Séminaire BOURBAKI Novembre 2010
63ème année, 2010-2011, n$^{\text{o}}$ 1028

CRIBLE EN EXPANSION

par **Emmanuel KOWALSKI**

1. INTRODUCTION

L'objet de ce rapport est de présenter des travaux récents qui étendent les méthodes de crible depuis leur cadre classique, vers des situations nouvelles caractérisées par l'apparition d'ensembles discrets « à croissance exponentielle », provenant tout particulièrement de groupes discrets tels que $\mathrm{SL}_m(\mathbf{Z})$ ou ses sous-groupes suffisamment « grand », en un certain sens.

Un exposé récent de Sarnak [54] indique en partie les premières motivations de ces travaux (liées à l'équation de Markov et aux géodésiques de la surface modulaires). Les premiers résultats généraux concernant ces problèmes sont apparus vers 2005 sous forme de prépublications, et Bourgain, Gamburd et Sarnak ont publié un article présentant ses aspects particuliers [4]. D'autres applications, dont certaines ont une saveur géométrique très différente, sont aussi apparues indépendamment vers cette période, tout d'abord (un peu implicitement) dans certains travaux de Rivin [52].

L'aspect le plus crucial des applications des méthodes de crible dans ces nouvelles situations est qu'elles dépendent de propriétés d'expansion ou de « trou spectral », que ce soit d'un point de vue discret ou combinatoire (lié aux graphes expanseurs ou à la Propriété (τ) de Lubotzky [40]) ou d'un point de vue plus géométrique (généralisant par exemple l'inégalité de Selberg $\lambda_1 \geqslant 3/16$ pour la première valeur propre non-nulle de l'opérateur de Laplace sur les surfaces modulaires de congruence classiques).

Les développements existant (ou en cours de rédaction) se traduisent, en définitive, par l'existence aujourd'hui d'estimations de crible très générales qui font intervenir des objets discrets à croissance exponentielle. Ces inégalités ont un potentiel d'application considérable – y compris pour des questions qui sont, a priori, sans rapport avec la théorie analytique des nombres –, dû en grande partie aux nombreux cas nouveaux où la propriété de trou spectral désirée a été démontrée. Les théorèmes d'expansion pour les groupes linéaires finis sont particulièrement impressionnants (à commencer par l'article [26] de Helfgott dans le cas de SL_2 qui a été le point de départ de ces progrès), ainsi que ceux concernant l'application de méthodes ergodiques aux réseaux dans des groupes semisimples ayant la Propriété (τ) (en particulier les travaux de Gorodnik et Nevo [21]).

Avant de se diriger vers le cœur de ce rapport, nous commençons par énoncer un résultat simple qui provient du crible en expansion. Rappelons pour cela tout d'abord que $\Omega(n)$ est

la fonction arithmétique qui donne le nombre de facteurs premiers, comptés avec multiplicité, d'un entier $n \neq 0$, étendue à 0 en posant $\Omega(0) = +\infty$.

THÉORÈME 1.1. — *Soit $\Lambda \subset \mathrm{SL}_m(\mathbf{Z})$ un sous-groupe Zariski-dense, par exemple, le groupe L engendré par les éléments*

$$\begin{pmatrix} 1 & \pm 3 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ \pm 3 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}), \tag{1}$$

dans le cas $m = 2$

Soit f une fonction polynôme à coefficients entiers en m variables, par exemple $f = X_1 \cdots X_m$. Soit $x_0 \in \mathbf{Z}^m - \{0\}$ un vecteur fixé. Il existe un entier $r = r(f, x_0, \Lambda) \geqslant 1$ tel que l'ensemble

$$\mathcal{O}_f(x_0; r) = \{\gamma \in \Lambda \mid \Omega(f(\gamma \cdot x_0)) \leqslant r\}$$

est Zariski-dense *dans SL_m, et en particulier est infini. Plus précisément, il existe un tel r pour lequel $\mathcal{O}_f(x_0; r)$ est un ensemble* non mince*, au sens de* [57, Def. 3.1.1].

Il est important de noter – comme cela sera rappelé plus bas – que Λ peut très bien avoir un indice infini dans $\mathrm{SL}_m(\mathbf{Z})$. C'est le cas, par exemple, du groupe L engendré par les matrices (1) (ce qu'on peut voir, par exemple, en déterminant un domaine fondamental pour l'action de L par homographies sur le demi-plan de Poincaré et en vérifiant que son aire hyperbolique est $+\infty$.)

