90.01M

SESSION 2009

Filière MP

MATHÉMATIQUES MPI 1

Épreuve commune aux ENS de Paris, Lyon et Cachan

Durée : 6 heures

L'usage de calculatrice est interdit

Préambule

Le problème est consacré à quelques propriétés de nature combinatoire des groupes abéliens.

Soit G un groupe abélien et soit A une partie non vide de G ; on relie ainsi des propriétés atypiques des cardinaux des ensembles A, $A+A$, d'une part, notamment le fait que le cardinal de $A+A$ soit « petit » par rapport à celui de A et des propriétés algébriques de l'ensemble A, comme le fait d'être une progression arithmétique.

Le résultat principal du problème, le théorème de Freiman–Rusza–Chang, affirme que toute partie non vide A de $\mathbf{Z}$ est contenue dans une progression arithmétique de dimension et taille contrôlées en fonction du rapport $\sigma = \mathrm{Card}(A+A)/\mathrm{Card}(A)$. Il est démontré à la fin de la partie V.

La partie I développe quelques généralités sur les sommes d'ensembles. La démonstration du théorème de Freiman–Rusza–Chang utilise des arguments de nature arithmétique (valeurs aux vecteurs à coordonnées entières de formes quadratiques définies positives) qui font l'objet de la partie II et d'autres de nature analytique (séries de Fourier) qui sont développés dans la partie III.

Ces trois premières parties sont indépendantes l'une de l'autre.

Leurs arguments sont combinés dans la partie IV pour démontrer que l'ensemble $2A-2A$ *contient* une progression arithmétique de dimension et taille contrôlée en fonction de σ. Le théorème de Freiman–Rusza–Chang fait alors l'objet de la partie V et clôt le problème.

Notations

Les lettres **N**, $\mathbf{N}^*$, **Z**, **R** et **C** désignent respectivement l'ensemble des entiers naturels, celui des entiers naturels strictement positifs, l'anneau des entiers relatifs, le corps des nombres réels et le corps des nombres complexes. On note $\Re(z)$, $\Im(z)$ et $|z|$ la partie réelle, la partie imaginaire et le module d'un nombre complexe z.

La fonction log est la fonction logarithme népérien, réciproque de la fonction exponentielle. On désigne par cosh et sinh les fonctions « cosinus hyperbolique » et « sinus hyperbolique » ; elles sont définies pour tout nombre complexe z par les relations

$$\cosh(z) = \frac{1}{2}(e^z + e^{-z}) \quad \text{et} \quad \sinh(z) = \frac{1}{2}(e^z - e^{-z}).$$

Une partition d'un ensemble A est un ensemble de parties de A deux à deux disjointes dont la réunion est égale à A. Si A est un ensemble fini, on notera $\mathrm{Card}(A)$ son cardinal.

Si n est un entier naturel, $n!$ désigne le produit $1 \cdot 2 \cdots n$ de tous les entiers de 1 à n ; par convention, on pose $0! = 1$. Si n et p sont des entiers naturels, on note $\binom{n}{p}$ l'entier $n!/p!(n-p)!$ (coefficient binomial).

L'espace vectoriel $\mathbf{R}^n$ sera muni de la norme euclidienne standard telle que $\|\vec{x}\|^2 = x_1^2 + \cdots + x_n^2$ si $\vec{x} = (x_1, \ldots, x_n)$. La base canonique de cet espace est la famille $(\vec{e}_1, \ldots, \vec{e}_n)$ telle que $\vec{x} = x_1\vec{e}_1 + \cdots + x_n\vec{e}_n$ si $\vec{x} = (x_1, \ldots, x_n)$.

Soit N un entier naturel strictement positif ; si a et b sont des entiers relatifs, on note $a \equiv b \pmod{N}$ pour dire que a et b sont congrus modulo N, c'est-à-dire que $a - b$ est multiple de N. La classe de congruence modulo N d'un entier relatif x est l'ensemble des entiers relatifs qui sont congrus à x modulo N. On note $\mathbf{Z}/N\mathbf{Z}$ l'anneau des entiers modulo N.

Soit G un groupe abélien dont la loi de groupe est notée additivement. Si A, B sont des parties de G, on note respectivement $A+B$ et $A-B$ l'ensemble des sommes $a+b$ et l'ensemble des différences $a-b$, où a parcourt A et b parcourt B. Lorsque ces parties ne sont pas vides, on pose aussi

$$d_{\mathrm{R}}(A,B) = \log \frac{\mathrm{Card}(A-B)}{\sqrt{\mathrm{Card}(A)\,\mathrm{Card}(B)}}.$$

Si A est une partie de G et n est un entier naturel, on note nA l'ensemble $A + A + \cdots + A$ (où il y a n termes). Enfin, si $b \in G$, on fera l'abus de notation consistant à noter $b + A$ l'ensemble $\{b\} + A$.

