} + H| - |H| \leqslant |\mathcal{S}| - 1. \tag{4.14}$$

Prenons un H-pavage de $\mathcal{S}$, c'est-à-dire une partition de $\mathcal{S}$ selon la classe modulo H :

$$\mathcal{S} = \mathcal{S}_1 \cup \cdots \cup \mathcal{S}_u$$

où u compte le nombre de classes modulo H rencontrées par $\mathcal{S}$ et vérifie par conséquent $u \geqslant 2$. En effet, puisque $\mathcal{S}$ est foncièrement générateur de $\mathbb{Z}/n\mathbb{Z}$, l'ensemble $\overline{\mathcal{S}}$ est foncièrement générateur de $(\mathbb{Z}/n\mathbb{Z})/H$ de sorte que, si u valait 1, tout multiple de $\mathcal{S}$ serait inclus dans une seule classe modulo H, ce qui imposerait $H = \mathbb{Z}/n\mathbb{Z}$, une contradiction à la qualité d'ensemble 2-critique (pour $\mathcal{S}$) de H.

On a évidemment

$$|\mathcal{S} + H| = u|H|.$$

On supposera, ce qui est licite et ne porte aucunement préjudice à la généralité de l'argument, que

$$|\mathcal{S}_1| \geqslant \ldots \geqslant |\mathcal{S}_{u-1}| \geqslant |\mathcal{S}_u|.$$

Observons maintenant que pour tout couple d'indices (i, j), sauf peut-être pour le couple $(i, j) = (u, u)$, on a

$$|\mathcal{S}_i| + |\mathcal{S}_j| \geqslant |H| + 1, \tag{4.15}$$

puisque (4.14) est équivalente à

$$\sum_{i=1}^{u} |\mathcal{S}_i| \geqslant (u-1)|H| + 1.$$

Le lemme préhistorique joint à (4.15) montre alors que $\mathcal{S}_i + \mathcal{S}_j$ est une classe (complète) modulo H. Cela prouve que $2\mathcal{S}$ est la réunion de classes modulo H et de l'ensemble $2\mathcal{S}_u$ (qui est peut-être aussi une classe complète modulo H). Plus généralement, pour tout entier $i \geqslant 2$, $i\mathcal{S}$ est la réunion de classes modulo H et de $i\mathcal{S}_u$. Par translation, il en est de même pour $i\mathcal{E}$. Ainsi, si l'on note $\mathcal{E}_u = e + \mathcal{S}_u$, on peut écrire en particulier

$$\left(\frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil\right)\mathcal{E} = \left(\bigcup_{j=1}^{k}(a_j + H)\right) \cup \left(\frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil\right)\mathcal{E}_u,$$

où les a_j sont des représentants des différentes classes modulo H (sauf peut-être une, à savoir celle de $\left(\frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil\right)\mathcal{E}_u$) rencontrées par la somme multiple $\left(\frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil\right)\mathcal{E}$. Définissons a_0 comme un représentant de la classe modulo H dans laquelle se trouve $\left(\frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil\right)\mathcal{E}_u$ et notons bien qu'il n'est pas exclu que l'élément a_0 tombe dans l'un des $a_j + H$ $(1 \leqslant j \leqslant k)$. C'est d'ailleurs ce que nous allons montrer dans un instant. Ce résultat impliquera l'égalité

$$\left(\frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil\right)\mathcal{E} = \bigcup_{j=1}^{k}(a_j + H),$$

qui montre immédiatement que $\left(\frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil\right)\mathcal{E}$ est un ensemble dégénéré.

Il ne nous reste donc plus qu'à montrer qu'a_0 tombe dans l'un des $a_j + H$ $(1 \leqslant j \leqslant k)$. Pour ce faire, observons que l'ensemble $\overline{\mathcal{E}} \subset (\mathbb{Z}/n\mathbb{Z})/H$ (qui est bien un groupe cyclique) est foncièrement générateur et qu'il vérifie également, par simple projection,

$$\overline{\mathcal{E}} \cup 2\overline{\mathcal{E}} \cup \cdots \cup h\overline{\mathcal{E}} = (\mathbb{Z}/n\mathbb{Z})/H. \tag{4.16}$$

Comme $\overline{\mathcal{E}}$ est bien soit une progression arithmétique, soit un ensemble vospérien et que $|(\mathbb{Z}/n\mathbb{Z})/H| \geqslant 2$ (car H est 2-critique), on peut appliquer le lemme 24 qui montre alors que $\left(\frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil\right)\overline{\mathcal{E}}$ est un ensemble dégénéré de $(\mathbb{Z}/n\mathbb{Z})/H$ dont tout élément admet au moins deux représentations différentes (sauf dans le cas où $h = 2$, $(\mathbb{Z}/n\mathbb{Z})/H \simeq \mathbb{Z}/5\mathbb{Z}$ et $\overline{\mathcal{E}} = d.\{2,3\}$ avec d un inversible modulo 5 ou dans le cas où $h = 3$, $(\mathbb{Z}/n\mathbb{Z})/H \simeq \mathbb{Z}/8\mathbb{Z}$ et $\overline{\mathcal{E}} = d.\{2,3\}$ avec d un inversible modulo 8 – cas