Notations. Nous rappelons quelques notations essentielles.
– La lettre p désignera toujours un nombre premier ; on désigne en particulier par $\mathbf{F}_p$ le corps fini $\mathbf{Z}/p\mathbf{Z}$, et on écrit plus généralement $\mathbf{F}_q$ pour un corps fini à q éléments. Pour un ensemble X, $|X|$ désigne son cardinal, qui est un entier positif ou bien $+\infty$; pour un graphe Γ, $|\Gamma|$ est le nombre de sommets.
– Les notations de Landau et Vinogradov $f = O(g)$ et $f \ll g$ sont synonymes ; $f(x) = O(g(x))$ pour tout $x \in D$ signifie qu'il existe une constante « implicite » $C \geqslant 0$ (qui peut dépendre d'autres paramètres, qui seront indiqués explicitement) telle que $|f(x)| \leqslant Cg(x)$ pour tout $x \in D$. Cette définition *diffère* de celle de N. Bourbaki [1, Chap. V], puisque cette dernière est de nature topologique. Par contre, les notations $f(x) \sim g(x)$ et $f = o(g)$ ont dans ce texte le sens asymptotique de loc. cit. On écrire $f \asymp g$ pour $f \ll g$ et $g \ll f$ simultanément.

Remerciements. Je remercie chaleureusement J. Bourgain, N. Dunfield, E. Fuchs, A. Gamburd, C. Hall, F. Jouve, A. Kontorovich, H. Oh, L. Pyber, P. Sarnak, D. Zywina pour leur aide, remarques et corrections concernant ce texte. En particulier, les discussions avec O. Marfaing durant la préparation de son rapport de Master sur ce sujet [43] ont été très utiles.

2. MOTIVATION

Les méthodes de crible concernent les propriétés multiplicatives des entiers, ou de sous-ensembles d'entiers. Il est donc naturel de chercher, pour étendre ces méthodes, à décrire des ensembles d'entiers inhabituels. Afin de présenter l'esprit du sujet, nous présentons dans cette section deux exemples de tels ensembles. L'un d'entre eux est un cas particulièrement plaisant du « crible en orbite » de Bourgain, Gamburd et Sarnak, considéré dans [4] : il s'agit de l'ensemble des courbures d'empilements de cercles Apolloniens. Le second est peut-être

encore plus surprenant : il concerne l'ordre du premier groupe d'homologie entière de certaines variétés de dimension 3 aléatoires. Nous le traiterons moins en détail dans la suite, mais il s'agit néanmoins d'un exemple révélateur de la diversité des applications possibles du crible.

2.1. Empilements de cercles Apolloniens

Soient $(\bigcirc_1, \bigcirc_2, \bigcirc_3)$ trois cercles dans le plan, deux à deux tangents et bordant des disques intérieurs disjoints, de rayons respectifs (r_1, r_2, r_3) et courbures $(c_1, c_2, c_3) = (r_1^{-1}, r_2^{-1}, r_3^{-1})$. Une propriété géométrique très classique est l'existence de deux autres cercles exactement (disons $(\bigcirc_4, \bigcirc_4')$, de courbures (c_4, c_4')), tels que les quadruplets

$$(\bigcirc_1, \bigcirc_2, \bigcirc_3, \bigcirc_4) \text{ et } (\bigcirc_1, \bigcirc_2, \bigcirc_3, \bigcirc_4')$$

comportent quatre cercles tangents deux à deux bordant des disques disjoints, si l'on permet (ce qui est possible tant pour les cercles originaux que pour $\bigcirc_4$ et $\bigcirc_4'$) d'avoir des cercles de rayon *négatifs*, auquel cas le « disque » bordé par un cercle est, par convention, le complément dans le plan du disque borné auquel on pense naturellement (voir Figure 1). Un tel quadruplet est appelé une *configuration de Descartes*.