Soit d un entier naturel tel que $d > 0$; soit T un entier naturel. On dit qu'une partie P de G est une progression arithmétique de dimension d et de taille T s'il existe des éléments $x_0, \ldots, x_d$ de G et des entiers naturels non nuls $N_1, \ldots, N_d$ tels que $T = N_1 \cdots N_d$ et $P = \left\{ x_0 + \sum_{j=1}^{d} n_j x_j \,;\, 0 \leqslant n_j \leqslant N_j - 1 \right\}$; on dit qu'une telle progression arithmétique est *propre* si l'on a $\mathrm{Card}(P) = T$.

I. Sommes de parties

1. Soit t un entier naturel non nul et soit N un entier naturel.

a) Soit n et p des entiers naturels tels que $n \geqslant p$; démontrer l'égalité

$$\binom{p}{p} + \binom{p+1}{p} + \cdots + \binom{n}{p} = \binom{n+1}{p+1}.$$

b) Démontrer que l'ensemble des t-uplets $(a_1, \ldots, a_t)$ d'entiers naturels tels que $a_1 + \cdots + a_t = N$ a pour cardinal $\binom{N+t-1}{N}$.

c) Vérifier l'encadrement

$$\frac{1}{N!} t^N \leqslant \binom{N+t-1}{N} \leqslant t^N.$$

2. Soit G un groupe abélien fini et soit A, B des parties non vides de G telles que $\mathrm{Card}(A) + \mathrm{Card}(B) > \mathrm{Card}(G)$.

a) Démontrer que $G = A + B$.

b) Donner un exemple où l'on a $\mathrm{Card}(A) + \mathrm{Card}(B) = \mathrm{Card}(G)$ mais $G \neq A + B$.

3. Soit G un groupe abélien.

a) Si A et B sont des parties finies et non vides de G, démontrer les inégalités

$$\max(\mathrm{Card}(A), \mathrm{Card}(B)) \leqslant \mathrm{Card}(A+B) \leqslant \mathrm{Card}(A)\,\mathrm{Card}(B). \tag{I.1}$$

b) Soit A une partie finie et non vide de G. Démontrer pour tout entier naturel $n \geqslant 1$ les inégalités

$$\mathrm{Card}(A) \leqslant \mathrm{Card}(2A) \leqslant \cdots \leqslant \mathrm{Card}(nA) \leqslant \binom{\mathrm{Card}(A) + n - 1}{n}. \tag{I.2}$$

4. Soit A et B des parties finies et non vides de $\mathbf{Z}$.

a) Démontrer que $\mathrm{Card}(A+B) \geqslant \mathrm{Card}(A) + \mathrm{Card}(B) - 1$.

b) On suppose que $\mathrm{Card}(A+B) = \mathrm{Card}(A) + \mathrm{Card}(B) - 1$ et que A et B ne sont pas des singletons. Démontrer qu'il existe des entiers a, b et d tels que

$$A = \{a, a+d, \ldots, a + (\mathrm{Card}(A) - 1)d\} \quad \text{et} \quad B = \{b, b+d, \ldots, b + (\mathrm{Card}(B) - 1)d\}.$$

5. Soit G un groupe abélien et soit A, B des parties finies et non vides de G.

a) Soit H l'ensemble des éléments g de G tels que $A = g + A$. Démontrer que H est un sous-groupe fini de G.

b) Démontrer que $\mathrm{Card}(A+B) = \mathrm{Card}(A)$ si et seulement s'il existe $b \in G$ tel que $B \subset b + H$.

6. Soit G un groupe abélien et soit A, B, C des parties finies et non vides de G. Démontrer que $d_{\mathrm{R}}(A, B) \geqslant 0$. Démontrer aussi l'« inégalité triangulaire » :

$$d_{\mathrm{R}}(A, C) \leqslant d_{\mathrm{R}}(A, B) + d_{\mathrm{R}}(B, C). \tag{I.3}$$

7. Soit A et B des parties finies non vides de G. Démontrer que $d_{\mathrm{R}}(A,B) = 0$ si et seulement s'il existe un sous-groupe fini H de G et des éléments $a, b \in G$ tels que $A = a + H$ et $B = b + H$.

II. Valeurs aux entiers de formes quadratiques définies positives

On dira qu'une famille $(\vec{v}_1, \ldots, \vec{v}_n)$ de l'espace vectoriel $\mathbf{R}^n$ est une *base entière* si elle est formée d'éléments de $\mathbf{Z}^n$ et si tout élément de $\mathbf{Z}^n$ est combinaison linéaire à coefficients entiers des $\vec{v}_i$.