exclus jusqu'à la fin de ce paragraphe). C'est surtout la seconde partie de cette conclusion qui nous intéresse. En effet, elle nous apprend que l'élément $\left(\frac{h(h+1)}{2}+\left\lceil\frac{h-1}{3}\right\rceil\right)(\mathcal{E}_u/H)$ de $(\mathbb{Z}/n\mathbb{Z})/H$ peut s'écrire de deux façons distinctes (et en particulier, d'une *autre* façon) comme élément de $\left(\frac{h(h+1)}{2}+\left\lceil\frac{h-1}{3}\right\rceil\right)\overline{\mathcal{E}}$, ce qui signifie exactement que l'élément a_0 tombe dans l'un des a_j+H $(1\leqslant j\leqslant k)$.

Restent encore deux cas à envisager.

Si $h=2$, $(\mathbb{Z}/n\mathbb{Z})/H\simeq\mathbb{Z}/5\mathbb{Z}$ et $\overline{\mathcal{E}}=\{2,3\}$ (la multiplication par un inversible ne change rien), on observe que $\overline{\mathcal{E}}$ et $2\overline{\mathcal{E}}$ sont disjoints dans $(\mathbb{Z}/n\mathbb{Z})/H$. La relation $\mathcal{E}\cup 2\mathcal{E}=\mathbb{Z}/n\mathbb{Z}$ montre alors que les classes modulo H dans $\mathcal{E}$ sont complètes. Cela impose en particulier, et revenant à nos notations précédentes, que $\mathcal{E}_u$ puis $\left(\frac{h(h+1)}{2}+\left\lceil\frac{h-1}{3}\right\rceil\right)\mathcal{E}_u$ soit elle aussi une classe complète.

Si $h=3$, $(\mathbb{Z}/n\mathbb{Z})/H\simeq\mathbb{Z}/8\mathbb{Z}$ et $\overline{\mathcal{E}}=\{2,3\}$, on a $2\overline{\mathcal{E}}=\{4,5,6\}$ et $3\overline{\mathcal{E}}=\{6,7,0,1\}$. Puisque 2 et 3 n'ont qu'un représentant dans la réunion $\overline{\mathcal{E}}\cup 2\overline{\mathcal{E}}\cup 3\overline{\mathcal{E}}$, les classes correspondantes sont complètes et à nouveau $\left(\frac{h(h+1)}{2}+\left\lceil\frac{h-1}{3}\right\rceil\right)\mathcal{E}_u$ doit être elle aussi une classe complète.

Le lemme est prouvé. □

Une fois le lemme 25 acquis, on peut démontrer à peu de frais le théorème 3 énoncé dans l'introduction, un résultat qui stipule que l'hypothèse de foncière génération imposée à $\mathcal{E}$ dans le lemme 25 peut être affaiblie en $|\mathcal{E}|\geqslant 2$.

Démonstration du théorème 3.— Le cas $h=1$ étant évident, on supposera $h\geqslant 2$.

Soit e un élément quelconque de $\mathcal{E}$ et H le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par $\mathcal{E}-e$. Remarquons au passage que ce sous-groupe ne dépend pas du choix de e (car pour un autre élément e' de $\mathcal{E}$, $e'-e$ appartient à H et l'on a $\mathcal{E}-e'=\mathcal{E}-e+(e-e')\subset H+(e-e')=H$).

La définition de H entraîne en particulier que $\mathcal{E}\subset e+H$ ($\mathcal{E}$ est contenu dans une unique classe modulo H).

Puisque $0\in\mathcal{E}-e$, la définition de H montre qu'il existe un entier k_0 tel que $k_0(\mathcal{E}-e)=H$. Pour tout entier $k\geqslant k_0$, on a alors $k\mathcal{E}=ke+H$.

En particulier, notant l l'ordre de la projection de l'élément e dans le groupe quotient $(\mathbb{Z}/n\mathbb{Z})/H$, on a pour tout entier j, $jl\mathcal{E}\subset H$ et, pour

tout entier $j \geqslant k_0/l$, $jl\mathcal{E} = H$. Ainsi l'ensemble $\mathcal{F} = l\mathcal{E}$ est foncièrement générateur (de H).

De plus, la relation

$$\mathcal{E} \cup 2\mathcal{E} \cup \ldots \cup h\mathcal{E} = \mathbb{Z}/n\mathbb{Z}, \tag{4.17}$$

une fois quotientée par H, entraîne que la classe de e engendre $(\mathbb{Z}/n\mathbb{Z})/H$ et que

$$l \leqslant h.$$

Par ailleurs, (4.17) implique

$$\mathcal{F} \cup 2\mathcal{F} \cup \ldots \cup \left[\frac{h}{l}\right]\mathcal{F} = H.$$

Le groupe H étant lui-même cyclique, on peut appliquer le lemme 25 à $\mathcal{F}$ et H. On en déduit que

$$\left(\frac{[h/l]([h/l]+1)}{2} + \left\lceil\frac{[h/l]-1}{3}\right\rceil\right)\mathcal{F} = \left(\frac{[h/l]([h/l]+1)}{2} + \left\lceil\frac{[h/l]-1}{3}\right\rceil\right)l\mathcal{E}$$

est dégénéré (dans H donc dans $\mathbb{Z}/n\mathbb{Z}$). Ne reste plus alors qu'à établir l'inégalité

$$\left(\frac{[h/l]([h/l]+1)}{2} + \left\lceil\frac{[h/l]-1}{3}\right\rceil\right)l \leqslant \frac{h(h+1)}{2} + \left\lceil\frac{h-1}{3}\right\rceil, \tag{4.18}$$

ce qui établira que $\left(\frac{h(h+1)}{2} + \left\lceil\frac{h-1}{3}\right\rceil\right)\mathcal{E}$ est bien dégénéré.