En effet, Descartes a démontré que dans une telle configuration, les courbures des quadruplets vérifient les équations quadratiques

$$Q(c_1, c_2, c_3, c_4) = Q(c_1, c_2, c_3, c_4') = 0$$

où Q est la forme quadratique indéfinie donnée par

$$Q(x, y, z, t) = 2(x^2 + y^2 + z^2 + t^2) - (x + y + z + t)^2.$$

Ainsi, s'il se trouve que $(\bigcirc_1, \bigcirc_2, \bigcirc_3, \bigcirc_4)$ ont des courbures entières (positives ou négatives), on obtient une équation de degré 2 pour déterminer c_4', dans laquelle une solution (à savoir c_4) est supposée connue, et est entière : par conséquent, c_4' sera également un entier. Et si l'on veut continuer l'aventure, le même raisonnement indique que, partant des cercles $(\bigcirc_1, \bigcirc_2, \bigcirc_3, \bigcirc_4)$ à courbures entières, il existe d'autres cercles

$$\bigcirc_1', \bigcirc_2', \bigcirc_3',$$

tels que, par exemple, le quadruplet

$$(\bigcirc_1', \bigcirc_2, \bigcirc_3, \bigcirc_4)$$

soit une configuration de Descartes, avec courbure c_1' (et similairement c_2', c_3') entière. Plus précisément, en résolvant l'équation ci-dessus avec la racine connue, on trouve que

$$\begin{aligned}
(c_1', c_2, c_3, c_4) &= (c_1, c_2, c_3, c_4) \cdot {}^t s_1, \\
(c_1, c_2', c_3, c_4) &= (c_1, c_2, c_3, c_4) \cdot {}^t s_2, \\
(c_1, c_2, c_3', c_4) &= (c_1, c_2, c_3, c_4) \cdot {}^t s_3, \\
(c_1, c_2, c_3, c_4') &= (c_1, c_2, c_3, c_4) \cdot {}^t s_4,
\end{aligned}$$

où les matrices $s_1, \ldots, s_4$ appartiennent au groupe orthogonal entier $O(Q, \mathbf{Z})$ de la forme quadratique ci-dessus, et sont données par

$$s_1 = \begin{pmatrix} -1 & 2 & 2 & 2 \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}, \qquad s_2 = \begin{pmatrix} 1 & & & \\ 2 & -1 & 2 & 2 \\ & & 1 & \\ & & & 1 \end{pmatrix},$$

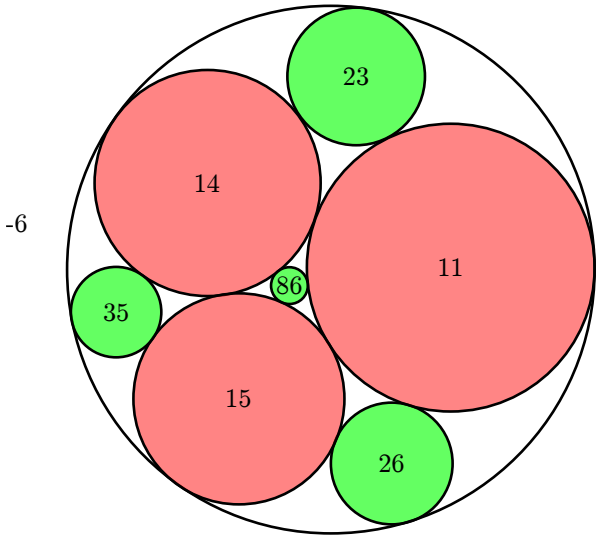

FIGURE 1. Empilement de cercles Apollonien pour $\boldsymbol{c} = (-6, 11, 14, 15)$, avec les courbures indiquées.

(et s_3, s_4 obtenues *mutatis mutandis*). Notons que $s_i^2 = 1$ pour tout i, et que l'on peut même montrer que ce sont les seules relations satisfaites par ces matrices.

Chacun des quadruplets de courbures ainsi obtenus peut être utilisé pour itérer ce procédé. Autrement dit, si l'on note $\mathcal{A}$ le sous-groupe de $O(Q, \mathbf{Z})$ qui est engendré par les s_i, les entiers apparaissant comme coefficients dans un vecteur de l'orbite $\mathcal{A} \cdot \boldsymbol{c}$ d'un « quadruplet racine » $\boldsymbol{c} = (c_1, \ldots, c_4)$, représentent toutes les courbures des cercles qui sont ainsi construits récursivement. On obtient en définitive un *empilement de cercles Apollonien*. La première itération en est représentée dans la Figure 1 dans un cas particulier (on note en particulier l'application de la convention concernant les cercles de rayon négatif.)

L'ensemble $\mathcal{C}(\boldsymbol{c})$ de ces courbures, considéré avec ou sans multiplicités, est notre premier exemple d'entiers susceptibles d'être soumis au crible. Il est d'emblée évident qu'une telle étude sera intimement reliée avec celle du groupe $\mathcal{A}$. De plus, il est également clair que si l'on s'intéresse aux propriétés multiplicatives des éléments de $\mathcal{C}(\boldsymbol{c})$, les propriétés des applications de réduction

$$\mathcal{A} \to \mathcal{A}_p = \mathcal{A} \pmod{p} \subset O(Q, \mathbf{Z}/p\mathbf{Z}),$$

modulo les nombres premiers seront importantes.