1. Soit $(\vec{v}_1, \ldots, \vec{v}_n)$ une famille d'éléments de $\mathbf{Z}^n$. Démontrer que c'est une base entière si et seulement si son déterminant (dans la base canonique) est égal à ± 1.

2. Pour $\vec{v} = (a_1, \ldots, a_n) \in \mathbf{Z}^n$, on pose $s(\vec{v}) = |a_1| + \cdots + |a_n|$.

Soit $\vec{v} \in \mathbf{Z}^n$ un vecteur non nul dont les coordonnées sont premières entre elles dans leur ensemble. Montrer par récurrence sur $s(\vec{v})$ qu'il existe une base entière $(\vec{v}_1, \ldots, \vec{v}_n)$ de $\mathbf{R}^n$ telle que $\vec{v} = \vec{v}_1$. (*Si $\vec{v} = (a_1, \ldots, a_n)$, choisir $i \in \{1, \ldots, n\}$ de sorte que $|a_i|$ soit minimal et considérer des vecteurs $\vec{w} = (b_1, \ldots, b_n)$ tels que $b_i = a_i$ et b_j est de la forme $a_j - q a_i$ pour $j \neq i$.*)

3. Soit Φ une forme quadratique sur $\mathbf{R}^n$. On note $\mathrm{disc}(\Phi)$ le déterminant de la matrice de Φ dans la base canonique de $\mathbf{R}^n$.

Soit u un endomorphisme de $\mathbf{R}^n$ et Φ_1 la forme quadratique $\Phi \circ u$. Démontrer que $\mathrm{disc}(\Phi_1) = \det(u)^2 \mathrm{disc}(\Phi)$.

4. Soit Φ une forme quadratique définie positive sur $\mathbf{R}^n$. On pose

$$m(\Phi) = \inf_{\vec{v} \in \mathbf{Z}^n \setminus \{0\}} \Phi(\vec{v}).$$

a) Démontrer que $m(\Phi) > 0$ et qu'il existe un vecteur $\vec{v}_1 \in \mathbf{Z}^n \setminus \{0\}$ tel que $\Phi(\vec{v}_1) = m(\Phi)$.

b) Démontrer qu'il existe une base entière de $\mathbf{R}^n$ de la forme $(\vec{v}_1, \ldots, \vec{v}_n)$, où $\Phi(\vec{v}_1) = m(\Phi)$.

c) Montrer qu'il existe une forme linéaire L_1 sur $\mathbf{R}^n$ et une forme quadratique Φ_1 sur $\mathbf{R}^{n-1}$ telles que

$$L_1(1, 0, \ldots, 0) = 1; \tag{II.1}$$

$$\Phi(x_1 \vec{v}_1 + \cdots + x_n \vec{v}_n) = m(\Phi) L_1(x_1, \ldots, x_n)^2 + \Phi_1(x_2, \ldots, x_n) \tag{II.2}$$

pour tout $(x_1, \ldots, x_n) \in \mathbf{R}^n$.

d) Démontrer que Φ_1 est une forme quadratique définie positive sur $\mathbf{R}^{n-1}$, et que l'on a l'égalité $\mathrm{disc}(\Phi) = m(\Phi)\,\mathrm{disc}(\Phi_1)$.

e) Démontrer que pour tout $(x_2, \ldots, x_n) \in \mathbf{Z}^{n-1}$, il existe $x_1 \in \mathbf{Z}$ tel que $|L_1(x_1, \ldots, x_n)| \leqslant 1/2$.

f) Démontrer que $m(\Phi) \leqslant \frac{4}{3} m(\Phi_1)$.

g) En déduire par récurrence que $m(\Phi) \leqslant (4/3)^{(n-1)/2} \mathrm{disc}(\Phi)^{1/n}$.

h) Démontrer par récurrence qu'il existe une base entière $(\vec{v}_1, \dots, \vec{v}_n)$ de $\mathbf{R}^n$ telle que

$$\Phi(\vec{v}_1) \cdots \Phi(\vec{v}_n) \leqslant (4/3)^{n(n-1)/2} \operatorname{disc}(\Phi).$$

III. Transformation de Fourier et sommes d'ensembles

Soit N un entier tel que $N \geqslant 1$; posons $\omega = \exp(2i\pi/N)$. Si a est un élément de $\mathbf{Z}/N\mathbf{Z}$, on notera ω^a le nombre complexe ω^n, où n est un élément quelconque de la classe de congruence a.