On se convainc immédiatement que cette inégalité est toujours vérifiée dans les deux cas suivants : $l = 1$ ou $h = 2$ (auquel cas l ne peut valoir que 1 ou 2).

On supposera donc dorénavant $l \geqslant 2$ et $h \geqslant 3$. On calcule alors que

$$\begin{aligned}
&\frac{h(h+1)}{2} + \left\lceil\frac{h-1}{3}\right\rceil - \left(\frac{[h/l]([h/l]+1)}{2} + \left\lceil\frac{[h/l]-1}{3}\right\rceil\right)l \\
&\geqslant \frac{h(h+1)}{2} + \frac{h-1}{3} - \frac{h(h/l+1)}{2} - \left(\frac{h/l-1}{3}+1\right)l \\
&= \left(1-\frac{1}{l}\right)\frac{h^2}{2} - \frac{2l+1}{3} \\
&= \frac{1}{2}\left(1-\frac{1}{l}\right)\left(h^2 - \frac{2l(2l+1)}{3(l-1)}\right).
\end{aligned}$$

Or, la fraction de l apparaissant dans la seconde parenthèse est maximale en $l = 2$ ou $l = h$. Dans les deux cas, on vérifie que cette parenthèse reste toujours positive (pour $h \geqslant 3$), ce qui achève la preuve de la validité de l'inégalité (4.18) et donc du théorème 3. □

5. Preuve du théorème 1.

5.1. La borne inférieure.

Elle résulte immédiatement du théorème 20, de la minoration $K(h) \geqslant K_2(h, 2)$ et du lemme suivant.

LEMME 26. — *Pour tout entier strictement positif h, on a*

$$X(h) \geqslant K(h).$$

Démonstration. — En effet, pour un entier positif h donné, considérons un entier g et un sous-ensemble $\mathcal{A}$ foncièrement générateur de $\mathbb{Z}/g\mathbb{Z}$ tel que

$$\mathcal{A} \cup 2\mathcal{A} \cup \ldots \cup h\mathcal{A} = \mathbb{Z}/g\mathbb{Z}, \tag{5.1}$$

et

$$(K(h) - 1)\mathcal{A} \neq \mathbb{Z}/g\mathbb{Z}. \tag{5.2}$$

Soit maintenant $\mathcal{B}$ l'ensemble

$$\mathcal{B} = \{0\} \cup \bigcup_{a \in \mathcal{A}} \{a, a + g, a + 2g, \ldots\} = \{0\} \cup \big(\mathcal{A} + g.\mathbb{N}\big).$$

Par la propriété (5.1), l'ensemble $\mathcal{B}$ est une base d'ordre au plus h. Par la propriété (5.2) et le fait que $K(h)\mathcal{A} = \mathbb{Z}/g\mathbb{Z}$, l'ensemble $\mathcal{B} \setminus \{0\}$ est une base d'ordre fini égal à $K(h)$. □

5.2. La borne supérieure.

La partie essentielle de cette démonstration est concentrée dans le lemme suivant.

LEMME 27. — *Soient l et h deux entiers satisfaisant $l \geqslant 1$ et $h \geqslant 2$. Soit $\mathcal{A}$ une base d'ordre h. On suppose que $0 \in \mathcal{A}^*$ et on pose $\mathcal{B} = \mathcal{A} \setminus \{0\}$. L'ensemble*

$$\left(\frac{h(h+1)}{2} + l\right)\mathcal{B}$$

coïncide, pour un certain entier g et à un nombre fini d'éléments près, avec la réunion de progressions arithmétiques de raison g :

$$\left(\frac{h(h+1)}{2} + l\right)\mathcal{B} + g.\mathbb{N}.$$

Une fois ce lemme obtenu, on conclura la preuve de la borne supérieure de la façon suivante. Soit h un entier supérieur ou égal à deux quelconque (le cas $h = 1$ est sans intérêt). Soient $\mathcal{A}$ une base d'ordre h quelconque, a un élément de $\mathcal{A}^*$ et $\mathcal{B} = \mathcal{A} \setminus \{a\}$. Quitte à translater $\mathcal{A}$, on peut sans restriction supposer que $a = 0$. En décomposant $h\mathcal{A} \sim \mathbb{N}$, on trouve

$$h\mathcal{B} \cup (h-1)\mathcal{B} \cup \ldots \cup \mathcal{B} \sim \mathbb{N}. \tag{5.3}$$

D'après le lemme 27 appliqué avec $l = \left\lceil \frac{h-1}{3} \right\rceil \geqslant 1$, on a

$$\left(\frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil\right)\mathcal{B} \sim \left(\left(\frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil\right)\overline{\mathcal{B}}\right) + g.\mathbb{N}, \tag{5.4}$$

où l'on a noté g la raison commune aux progressions arithmétiques apparaissant dans l'énoncé du lemme et $\overline{\mathcal{B}}$ la projection de $\mathcal{B}$ sur $\mathbb{Z}/g\mathbb{Z}$. Dans cette relation, nous prenons soin de choisir g *minimum* avec cette propriété.