Les deux propriétés suivantes de $\mathcal{A}$ expliquent pourquoi ces questions sont abordables, mais très délicates :

– Le groupe $\mathcal{A}$ est « gros » en un sens, à savoir qu'il est *Zariski-dense* dans le groupe $O(Q)$ (vue comme groupe algébrique sur $\mathbf{Q}$) – cela signifie que les identités polynômiales valides pour tout élément de $\mathcal{A}$ sont exactement les mêmes que celles (à priori moins nombreuses) valides pour tout élément du groupe continu $O(Q, \mathbf{C})$.

– Mais cependant, $\mathcal{A}$ est « petit », en un autre sens ; précisément, $\mathcal{A}$ est *d'indice infini* dans le groupe discret $O(Q, \mathbf{Z})$. Comme pour le groupe L de Lubotzky, on peut aussi énoncer cela en disant que le quotient $\mathcal{A}\backslash O(Q, \mathbf{R})$ (une variété hyperbolique de dimension 3) a un *volume infini*, pour la mesure naturelle provenant d'une mesure de Haar sur $O(Q, \mathbf{R})$.

Remarque 2.1. — Les aspects arithmétiques des empilements de cercles Apolloniens ont été discutées pour la première fois dans l'article [23], qui détaille quelques propriétés de $\mathcal{C}(\boldsymbol{c})$, mais l'application de méthodes de crible pour $\mathcal{C}(\boldsymbol{c})$ a commencé dans [4].

2.2. Variétés aléatoires de Dunfield-Thurston

Le second exemple est choisi pour illustrer l'intérêt des méthodes de crible pour étudier des objets a priori assez éloignés des entiers. Il est basé sur un article de Dunfield et Thurston [13] (qui ne mentionne pas explicitement le crible), qui a été développé par Maher [42] et l'auteur [35] (où le crible est appliqué explicitement).

Soit $g \geqslant 2$ un entier donné, et soit H_g un « handlebody » de genre g ; il s'agit d'une variété connexe compacte orientée de dimension 3, dont le bord $\Sigma_g = \partial H_g$ est une surface (compacte connexe orientée) de genre g. Une construction extrêmement classique de variétés compactes de dimension 3 (qui remonte à la thèse de P. Heegaard, et qui – pour un certain g dépendant de la variété – est toujours possible) est la suivante : on prend un homéomorphisme ϕ de Σ_g, et on construit la variété

$$M_\phi = H_g \cup_\phi H_g$$

obtenue en collant deux copies de H_g à l'aide de l'application ϕ qui identifie les points de leur bord commun Σ_g qui se correspondent.

La variété M_ϕ ne change pas, à homéomorphisme près, lorsque ϕ est changé continûment, ce qui signifie que M_ϕ ne dépend que de la classe de ϕ dans le groupe modulaire (« mapping class group ») Γ_g de Σ_g (qui est, grosso modo, le groupe des invariants « discrets » des homéomorphismes de surfaces ; ainsi qu'il a été décrit dans un exposé récent dans ce séminaire [50], ces groupes ont un certain nombre de propriétés communes avec les groupes arithmétiques comme $\mathrm{SL}_m(\mathbf{Z})$, ou mieux comme $\mathrm{Sp}_{2g}(\mathbf{Z})$, qui est un quotient de Γ_g, comme rappelé ci-dessous).

L'article [13] (en partie inspiré par les heuristiques de Cohen-Lenstra concernant les groupes de classes d'idéaux de corps de nombres) étudie les propriétés statistiques du groupe fondamental $\pi_1(M_\phi)$ lorsque ϕ est choisi « au hasard » dans Γ_g (en un sens décrit précisément ci-dessous), et spécialement de l'abélianisé $H_1(M_\phi, \mathbf{Z})$ de $\pi_1(M_\phi)$. La motivation pour cela est la conjecture de Haken virtuelle, selon laquelle toute variété compacte de dimension 3 dont le groupe fondamental est infini devrait avoir un revêtement fini $N \to M$ tel que $H_1(N, \mathbf{Z})$ soit infini.