Pour toute application $f : \mathbf{Z}/N\mathbf{Z} \to \mathbf{C}$, on définit alors une application $\hat{f} : \mathbf{Z}/N\mathbf{Z} \to \mathbf{C}$ en posant

$$\hat{f}(x) = \sum_{a \in \mathbf{Z}/N\mathbf{Z}} f(a)\omega^{ax}, \quad \text{pour tout } x \in \mathbf{Z}/N\mathbf{Z}.$$

Si f et g sont des applications de $\mathbf{Z}/N\mathbf{Z}$ dans $\mathbf{C}$, on définit aussi une application $f * g$ de $\mathbf{Z}/N\mathbf{Z}$ dans $\mathbf{C}$ par la formule

$$(f * g)(a) = \sum_{t \in \mathbf{Z}/N\mathbf{Z}} f(t)g(a-t), \quad \text{pour tout } a \in \mathbf{Z}/N\mathbf{Z}.$$

Pour $a \in \mathbf{Z}/N\mathbf{Z}$, on note $d_N(a)$ le minimum des $|x/N|$ où x parcourt l'ensemble des éléments de la classe de congruence a. Si X est une partie de $\mathbf{Z}/N\mathbf{Z}$ et r un nombre réel strictement positif, on définit $\mathscr{B}(X, r)$ comme l'ensemble des $a \in \mathbf{Z}/N\mathbf{Z}$ tels que $d_N(ax) \leqslant r$ pour tout $x \in X$.

1. Soit $a \in \mathbf{Z}/N\mathbf{Z}$. Démontrer que $\sum_{x \in \mathbf{Z}/N\mathbf{Z}} \omega^{ax}$ vaut N si $a = 0$, et vaut 0 sinon.

2. Soit f, g des applications de $\mathbf{Z}/N\mathbf{Z}$ dans $\mathbf{C}$. Démontrer les formules suivantes :

a) pour $a \in \mathbf{Z}/N\mathbf{Z}$, $f(a) = \dfrac{1}{N} \displaystyle\sum_{x \in \mathbf{Z}/N\mathbf{Z}} \hat{f}(x)\omega^{-ax}$;

b) on a $\displaystyle\sum_{a \in \mathbf{Z}/N\mathbf{Z}} f(a)g(a) = \frac{1}{N} \sum_{x \in \mathbf{Z}/N\mathbf{Z}} \hat{f}(x)\hat{g}(-x)$;

c) pour tout $x \in \mathbf{Z}/N\mathbf{Z}$, on a $\widehat{(f * g)}(x) = \hat{f}(x)\hat{g}(x)$.

3. Soit A une partie de $\mathbf{Z}/N\mathbf{Z}$ et soit $f_A : \mathbf{Z}/N\mathbf{Z} \to \mathbf{C}$ sa fonction indicatrice.

a) Démontrer les formules

$$\text{(III.1)} \qquad \frac{1}{N} \sum_{x \in \mathbf{Z}/N\mathbf{Z}} \left|\widehat{f_A}(x)\right|^2 = \operatorname{Card}(A);$$

$$\text{(III.2)} \qquad \frac{1}{N} \sum_{x \in \mathbf{Z}/N\mathbf{Z}} \left|\widehat{f_A}(x)\right|^4 = \operatorname{Card}\left(\{(a_1, a_2, a_3, a_4) \in A^4 ; a_1 + a_2 = a_3 + a_4\}\right).$$

b) Démontrer qu'un élément a de $\mathbf{Z}/N\mathbf{Z}$ appartient à $2A - 2A$ si et seulement si l'expression

$$\sum_{x \in \mathbf{Z}/N\mathbf{Z}} \left|\widehat{f_A}(x)\right|^4 \omega^{-ax}$$

n'est pas nulle.

4. Soit κ un entier naturel. On dit qu'une suite $(x_1,\dots,x_\kappa)$ d'éléments de $\mathbf{Z}/N\mathbf{Z}$ est indépendante si la seule suite $(\varepsilon_1,\dots,\varepsilon_\kappa)$ d'entiers de $\{-1,0,1\}$ telle que $\sum_{j=1}^{\kappa}\varepsilon_j x_j = 0$ est la suite $(0,\dots,0)$.

Soit X une partie de $\mathbf{Z}/N\mathbf{Z}$ et soit $(x_1,\dots,x_\kappa)$ une suite indépendante d'éléments de X telle que κ soit maximal.

a) Démontrer que X est contenu dans l'ensemble des éléments de $\mathbf{Z}/N\mathbf{Z}$ de la forme $\sum_{j=1}^{\kappa}\varepsilon_j x_j$, où $\varepsilon_j \in \{-1,0,1\}$ pour tout j.

b) On pose $K = \{x_1,\dots,x_\kappa\}$. Démontrer que pour tout nombre réel $r > 0$, l'ensemble $\mathscr{B}(X,r)$ contient l'ensemble $\mathscr{B}(K,r/\kappa)$. (Ces ensembles sont définis au début de cette partie.)