Nous allons montrer que $g = 1$ (ce qui finira la preuve du théorème par (5.4)) en procédant par l'absurde. Supposons que g vaille au moins deux. Puisque $\mathcal{B}$ est une base, sa projection sur $\mathbb{Z}/g\mathbb{Z}$ est foncièrement génératrice : en effet, on a, pour un certain entier l,

$$\mathbb{N} \sim l\mathcal{B} \subset l\overline{\mathcal{B}} + g.\mathbb{N}$$

de sorte que $l\overline{\mathcal{B}}$ doit contenir toutes les classes modulo g.

Par ailleurs, de l'équation (5.3), on tire immédiatement que

$$\overline{\mathcal{B}} \cup 2\overline{\mathcal{B}} \cup \ldots \cup h\overline{\mathcal{B}} = \mathbb{Z}/g\mathbb{Z}.$$

On peut donc appliquer le lemme-clef de la partie 4 (lemme 25), qui montre que $\left(\frac{h(h+1)}{2} + \lceil \frac{h-1}{3} \rceil\right) \overline{\mathcal{B}}$ est dégénéré. Mais la minimalité de g implique que $\left(\frac{h(h+1)}{2} + \lceil \frac{h-1}{3} \rceil\right) \overline{\mathcal{B}}$ est non dégénéré (sans quoi on pourrait diminuer la valeur de g, contredisant sa minimalité). On aboutit donc à une contradiction montrant que $g = 1$ et le théorème est prouvé.

Finalement, il ne reste plus à prouver que le lemme 27.

Démonstration du lemme 27. — Comme en (5.3), on a

$$h\mathcal{B} \cup (h-1)\mathcal{B} \cup \ldots \cup \mathcal{B} \sim \mathbb{N}. \tag{5.5}$$

Pour tout entier i, on note ci-dessous B_i la fonction de comptage de $i\mathcal{B}$. On notera également $b_0 = \min\{b \in \mathcal{B},\ b > 0\}$. Du fait que chaque $i\mathcal{B}$ $(i \geqslant 2)$ contient $(i-1)\mathcal{B} + b_0$, on a

$$B_i(n) \geqslant B_{i-1}(n - b_0) \geqslant B_{i-1}(n) - b_0. \tag{5.6}$$

En particulier, la suite $\underline{d}(i\mathcal{B})$ est croissante. De l'équation (5.5), on tire que

$$S(n) = B_h(n) + B_{h-1}(n) + \cdots + B_1(n) \geqslant n - c, \tag{5.7}$$

où c est un entier à partir duquel tout entier est dans la réunion figurant dans le membre de gauche de (5.5). Il en résulte alors, avec (5.6), que $\underline{d}(h\mathcal{B}) \geqslant 1/h > 0$. Nous pouvons ainsi définir sans ambiguïté la quantité

$$j = \min\{k \in \mathbb{N} \text{ tel que } \underline{d}(k\mathcal{B}) > 0\}$$

qui vérifie $j \leqslant h$.

Si l'on note

$$\alpha = \liminf_{n \to +\infty} \frac{S(n)}{n},$$

on tire de (5.7) l'inégalité $\alpha \geqslant 1$.

On peut supposer que l'on a $\alpha = 1$ et $\underline{d}\mathcal{B} = 0$ (i.e. $j \geqslant 2$). En effet, dans le cas contraire, on a $\alpha + l\underline{d}\mathcal{B} > 1$, d'où il vient

$$\liminf_{n \to +\infty} \frac{S(n) + lB_1(n)}{n} \geqslant \liminf_{n \to +\infty} \frac{S(n)}{n} + l\underline{d}\mathcal{B} = \alpha + l\underline{d}\mathcal{B} > 1,$$

et le corollaire 5 implique alors que

$$(1+2+\cdots+h+l)\,\mathcal{B} = \left(\frac{h(h+1)}{2}+l\right)\mathcal{B}$$

vérifie la conclusion du lemme.