Ainsi, on va considérer pour le crible l'ensemble des entiers apparaissant comme ordre des sous-groupes de torsion de $H_1(M_\phi, \mathbf{Z})$, lorsque ϕ parcourt Γ_g. Ou plutôt, puisque il est très difficile de contrôler la multiplicité d'apparition de ces entiers, on peut penser à l'application

$$\Gamma_g \to |H_1(M_\phi, \mathbf{Z})| \in \{0, 1, 2, 3, \ldots\} \cup \{+\infty\}.$$

Pourquoi vouloir appliquer le crible ici ? L'idée est de remarquer que l'on dispose d'informations « locales » pour chaque nombre premier p, à savoir l'homologie à coefficients dans $\mathbf{F}_p$, qui est aussi la « réduction modulo p » de $H_1(M_\phi, \mathbf{Z})$:

$$H_1(M_\phi, \mathbf{Z}) \otimes \mathbf{Z}/p\mathbf{Z} = H_1(M_\phi, \mathbf{Z}/p\mathbf{Z}),$$

et qu'on a également une description « locale-globale » des variétés M_ϕ dont le premier groupe d'homologie est infini :

$$\dim H_1(M_\phi, \mathbf{Z}) \otimes \mathbf{Q} \geqslant 1 \iff (\text{Pour tout } p \text{ premier, } \dim_{\mathbf{Z}/p\mathbf{Z}} H_1(M_\phi, \mathbf{Z}/p\mathbf{Z}) \geqslant 1)$$

(ceci étant valide parce que $H_1(M_\phi, \mathbf{Z})$ est un groupe abélien de type fini).

Il y a en fait une certaine similarité avec le premier exemple : comme l'indiquent Dunfield et Thurston, il y a une description naturelle de l'homologie de M_ϕ, qui est donnée par

$$H_1(M_\phi, \mathbf{Z}) \simeq V/\langle J, \phi_* J\rangle \tag{2}$$

où $V = H_1(\Sigma_g, \mathbf{Z}) \simeq \mathbf{Z}^{2g}$ est le premier groupe d'homologie de la surface Σ_g, J est l'image dans V de $H_1(H_g, \mathbf{Z}) \simeq \mathbf{Z}^g$, tandis que ϕ_* est l'application linéaire induite par ϕ sur V. Notons que J est un sous-espace Lagrangien (fixé !) de V, par rapport à la forme d'intersection sur V (c'est-à-dire que celle-ci est identiquement nulle sur J). En particulier, $H_1(M_\phi, \mathbf{Z})$ ne dépend que de l'application induite ϕ_*, qui est un élément du groupe discret $\mathrm{Sp}(V) \simeq \mathrm{Sp}_{2g}(\mathbf{Z})$ des automorphismes symplectiques de V (pour la forme d'intersection). Et bien évidemment, la réduction modulo p est donnée par

$$H_1(M_\phi, \mathbf{Z}/p\mathbf{Z}) \simeq V_p/\langle J_p, \phi_* J_p\rangle \tag{3}$$

où $V_p = V/pV \simeq \mathbf{F}_p^{2g}$, $J_p = J/pJ \simeq \mathbf{F}_p^g$, qui ne dépend également que de la réduction modulo p de ϕ_*, un élément du groupe fini $\mathrm{Sp}(V/pV) \simeq \mathrm{Sp}_{2g}(\mathbf{Z}/p\mathbf{Z})$.

3. UN SURVOL RAPIDE DU CRIBLE

Dans cette section, nous allons présenter (assez rapidement) les méthodes de crible, et en énoncer le résultat fondamental, dont le principe remonte aux travaux de V. Brun au début du 20ème siècle. L'objectif est de rendre accessible une partie au moins de la littérature concernant le crible, en présentant sa terminologie et ses notations usuelles. Pour cette raison, cette section est rédigée afin d'être lisible indépendamment du reste du texte. C'est seulement dans la suivante que les exemples de la Section 2 – et beaucoup d'autres – seront insérés dans le cadre du crible.

3.1. Crible classique

Les méthodes de crible classiques ont leur origine dans des questions très naturelles concernant les interactions possibles entre des contraintes de type multiplicatives et des propriétés additives des entiers positifs. L'exemple le plus emblématique, qui a motivé V. Brun et beaucoup d'autres arithméticiens depuis, est la conjecture des nombres premiers jumeaux : existe-t-il une infinité de nombres premiers p tels que $p+2$ soit également premier ? Mais la versatilité remarquable du crible l'amène à servir d'outil dans beaucoup d'autres questions. Nous renvoyons, tant pour les détails de la théorie générale que pour de nombreux exemples d'applications, au livre récent de J. Friedlander et H. Iwaniec [16].