Les trois questions suivantes ont pour but de majorer la taille maximale d'une suite indépendante formée d'éléments d'une partie X. Cet objectif est atteint à la question III.7, c).

5. *a*) Soit t un nombre réel ; démontrer que la fonction F de $\mathbf{R}$ dans $\mathbf{R}$ donnée par $F(x) = \exp(tx)$ est convexe.

b) Soit t et y des nombres réels tels que $|y| \leqslant 1$; démontrer que $\exp(ty) \leqslant \cosh(t) + y\sinh(t)$.

c) Pour $t \in \mathbf{R}$, démontrer que $\cosh(t) \leqslant \exp(t^2/2)$.

6. Soit $(x_1,\dots,x_\kappa)$ une suite indépendante d'éléments de $\mathbf{Z}/N\mathbf{Z}$, soit $(c_1,\dots,c_\kappa)$ une suite de nombres complexes et soit $g\colon \mathbf{Z}/N\mathbf{Z} \to \mathbf{C}$ l'application définie par

$$g(a) = \sum_{j=1}^{\kappa} \Re\left(c_j \omega^{-ax_j}\right), \quad \text{pour } a \in \mathbf{Z}/N\mathbf{Z}.$$

a) Calculer $\hat{g}(x)$ pour $x \in \mathbf{Z}/N\mathbf{Z}$. En déduire que $\sum_{a\in\mathbf{Z}/N\mathbf{Z}} g(a) = 0$.

b) Démontrer que $\displaystyle\sum_{a\in\mathbf{Z}/N\mathbf{Z}} g(a)^2 = \frac{1}{2}N\sum_{j=1}^{\kappa}|c_j|^2$.

c) Pour $j \in \{1,\dots,\kappa\}$, soit $\tilde{x}_j$ un entier naturel dans la classe de congruence x_j et soit θ_j un nombre réel. Démontrer que pour toute partie non vide J de $\{1,\dots,\kappa\}$,

$$\sum_{a=0}^{N-1}\prod_{j\in J}\cos\left(\frac{2\pi}{N}a\tilde{x}_j + \theta_j\right) = 0.$$

d) Démontrer que pour tout $t \in \mathbf{R}$, on a

$$\frac{1}{N}\sum_{a\in\mathbf{Z}/N\mathbf{Z}}\exp(tg(a)) \leqslant \exp\left(\frac{1}{N}t^2\sum_{a\in\mathbf{Z}/N\mathbf{Z}}g(a)^2\right).$$

7. Dans cette question et dans la suivante, on considère la situation suivante. Soit ρ et α des nombres réels tels que $0 < \rho < 1$ et $0 < \alpha < 1$. Soit A une partie de $\mathbf{Z}/N\mathbf{Z}$ telle que $\mathrm{Card}(A) \geqslant \alpha N$ et soit f_A sa fonction indicatrice. Soit X l'ensemble des $x \in \mathbf{Z}/N\mathbf{Z}$ tels que $\left|\widehat{f_A}(x)\right| \geqslant \rho\,\mathrm{Card}(A)$.

a) Soit κ un entier naturel et soit $(x_1,\dots,x_\kappa)$ une suite indépendante de $\mathbf{Z}/N\mathbf{Z}$ telle que $x_j \in X$ pour tout $j \in \{1,\dots,\kappa\}$. Pour $a \in \mathbf{Z}/N\mathbf{Z}$, on pose

$$g(a) = \sum_{j=1}^{\kappa} \Re(\widehat{f_A}(x_j)\omega^{-ax_j}).$$

Démontrer que

$$\sum_{a\in\mathbf{Z}/N\mathbf{Z}} f_A(a)g(a) = \frac{2}{N}\sum_{a\in\mathbf{Z}/N\mathbf{Z}} g(a)^2.$$

b) Minorer l'expression $\sum_{a\in A}\exp(tg(a))$, pour $t \in \mathbf{R}$, et démontrer que

$$\sum_{a\in\mathbf{Z}/N\mathbf{Z}} g(a)^2 \leqslant N\,\mathrm{Card}(A)^2\log(1/\alpha).$$

c) En déduire que $\kappa \leqslant 2\rho^{-2}\log(1/\alpha)$.