On pose maintenant

$$\begin{aligned} R(n) &= S(n) + B_j(n) - B_{j-1}(n) \\ &= B_1(n) + B_2(n) + \cdots + B_{j-2}(n) + 2B_j(n) + B_{j+1}(n) + \cdots + B_h(n). \end{aligned}$$

Si $\liminf_{n\to+\infty} R(n)/n > 1$, on conclut comme précédemment (via la fonction $R(n)+(l-1)B_1(n) \geqslant R(n)$) en notant que $(1+2+\cdots+(j-2)+2j+(j+1)+\cdots+h)+l-1$ vaut $h(h+1)/2+l$. De l'inégalité immédiate par (5.6)

$$R(n) \geqslant S(n) - b_0, \tag{5.8}$$

on peut tirer $\liminf_{n\to+\infty} R(n)/n \geqslant \liminf_{n\to+\infty} S(n)/n = \alpha = 1$. On pourra donc désormais supposer que

$$\liminf_{n\to+\infty} \frac{R(n)}{n} = 1. \tag{5.9}$$

Choisissons alors une suite strictement croissante d'entiers $(n_i)_{i\in\mathbb{N}}$ telle que

$$\lim_{i\to+\infty} \frac{R(n_i)}{n_i} = 1.$$

En utilisant l'égalité $\alpha = 1$ et (5.8), cela implique que l'on a également

$$\lim_{i\to+\infty} \frac{S(n_i)}{n_i} = 1 \tag{5.10}$$

et donc par définition que

$$\lim_{i\to+\infty} \frac{B_j(n_i) - B_{j-1}(n_i)}{n_i} = 0.$$

Comme $B_j(n_i)/n_i \gtrsim \underline{d}(j\mathcal{B}) > 0$, on en déduit que

$$\lim_{i\to+\infty} \frac{B_j(n_i)}{B_{j-1}(n_i)} = 1. \tag{5.11}$$

Puisque $0 \in \mathcal{A}^*$, l'ensemble $\mathcal{B}$ est une base, ce qui impose que pgcd $\{b - b' \text{ où } b, b' \in \mathcal{B}\} = 1$ (sinon les éléments de $\mathcal{B}$ auraient tous la même valeur modulo ce plus grand commun diviseur et il en serait de même pour les éléments de $k\mathcal{B}$, quel que soit l'entier k, ce qui empêcherait $\mathcal{B}$ d'être une base). Par suite, il existe, par le théorème de Bachet-Bezout, un entier s et des entiers $u_1, u_2, \ldots, u_s$ (tous strictement positifs) ainsi que des éléments $b_1, b_1', b_2, b_2', \ldots, b_s, b_s' \in \mathcal{B}$ tels que

$$u_1(b_1 - b_1') + u_2(b_2 - b_2') + \cdots + u_s(b_s - b_s') = 1. \tag{5.12}$$

On notera $b_\infty = \max_{1 \leqslant i \leqslant s}\{b_i, b_i'\}$, $\delta_k = b_k - b_k'$ et

$$\mathcal{B}_0 = \mathcal{B} \cap \{1, \ldots, b_\infty\}.$$

Choisissons maintenant

$$\epsilon = \frac{1}{6b_0 \sum_{k=1}^{s} u_k}$$

qui vérifie $0 < \epsilon < 1$. Pour i assez grand, disons $i \geqslant i_0$, on a d'après (5.11)

$$B_j(n_i) \leqslant (1 + \epsilon) B_{j-1}(n_i), \tag{5.13}$$

$$B_{j-1}(n_i - b_\infty) \geqslant B_{j-1}(n_i) - b_\infty \geqslant \frac{3}{4} B_j(n_i) - b_\infty \geqslant \frac{1}{2} \underline{\mathrm{d}}(j\mathcal{B}) n_i \tag{5.14}$$

(puisque $B_j(n_i) \gtrsim \underline{\mathrm{d}}(j\mathcal{B}) n_i$) et

$$B_{j-1}(n_i) \leqslant (1 + \epsilon)(B_{j-1}(n_i) - b_\infty) \leqslant (1 + \epsilon) B_{j-1}(n_i - b_\infty). \tag{5.15}$$

Pour $i \geqslant i_0$, posons

$$\mathcal{C}_i = \big((j-1)\mathcal{B}\big) \cap \{1, \ldots, n_i - b_\infty\}.$$

Comme $(j\mathcal{B}) \cap \{1, \ldots, n_i\} \supset \mathcal{C}_i + \mathcal{B}_0$, on en déduit, avec (5.13) et (5.15), que

$$\begin{aligned} |\mathcal{C}_i + \mathcal{B}_0| \leqslant B_j(n_i) &\leqslant (1 + \epsilon) B_{j-1}(n_i) \leqslant (1 + \epsilon)^2 B_{j-1}(n_i - b_\infty) \\ &\leqslant (1 + 3\epsilon) B_{j-1}(n_i - b_\infty). \end{aligned}$$

En particulier

$$|\mathcal{C}_i + \{b_1, b_1', b_2, b_2', \dots, b_s, b_s'\}| \leqslant (1+3\epsilon)|\mathcal{C}_i|.$$

Le principe d'inclusion-exclusion montre alors que, pour tout entier k entre 1 et s, on dispose de la minoration

$$|(b_k + \mathcal{C}_i) \cap (b_k' + \mathcal{C}_i)| \geqslant (1-3\epsilon)|\mathcal{C}_i|$$

ou encore, par translation,

$$|(\delta_k + \mathcal{C}_i) \cap \mathcal{C}_i| \geqslant (1-3\epsilon)|\mathcal{C}_i|.$$