Dans leur présentation moderne, les méthodes de crible ont l'objectif suivant : étant donnée une suite[(1)] $\mathcal{F} = (a_n)_{n\geqslant 1}$ de réels positifs (qui, en général, a un support fini, la taille de celui-ci étant un paramètre qui a vocation à tendre vers l'infini), et un ensemble (fixé, en général infini) $\mathcal{P}$ de nombres premiers (par exemple, tous les nombres premiers), on désire comprendre la somme

$$S(\mathcal{F}, z) = \sum_{\substack{n\geqslant 1\\(n,P(z))=1}} a_n, \quad \text{où} \quad P(z) = \prod_{\substack{p\in\mathcal{P}\\p<z}} p,$$

(1) « $\mathcal{F}$ » comme « Folge » en Allemand.

qui donne la contribution à la somme totale

$$S(\mathcal{F}) = \sum_{n \geqslant 1} a_n < +\infty,$$

des entiers qui ne sont divisibles par aucun nombre premier p dans $\mathcal{P}$ qui soit $< z$. Et, crucialement, on souhaite procéder en utilisant des propriétés de la suite donnée qui sont fournies par les *axiomes du crible*, qui portent sur le comportement des sommes de congruence

$$S_d(\mathcal{F}) = \sum_{\substack{n \geqslant 1 \\ n \equiv 0 \pmod{d}}} a_n, \tag{4}$$

pour $d \geqslant 1$ divisible seulement par des nombres premiers dans $\mathcal{P}$.

La relation fondamentale qui rend cela raisonnable est la formule *d'inclusion-exclusion*[(2)]

$$S(\mathcal{F}, z) = \sum_{d | P(z)} \mu(d) S_d(\mathcal{F}),$$

et la philosophie sous-jacente est que, pour beaucoup de suites ayant un grand intérêt arithmétique, les sommes de congruence peuvent être analysées avec succès. La notion de « crible de dimension $\kappa > 0$ » apparaît alors, lorsque la suite $\mathcal{F}$ est telle (intuitivement) que la « densité » parmi les entiers divisibles par un nombre premier p fixé (appartenant à $\mathcal{P}$) est approximativement κp^{-1}. Cela revient à demander que l'on sache écrire

$$S_d(\mathcal{F}) = g(d) S(\mathcal{F}) + r_d(\mathcal{F}), \tag{5}$$

où $r_d(\mathcal{F})$ est un terme de « reste » tandis que g est une fonction multiplicative de $d \geqslant 1$ pour laquelle $g(p)$ vérifie

$$g(p) = \frac{\kappa}{p} + O(p^{-1-\delta}) \tag{6}$$

pour un certain $\delta > 0$ (on peut en fait se contenter de conditions plus faibles, ou valables seulement en moyenne, comme par exemple

$$\sum_{p \leqslant x} g(p) \log p = \kappa \log x + O(1) \ ; \tag{7}$$

puisque on sait que

$$\sum_{p \leqslant x} \frac{\log p}{p} = \log x + O(1),$$

pour $x \geqslant 2$, d'après le Théorème des Nombres Premiers, une telle hypothèse reste consistante avec l'heuristique ci-dessus, interprétée en moyenne sur p).

Cette condition de dimension signifie, le plus souvent, que la somme $S(\mathcal{F}, z)$ correspond aux entiers (dans une suite finie) dont la réduction modulo $p \in \mathcal{P}$ doit éviter κ classes de congruences.

Exemple 3.1. — Un exemple caractéristique est la suite $\mathcal{F}_f = \mathcal{F}_{f,X}$, associée à un polynôme unitaire fixé $f \in \mathbf{Z}[T]$ de degré $r \geqslant 1$ et à un paramètre X (grand), qui est définie comme étant le nombre de représentations

$$a_n = |\{m \leqslant X \mid f(m) = n\}| \tag{8}$$

(2) Où $\mu(d)$ est la fonction de Möbius, valant 0 si d a un facteur carré non-trivial, et égale sinon à $(-1)^{\Omega(n)}$.

d'un entier $n \geqslant 1$ comme valeur $f(m)$ de f avec $m \leqslant X$. Dans ce cas, si $\mathcal{P}$ est l'ensemble de tout les nombres premiers, on trouve

$$S(\mathcal{F}, z) = |\{m \leqslant X \mid f(m) \text{ n'a pas de facteurs premiers } < z\}|, \tag{9}$$

et en particulier, si $z \approx X^{r/2}$, il en découle que

$$S(\mathcal{F}, z) = |\{\text{nombres premiers} \gg X^{r/2} \text{ de la forme } f(m) \text{ avec } m \leqslant X\}|,$$

ce qui est une fonction d'un intérêt arithmétique évident.