8. On pose $\sigma = \mathrm{Card}(A+A)/\mathrm{Card}(A)$ et on choisit $\rho = 1/2\sqrt{\sigma}$.

a) Démontrer que $\sum_{x\in\mathbf{Z}/N\mathbf{Z}} \left|\widehat{f_A}(x)\right|^4 \geqslant \alpha^3N^4/\sigma$.

b) Démontrer que $\sum_{x\notin X} \left|\widehat{f_A}(x)\right|^4 \leqslant \alpha^3N^4/4\sigma$.

c) Démontrer que $2A-2A$ contient $\mathscr{B}(X,1/16)$. (*On pourra utiliser, après l'avoir démontrée, l'inégalité* $|1-\omega^a| \leqslant 2\pi d_N(a)$ *pour tout* $a \in \mathbf{Z}$.)

d) On pose $r = \left(128\sigma\log(1/\alpha)\right)^{-1}$. Démontrer qu'il existe une partie K de $\mathbf{Z}/N\mathbf{Z}$ de cardinal $\leqslant 8\sigma\log(1/\alpha)$ telle que $2A-2A$ contienne $\mathscr{B}(K,r)$.

IV. Progressions arithmétiques

1. Soit N un nombre premier, soit n un entier naturel non nul. On désigne par $N\cdot\mathbf{Z}^n$ l'ensemble des éléments de $\mathbf{Z}^n$ dont toutes les coordonnées sont divisibles par N. Soit $\vec{\xi} = (\xi_1,\dots,\xi_n)$ un élément de $\mathbf{Z}^n$ qui n'appartient pas à $N\cdot\mathbf{Z}^n$.

a) Démontrer qu'il existe des entiers relatifs $a, b_1,\dots,b_n$ tels que les nombres entiers $a\xi_1+Nb_1, a\xi_2+Nb_2,\dots,a\xi_n+Nb_n$ soient premiers entre eux dans leur ensemble.

b) Soit L l'ensemble des éléments $\vec{x}$ de $\mathbf{Z}^n$ tels qu'il existe $u \in \mathbf{Z}$ de sorte que $\vec{x}-u\vec{\xi} \in N\cdot\mathbf{Z}^n$. Démontrer qu'il existe une base entière $(\vec{v}_1,\dots,\vec{v}_n)$ de $\mathbf{R}^n$ telle que L soit l'ensemble des combinaisons linéaires $t_1\vec{v}_1+Nt_2\vec{v}_2+\cdots+Nt_n\vec{v}_n$, pour $(t_1,\dots,t_n) \in \mathbf{Z}^n$. (*On pourra commencer par trouver un vecteur* $\vec{v}_1 \in L$ *dont les coordonnées sont premières entre elles.*)

c) Démontrer qu'il existe une base $(\vec{w}_1,\dots,\vec{w}_n)$ de $\mathbf{R}^n$ formée de vecteurs appartenant à L tels que $\|\vec{w}_1\|\cdots\|\vec{w}_n\| \leqslant (4/3)^{n(n-1)/4}N^{n-1}$. (*On pourra introduire la forme quadratique sur* $\mathbf{R}^n$ *définie par* $\Phi(x_1,\dots,x_n) = \|x_1\vec{v}_1+Nx_2\vec{v}_2+\cdots+Nx_n\vec{v}_n\|^2$ *et utiliser les résultats de la partie II.*)

2. On conserve les notations de la question précédente.

Pour tout $i \in \{1,\dots,n\}$, soit x_i un entier relatif tel que $\vec{w}_i - x_i\vec{\xi}$ appartienne à $N\cdot\mathbf{Z}^n$. On note X la partie de $\mathbf{Z}/N\mathbf{Z}$ formée des classes des ξ_i modulo N. Soit r un nombre réel

strictement positif tel que $r < 1/2$. Soit M l'ensemble des éléments $\mu = (\mu_1, \dots, \mu_n) \in \mathbf{Z}^n$ tels que $|\mu_i| \leqslant Nr/(n\|\vec{w}_i\|)$ pour tout $i \in \{1, \dots, n\}$. Pour $\mu \in M$, posons $p(\mu) = \sum_{i=1}^n \mu_i x_i$ et soit $P = \{p(\mu)\,;\, \mu \in M\}$.

Démontrer les propriétés suivantes :

a) Si μ et μ' sont deux éléments distincts de M, $p(\mu)$ et $p(\mu')$ ne sont pas congrus modulo N.

b) Le cardinal de P est supérieur ou égal à $(r/n)^n (3/4)^{n(n-1)/4} N$.

c) Pour tout $\mu \in M$, la classe modulo N de $p(\mu)$ appartient à $\mathscr{B}(X, r)$.

3. Soit X une partie de $\mathbf{Z}/N\mathbf{Z}$ de cardinal $n > 0$ et r un nombre réel tel que $0 < r < 1/2$. Démontrer que $\mathscr{B}(X, r)$ contient une progression arithmétique propre de dimension n et de taille au moins $(3/4)^{n(n-1)/4}(r/n)^n N$.