D'une nouvelle translation, on déduit que

$$|(2\delta_k + \mathcal{C}_i) \cap (\delta_k + \mathcal{C}_i)| \geqslant (1-3\epsilon)|\mathcal{C}_i|,$$

puis, d'une nouvelle application du principe d'inclusion-exclusion aux deux dernières inégalités obtenues,

$$\begin{aligned}
|(2\delta_k + \mathcal{C}_i) \cap \mathcal{C}_i| &\geqslant |(2\delta_k + \mathcal{C}_i) \cap (\delta_k + \mathcal{C}_i) \cap \mathcal{C}_i| \\
&= \big|\big((2\delta_k + \mathcal{C}_i) \cap (\delta_k + \mathcal{C}_i)\big) \cap \big((\delta_k + \mathcal{C}_i) \cap \mathcal{C}_i\big)\big| \\
&= |(2\delta_k + \mathcal{C}_i) \cap (\delta_k + \mathcal{C}_i)| + |(\delta_k + \mathcal{C}_i) \cap \mathcal{C}_i| \\
&\qquad - \big|\big((2\delta_k + \mathcal{C}_i) \cap (\delta_k + \mathcal{C}_i)\big) \cup \big((\delta_k + \mathcal{C}_i) \cap \mathcal{C}_i\big)\big| \\
&\geqslant |(2\delta_k + \mathcal{C}_i) \cap (\delta_k + \mathcal{C}_i)| + |(\delta_k + \mathcal{C}_i) \cap \mathcal{C}_i| - |\delta_k + \mathcal{C}_i| \\
&\geqslant (1-3\epsilon)|\mathcal{C}_i| + (1-3\epsilon)|\mathcal{C}_i| - |\mathcal{C}_i| = (1-6\epsilon)|\mathcal{C}_i|,
\end{aligned}$$

et, par récurrence,

$$|(u_k\delta_k + \mathcal{C}_i) \cap \mathcal{C}_i| \geqslant (1-3\epsilon u_k)|\mathcal{C}_i|.$$

Enfin, par la même méthode, on montre que

$$\left|\left(\sum_{k=1}^{s} u_k\delta_k + \mathcal{C}_i\right) \cap \mathcal{C}_i\right| \geqslant \left(1 - 3\epsilon\sum_{k=1}^{s} u_k\right)|\mathcal{C}_i|,$$

ou, plus simplement d'après la relation (5.12) et la définition d'ϵ,

$$|(1 + \mathcal{C}_i) \cap \mathcal{C}_i| \geqslant \left(1 - \frac{1}{2b_0}\right)|\mathcal{C}_i|.$$

De là (à nouveau par la même méthode)

$$|(b_0 + \mathcal{C}_i) \cap \mathcal{C}_i| \geqslant \frac{1}{2}|\mathcal{C}_i|.$$

Finalement, comme $b_0 \in \mathcal{B}_0$, on trouve que

$$|(\mathcal{B}_0 + \mathcal{C}_i) \cap \mathcal{C}_i| \geqslant |(b_0 + \mathcal{C}_i) \cap \mathcal{C}_i| \geqslant \frac{1}{2}|\mathcal{C}_i| = \frac{1}{2}B_{j-1}(n_i - b_\infty) \geqslant \frac{1}{4}\underline{\mathrm{d}}(j\mathcal{B})n_i,$$

d'après (5.14). Revenant à nos notations d'origine, cette inégalité implique que

$$\big|\big(j\mathcal{B}\big) \cap \big((j-1)\mathcal{B}\big) \cap \{1, \ldots, n_i\}\big| \geqslant \frac{1}{4}\underline{\mathrm{d}}(j\mathcal{B})n_i\,;$$

autrement dit, entre 1 et n_i, une proportion positive des entiers appartient à l'intersection $\big(j\mathcal{B}\big) \cap \big((j-1)\mathcal{B}\big)$. En utilisant (5.5), il vient alors

$$S(n_i) \geqslant n_i - c + \frac{1}{4}\underline{\mathrm{d}}(j\mathcal{B})n_i$$

ce qui induit une contradiction au regard de (5.10) puisque $\underline{\mathrm{d}}(j\mathcal{B}) > 0$. □

5.3. Amélioration de la borne supérieure.

Le but de ce chapitre est l'obtention des inégalités (1.7). L'amélioration en question repose sur la remarque qui a été faite après la preuve du lemme 24.

Soit $h \geqslant 4$ un entier fixé. Il est bien clair que l'étape limitante dans la majoration de $X(h)$ par $\frac{h(h+1)}{2} + \lceil \frac{h-1}{3} \rceil$ n'est ni la preuve du théorème proprement dite (chapitre 5.2) – en particulier, pas le lemme 27 – ni la preuve du lemme 25 mais seulement le lemme 24 et encore uniquement dans le cas (iii). Ainsi toute amélioration du coefficient $\frac{h(h+1)}{2} + \lceil \frac{h-1}{3} \rceil$ dans le (iii) de ce lemme en un coefficient de la forme $\frac{h(h+1)}{2} + l$ avec $l \geqslant 1$ implique immédiatement la borne $X(h) \leqslant \frac{h(h+1)}{2} + l$.