Cet exemple montre déjà que, pour être effectif, le crible doit être capable de donner des résultats uniformes par rapport au support de la suite (X ici) et au paramètre z qui détermine les nombres premiers intervenant effectivement dans le crible ; en effet, dans les applications les plus intéressantes, z sera nécessairement une fonction de X.

Quoi qu'il en soit, on voit tout de suite dans cet exemple que les sommes de congruence sont plus faciles à comprendre. Par définition, on a

$$S_d(\mathcal{F}_{f,X}) = \sum_{\substack{m \leqslant X \\ d \mid f(m)}} 1,$$

et l'on peut reformuler cette somme en exploitant la périodicité de $f(m)$ modulo d. En sommant d'abord sur les entiers m dans une classe donnée modulo d, et en notant

$$\rho_f(d) = |\{\alpha \in \mathbf{Z}/d\mathbf{Z} \mid f(\alpha) \equiv 0 \pmod{d}\}|$$

le nombre de racines de f modulo d, on trouve

$$S_d(\mathcal{F}_{f,X}) = \sum_{\substack{\alpha \in \mathbf{Z}/d\mathbf{Z} \\ f(\alpha) = 0 \pmod{d}}} \sum_{\substack{m \leqslant X \\ m \equiv \alpha \pmod{d}}} 1 = \frac{\rho_f(d)}{d} X + O(1) \tag{10}$$

pour $X \geqslant 2$, où la constante implicite dépend de f seulement. D'après le Théorème des Restes Chinois, l'application $d \mapsto \rho_f(d)$ est effectivement multiplicative. D'après le théorème de densité de Chebotarev (qui est nécessaire dans le cas général, mais peut être évité lorsque $f(T) = (T - a_1) \cdots (T - a_r)$ est complètement scindé sur $\mathbf{Z}$, un cas important puisqu'il correspond à la conjecture de Hardy-Littlewood[(3)]), on sait que

$$\sum_{p \leqslant x} \frac{\rho_f(p)}{p} = \kappa \log\log x + O(1),$$

où $\kappa = \kappa(f)$ est le nombre de facteurs irréductibles distincts de f in $\mathbf{Q}[T]$. Ainsi, on est ici dans le cas d'un crible de dimension κ. (Par exemple, pour $f(T) = T^2 + 1$, on a $\kappa = 1$: en moyenne sur p, il existe une racine carrée de -1 dans $\mathbf{Z}/p\mathbf{Z}$.)

Un énoncé général de crible prend alors la forme suivante (voir [16, Th. 11.13], où se trouvent davantage de détails ; cette version est un théorème difficile) :

---

(3) Dont on peut rappeler qu'elle joue un rôle important dans les travaux récents de Goldston, Pintz et Yıldırım au sujet des écarts entre nombres premiers successifs.

THÉORÈME 3.2. — *Avec les notations ci-dessus, pour un problème de crible de dimension $\kappa > 0$, il existe un nombre réel $\beta(\kappa) > 0$ tel que l'on ait*

$$(f(s)+O(\log D)^{-1/6}))S(\mathcal{F})\prod_{p|P(z)}(1-g(p))+R(D)\leqslant S(\mathcal{F},P)$$
$$\leqslant (F(s)+O((\log D)^{-1/6})S(\mathcal{F})\prod_{p|P(z)}(1-g(p))+R(D)$$

lorsque $z = D^{1/s}$ avec $s > \beta(\kappa)$, où $F(s) > 0$ et $f(s) > 0$ sont des fonctions de $s \geqslant 0$, dépendant de κ, définies comme solutions d'équations différentielles aux différences explicites, telles que

$$\lim_{s\to+\infty} f(s) = \lim_{s\to+\infty} F(s) = 1,$$

et où

$$R(D) = \sum_{d<D} |r_d(\mathcal{F})|.$$

Les constantes implicites dans les bornes inférieures et supérieures dépendent seulement de κ et des constantes dans l'asymptotique (6)*, ou sa variante en moyenne.*

Le terme dominant dans les deux estimations (quand $s \to +\infty$) a une signification intuitive claire : une condition de congruence modulo un seul nombre premier $p \in \mathcal{P}$ est satisfaite par une proportion $1-g(p)$ de la somme totale $S(\mathcal{F})$; puis des conditions de congruences répétées se comportent (asymptotiquement) comme si elles étaient indépendantes.