4. Soit A une partie non vide de $\mathbf{Z}/N\mathbf{Z}$; soit α et σ des nombres réels strictement positifs tels que $\mathrm{Card}(A) \geqslant \alpha N$; on pose $\sigma = \mathrm{Card}(A+A)/\mathrm{Card}(A)$. Démontrer que $2A - 2A$ contient une progression arithmétique propre de dimension $d \leqslant 8\sigma \log(1/\alpha)$ et de taille $\geqslant N(128\sigma \log(1/\alpha)(4/3)^{(d-1)/4})^{-d}$.

V. Théorème de Freiman–Rusza–Chang

Soit G un groupe abélien, soit A une partie non vide de G. À partir de la question V.4, on pourra utiliser librement l'inégalité remarquable due à Plünnecke affirmant que pour tous entiers naturels m et n, $\mathrm{Card}(mA - nA) \leqslant \sigma^{m+n}\mathrm{Card}(A)$, où $\sigma = \mathrm{Card}(A+A)/\mathrm{Card}(A)$.

Soit H un groupe abélien et soit f une application de A dans H. Si k est un entier $\geqslant 1$, on dit que f est k-tendue si l'on a $f(x_1) + \cdots + f(x_k) = f(y_1) + \cdots + f(x_k)$ dès que $x_1, \dots, x_k, y_1, \dots, y_k$ sont des éléments de A tels que $x_1 + \cdots + x_k = y_1 + \cdots + y_k$.

Soit B une partie non vide de H. On dit que A est k-semblable à B s'il existe des applications bijectives $f\colon A \to B$ et $g\colon B \to A$ inverses l'une de l'autre qui sont k-tendues.

1. Soit G et H des groupes abéliens, soit k un entier naturel $\geqslant 2$, soit A une partie de G et soit $f\colon A \to H$ une application qui est k-tendue. Soit n et m des entiers naturels tels que $1 \leqslant m + n \leqslant k$.

a) Démontrer que pour tout entier p tel que $1 \leqslant p \leqslant k$, f est p-tendue.

b) Vérifier qu'il existe une unique application $F\colon mA - nA \to H$ telle que

$$F(a_1 + \cdots + a_m - b_1 - \cdots - b_n) = f(a_1) + \cdots + f(a_m) - f(b_1) - \cdots - f(b_n)$$

pour tout $(a_1, \dots, a_m, b_1, \dots, b_n) \in A^{m+n}$.

c) Si p est un entier naturel tel que $1 \leqslant p \leqslant k/(m+n)$, démontrer que F est p-tendue.

d) On suppose que A est une progression arithmétique de dimension d et de taille M, pour des entiers naturels non nuls d et M. Démontrer qu'il en est de même de $f(A)$.

2. Soit G et H des groupes abéliens, soit k un entier naturel tel que $k \geqslant 2$. Soit A et B des parties finies non vides de G et H respectivement qui sont k-semblables.

a) Soit m, n, p des entiers naturels tels que $(m+n)p \leqslant k$. Démontrer que $mA - nA$ et $mB - nB$ sont p-semblables.

b) En déduire que $\mathrm{Card}(mA - nA) = \mathrm{Card}(mB - nB)$ pour tout couple (m, n) d'entiers naturels tels que $m + n \leqslant k$.

3. Soit N un entier naturel ; soit p un nombre premier. Soit $f : \mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}$ l'application qui, à $x \in \mathbf{Z}/p\mathbf{Z}$, associe l'unique entier de $\{0, \ldots, p-1\}$ qui appartient à la classe de congruence x. Soit k un entier naturel tel que $k \geqslant 2$.

a) Pour $j \in \{1, \ldots, k\}$, on note $I(j)$ l'ensemble $\left[\frac{j-1}{k}p, \frac{j}{k}p\right[\cap \mathbf{N}$. Démontrer que pour tout entier $j \in \{1, \ldots, k\}$, la restriction de f à $f^{-1}(I(j))$ est une application k-tendue de $f^{-1}(I(j))$ dans $\mathbf{Z}$.

b) Soit A une partie de $\mathbf{Z}/p\mathbf{Z}$. Démontrer que pour tout $u \in (\mathbf{Z}/p\mathbf{Z})^*$, il existe une partie $A(u)$ de A de cardinal $\geqslant \mathrm{Card}(A)/k$ telle que l'application $f_u : A(u) \to \mathbf{Z}/N\mathbf{Z}$ définie par $x \mapsto f(ux) \pmod N$ soit k-tendue.

c) Soit z un élément non nul de $kA - kA$; combien y a-t-il d'éléments $u \in (\mathbf{Z}/p\mathbf{Z})^*$ tels que $f(uz) \equiv 0 \pmod N$? En déduire que si $N \geqslant \mathrm{Card}(kA - kA)$, il existe $u \in (\mathbf{Z}/p\mathbf{Z})^*$ tels que $A(u)$ et $f_u(A(u))$ soient k-semblables.