Or, il est naturel de conjecturer ceci :

CONJECTURE 28. — *Soient $h, n \geqslant 3$ deux entiers. Soit $\mathcal{E}$ un sous-ensemble foncièrement générateur et vospérien de $\mathbb{Z}/n\mathbb{Z}$, de cardinal au moins égal à 3, tel que*

$$\mathcal{E} \cup 2\mathcal{E} \cup \ldots \cup h\mathcal{E} = \mathbb{Z}/n\mathbb{Z}.$$

Dans ces conditions, l'ensemble $\left(\frac{h(h+1)}{2}+1\right)\mathcal{E}$ *est un ensemble dégénéré dont tout élément admet au moins deux représentations différentes.*

D'après ce qu'on vient de dire, cette conjecture impliquerait alors la conjecture 2.

Nous allons prouver la conjecture 28 dans les cas $h = 5$ et 6 (elle est vraie pour $h = 3$ et 4, d'après le lemme 24). Ce résultat impliquera alors les inégalités (1.7). Pour ce faire, on va démontrer d'abord le résultat suivant.

LEMME 29. — *Soient h et n deux entiers vérifiant $h \geqslant 5$ et $n \geqslant 3$. Soit $\mathcal{E}$ un sous-ensemble foncièrement générateur et vospérien de $\mathbb{Z}/n\mathbb{Z}$, de cardinal au moins égal à 3, tel que*

$$\mathcal{E} \cup 2\mathcal{E} \cup \ldots \cup h\mathcal{E} = \mathbb{Z}/n\mathbb{Z}.$$

Supposons que pour tout entier $c \in \{3, \ldots, h-2\}$, on ait $M_2(h,c) \geqslant h-1-c$, alors l'ensemble $\left(\frac{h(h+1)}{2}+1\right)\mathcal{E}$ *est un ensemble dégénéré dont tout élément admet au moins deux représentations différentes.*

Cette preuve étant une modification du cas (iii) de celle du lemme 24, on fera référence à celle-ci dans ce qui suit.

Démonstration. — Soit $\mathcal{E} \subset \mathbb{Z}/n\mathbb{Z}$, foncièrement générateur, vospérien et de cardinal au moins égal à 3, tel que

$$\mathcal{E} \cup 2\mathcal{E} \cup \ldots \cup h\mathcal{E} = \mathbb{Z}/n\mathbb{Z}. \tag{5.16}$$

On va supposer que

$$\left|\frac{h(h+1)}{2}\mathcal{E}\right| \leqslant n-2,$$

sans quoi la conclusion est immédiate d'après le corollaire 11. On dispose donc de l'inégalité (4.7) pour tout $i \leqslant h(h+1)/2 - 1$.

Supposons d'abord que

$$|\mathcal{E}| \geqslant h-1.$$

De (4.8) (qui est évidemment encore valable), on tire

$$|\mathcal{E}| + \big(|\mathcal{E}| + |2\mathcal{E}| + \cdots + |h\mathcal{E}|\big) \geqslant |\mathcal{E}| + n \geqslant n + h - 1$$

puis, en appliquant la propriété de Vosper (4.7),

$$|3\mathcal{E}| + |4\mathcal{E}| + |4\mathcal{E}| + \cdots + |h\mathcal{E}| \geqslant n + h - 1.$$

Comme dans la preuve du lemme 24, on définit $c'_1 = 3$, $c'_2 = 4$, $c'_3 = 4$, $c'_4 = 5, \ldots,$ $c'_{h-1} = h$.

Maintenant, opérant comme à la fin de la preuve du lemme 24, on trouve que :

– soit une certaine somme du type $(c'_2 + \ldots + c'_i)\mathcal{E}$ est dégénérée d'après le théorème de Kneser et chacun de ses éléments admet au moins deux représentations d'après le théorème de Scherk. Comme $c'_2 + \ldots + c'_i \leqslant h(h+1)/2$, il en sera de même pour les multiples suivants et en particulier pour $\left(\frac{h(h+1)}{2} + 1\right)\mathcal{E}$,

– soit

$$|3\mathcal{E}| + \left|\left(\frac{h(h+1)}{2} - 2\right)\mathcal{E}\right| + h - 3 \geqslant n + h - 1,$$

c'est-à-dire

$$|3\mathcal{E}| + \left|\left(\frac{h(h+1)}{2} - 2\right)\mathcal{E}\right| \geqslant n + 2$$

et on peut conclure par l'application du corollaire 11 qui donne alors le résultat et clôt ce cas.

Supposons maintenant que

$$c = |\mathcal{E}| \leqslant h - 2.$$

Par hypothèse $c \geqslant 3$, et on peut améliorer (4.8) en utilisant ce que l'on sait sur le problème du recouvrement économique. De la relation (5.16) et de la définition de $M_2(h, c)$, on tire en effet

$$|\mathcal{E}| + |2\mathcal{E}| + \cdots + |h\mathcal{E}| \geqslant n + M_2(h, c).$$

Comme par hypothèse, pour $3 \leqslant c \leqslant h-2$, on a $M_2(h,c) \geqslant h-1-c$, il vient

$$|\mathcal{E}| + (|\mathcal{E}| + |2\mathcal{E}| + \cdots + |h\mathcal{E}|) \geqslant c + n + M_2(h,c) \geqslant n + h - 1,$$

et l'on finit comme ci-dessus. □

Comme les tables 2 et 3 nous montrent que, pour $h = 5$, on a

$$M_2(h,3) = M_2(5,3) = 7 \geqslant 1 = h-4 = h-1-3$$

et que, pour $h = 6$, on a

$$M_2(h,3) = M_2(6,3) = 11 \geqslant 2 = h-4 = h-1-3$$

et

$$M_2(h,4) = M_2(6,4) = 12 \geqslant 1 = h-5 = h-1-4,$$

on déduit du lemme 29 la validité de la conjecture 28 pour $h = 5$ et 6 et donc la validité des inégalités (1.7).