4. Soit A une partie finie de $\mathbf{Z}$. On suppose que A est de cardinal au moins 2 et on pose $\sigma = \mathrm{Card}(A+A)/\mathrm{Card}(A)$.

a) Démontrer que $\sigma \geqslant 3/2$.

b) Soit k un entier naturel. Démontrer que pour tout nombre premier p assez grand, A est k-semblable à une partie de $\mathbf{Z}/p\mathbf{Z}$.

c) Soit k un entier naturel tel que $k \geqslant 2$. Démontrer que pour tout entier naturel N tel que $N > \sigma^{2k}\mathrm{Card}(A)$, il existe une partie B de A de cardinal $\geqslant \mathrm{Card}(A)/k$ qui est k-semblable à une partie de $\mathbf{Z}/N\mathbf{Z}$.

d) En prenant $k = 8$ et en choisissant pour N un nombre premier tel que $\sigma^{2k}\mathrm{Card}(A) < N < 2\sigma^{2k}\mathrm{Card}(A)$ (*on ne cherchera pas à démontrer l'existence d'un tel nombre premier N*), démontrer l'énoncé suivant : il existe un nombre réel $c_1 > 0$ (indépendant de A et de σ) tel que $2A - 2A$ contienne une progression arithmétique propre de dimension au plus $c_1\sigma\log\sigma$ et de taille au moins $\mathrm{Card}(A)\exp(-c_1\sigma^2(\log\sigma)^2)$.

5. Soit A une partie finie non vide de $\mathbf{Z}$; on pose $\sigma = \mathrm{Card}(A+A)/\mathrm{Card}(A)$ et on note c le plus petit entier naturel tel que $c \geqslant 2\sigma$. Soit P une progression arithmétique propre de dimension d et taille $\beta\mathrm{Card}(A)$ qui est contenue dans $2A - 2A$, où β est un nombre réel strictement positif.

On définit des suites (P_i) et (S_i) de parties de $\mathbf{Z}$ par récurrence comme suit :

- on pose $P_0 = P$;
- si $P_0, S_0, P_1, \ldots, P_i$ sont définis, on considère une partie S_i de A de cardinal maximal de sorte que les parties $x + P_i$, pour $x \in S_i$, soient deux à deux disjointes ;
- si $\mathrm{Card}(S_i) \leqslant c$, on s'arrête ;

– si $\mathrm{Card}(S_i) > c$, on choisit une partie S'_i de S_i dont le cardinal est égal à c, on pose $P_{i+1} = S'_i + P_i$ et on continue.

a) Soit t un entier tel que la partie P_t soit définie. Démontrer que l'on a $\mathrm{Card}(P_t) = c^t \mathrm{Card}(P)$. Démontrer que $P_t \subset (t+2)A - 2A$, et en déduire l'inégalité

$$2^t \leqslant \sigma^4 \mathrm{Card}(A) / \mathrm{Card}(P).$$

b) Soit t le plus grand entier tel que P_t soit définie. Démontrer l'inclusion

$$A \subset (P-P) + (S'_0 - S'_0) + \cdots + (S'_{t-1} - S'_{t-1}) + S_t.$$

c) Pour toute partie finie non vide S de $\mathbf{Z}$, démontrer que $S - S$ est contenue dans une progression arithmétique de dimension $\mathrm{Card}(S)$ et de taille $3^{\mathrm{Card}(S)}$. En déduire qu'il existe un nombre réel c_2 (indépendant de σ, β et d) tel que que A soit contenu dans une progression arithmétique de dimension δ et de taille τ, avec

$$\delta \leqslant c_2\big(d + \sigma \log\frac{\sigma}{\beta}\big) \quad \text{et} \quad \log\frac{\tau}{\mathrm{Card}(A)} \leqslant c_2\big(d + \log\frac{\sigma}{\beta}\big).$$

6. Démontrer qu'il existe un nombre réel $c_3 > 0$ de sorte que l'énoncé suivant (théorème de Freiman–Rusza–Chang) soit vérifié : Soit A une partie finie non vide de $\mathbf{Z}$ et posons $\sigma = \mathrm{Card}(A+A)/\mathrm{Card}(A)$; alors, A est contenue dans une progression arithmétique de dimension δ et de taille M, où

$$\delta \leqslant c_3\sigma^3(\log\sigma)^2 \quad \text{et} \quad \log\frac{M}{\mathrm{Card}(A)} \leqslant c_3\sigma^3(\log\sigma)^2 \quad .$$

Fin de l'épreuve.