Remerciements. — Le théorème 3 fut suggéré à l'auteur par l'un des rapporteurs anonymes de cet article. Que celui-ci soit publiquement remercié.

BIBLIOGRAPHIE

[1] J. CASSAIGNE, A. PLAGNE, Grekos' S function has a linear growth, Proc. Amer. Math. Soc. 132 (2004), 2833-2840.

[2] A.-L. CAUCHY, Recherches sur les nombres, J. École Polytech. 9 (1813), 99-123.

[3] M. DELÉGLISE, Recouvrement optimal du cercle par les multiples d'un intervalle, Acta Arith. 59 (1991), 21-35.

[4] B. DESCHAMPS, G. GREKOS, Estimation du nombre d'exceptions à ce qu'un ensemble de base privé d'un point reste un ensemble de base, J. Reine Angew. Math. 539 (2001), 45-53.

[5] P. ERDŐS, R. L. GRAHAM, On bases with an exact order, Acta Arith. 37 (1980), 201-207.

[6] P. ERDŐS, R. L. GRAHAM, Old and new problems and results in combinatorial number theory, Monographies de l'Enseignement Mathématique 28, 1980.

[7] G. GREKOS, Sur l'ordre d'une base additive, Séminaire de théorie des nombres de Bordeaux, Année 1987/88, exposé 31.

[8] H. HALBERSTAM, K. ROTH, «Sequences», Oxford University Press, 1966.

[9] Y. ould HAMIDOUNE, An isoperimetric method in Additive Theory, J. Algebra 179 (1996), 622-630.

[10] Y. ould HAMIDOUNE, Subsets with small sums in Abelian groups I : the Vosper property, Europ. J. of Combinatorics 18 (1997), 541-556.

[11] Y. ould HAMIDOUNE, Some results in additive number theory I : The critical pair theory, Acta Arith. 96 (2001), 97-119.

[12] Y. ould HAMIDOUNE, A. PLAGNE, A generalization of Freiman's $3k-3$ theorem, Acta Arith. 103 (2002), 147-156.

[13] Y. ould HAMIDOUNE, A. PLAGNE, A critical pair theorem applied to sum-free sets in abelian groups, Comment. Math. Helv. 79 (2004), 183-207.

[14] G. H. HARDY, E. M. WRIGHT, «An introduction to the theory of numbers», 5th edition, Clarendon Press, Oxford University Press, 1979.

[15] J. H. B. KEMPERMAN, On complexes in a semi-group, Indag. Math. 18 (1956), 247-254.

[16] M. KNESER, Abschätzung der asymptotischen Dichte von Summenmengen, Math. Z. 58 (1953), 459-484.

[17] M. KNESER, Summenmengen in lokalkompakten abelschen Gruppen, Math. Z. 66 (1956), 88-110.

[18] H. B. MANN, «Addition theorems», Wiley-Interscience, 1965.

[19] M. B. NATHANSON, «Additive number theory. Inverse problems and the geometry of sumsets», GTM 165, Springer Verlag, 1996.

[20] J. C. M. NASH, Some applications of a theorem of M. Kneser, J. Number Theory 44 (1993), 1-8.

[21] A. PLAGNE, Removing one element from an exact additive basis, J. Number Theory 87 (2001), 306-314.

[22] P. SCHERK, Distinct elements in a set of sums (solution of a problem of Leo Moser), Amer. Math. Monthly 62 (1955), 46-47.

[23] V. T. SÓS, On the distribution mod 1 of the sequence $n\alpha$, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 1 (1958), 127-134.

[24] A. STÖHR, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe I, J. Reine Angew. Math. 194 (1955), 40-65.

[25] A. STÖHR, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe II, J. Reine Angew. Math. 194 (1955), 111-140.

[26] J. SURÁNYI, Über die Anordnung der Vielfachen einer reellen Zahl mod 1, Ann. Univ. Sci. Budapest Eötvös Sect. Math. 1 (1958), 107-111.

[27] S. ŚWIERCZKOWSKI, On successive settings of an arc on the circumference of a circle, Fund. Math. 46 (1959), 187-189.

[28] A. G. VOSPER, The critical pairs of subsets of a group of prime order, J. London Math. Soc. 31 (1956), 200-205.

[29] A. G. VOSPER, Addendum to «The critical pairs of subsets of a group of prime order», J. London Math. Soc. 31 (1956), 280-282.

Manuscrit reçu le 11 décembre 2002,
révisé le 20 mars 2003,
accepté le 19 septembre 2003.

Alain PLAGNE,
École polytechnique
Centre de Mathématiques Laurent Schwartz
UMR 7640 du CNRS
91128 Palaiseau Cedex, (France).

plagne@math.polytechnique.fr