En particulier, dès que les termes de reste dans (5) sont petits pour d fixé, on en déduit une formule asymptotique concernant le crible avec un ensemble *fixé* de nombres premiers, lorsque le support de la suite $\mathcal{F}$ grandit.

L'ordre de grandeur du terme dominant est facile à déterminer : puisque $g(p) \approx \kappa p^{-1}$ (en moyenne au moins), la formule de Mertens[4] montre que

$$\prod_{p|P(z)}(1-g(p)) \asymp \frac{1}{\log X}$$

pour $z = X^{1/s}$ et tout $s > 0$ fixé. La définition qui suit est donc une expression naturelle du fait que, pour que le Théorème 3.2 donne un bon résultat, il est nécessaire que le terme de reste R soit d'un ordre de grandeur plus petit.

DÉFINITION 3.3 (Niveau de distribution). — *Soit $(\mathcal{F}_n)$ des suites comme ci-dessus, et $D_n > 0$. Alors $\mathcal{F}_n$ ont* niveau de distribution $\geqslant D_n$ *si*

$$R_n = \sum_{d<D_n} |r_d(\mathcal{F}_n)| \ll S(\mathcal{F}_n)(\log D_n)^{-B} \tag{11}$$

pour tout $B > 0$ et $n \geqslant 2$, la constante implicite dépendant de B.

Exemple 3.4. — Dans le contexte de l'Exemple 3.1, pour $f \in \mathbf{Z}[T]$ de degré $r \geqslant 1$, avec κ facteurs irréductibles, on a

$$r_d(\mathcal{F}_{f,X}) \ll d^{\varepsilon}$$

pour tout $d \geqslant 1$ sans facteurs carrés et $\varepsilon > 0$, la constante implicite dépendant de ε. Puisque $S(\mathcal{F}_{f,X}) \asymp X$, on voit que le niveau de distribution est $\geqslant D$ pour tout $D = X^{1-\delta}$ avec $\delta > 0$.

[4] On suppose ici que $\mathcal{P}$ contient tout les nombres premiers, avec peu d'exceptions.

Appliquant le Théorème 3.2 avec $z = D^{1/s}$, s assez grand, on déduit qu'il existe $r(f) \geqslant 1$ tel qu'il existe une infinité de nombres entiers m tels que $f(m)$ a au plus $r(f)$ facteurs premiers, comptés avec multiplicité (en fait, on déduit qu'il existe au moins $\gg X/(\log X)^{\kappa}$ tels entiers $m \leqslant X$).

3.2. Crible et principe local-global

Le point de vue de la section précédente est extrêmement efficace, et est utilisé dans toutes les présentations modernes du crible (par exemple [16]). Cependant, dans beaucoup d'applications, il est possible d'utiliser une description qui est essentiellement équivalente, mais d'aspect (peut-être) plus naturel.

Dans cette seconde approche, on considère un ensemble Y d'objets de nature « globale » (souvent, mais pas forcément nécessairement, arithmétique). Pour les étudier, on suppose données des applications

$$Y \to Y_p$$

pour p premier, qui servent d'analogue aux applications de réduction modulo p pour les entiers (et qui sont souvent définies de cette manière). Pour renforcer cette intuition, on écrira $y \pmod p$ pour l'image de $y \in Y$ dans Y_p. On pense à ces applications comme donnant des informations « locales » sur les objets de Y ; on suppose par ailleurs que Y_p est un ensemble fini, et bien que $Y \to Y_p$ soit souvent surjective, il est parfois plus pratique de ne pas l'imposer pour que Y_p soit défini plus naturellement.

On peut maintenant construire des ensembles « criblés » à partir de ces données, d'un ensemble $\mathcal{P}$ de nombres premiers, d'une borne $z \geqslant 2$, et d'ensembles de conditions de crible $\Omega_p \subset Y_p$, à savoir :

$$\mathcal{S}_z(Y;\Omega) = \{y \in Y \mid y \pmod p \notin \Omega_p \text{ pour tout } p \in \mathcal{P},\ p < z\} \subset Y. \tag{12}$$

Pour compter les éléments de cet ensemble criblé, on considère assez généralement une mesure finie μ sur Y, et le problème auquel on va s'attaquer est celui d'estimer la mesure $\mu(\mathcal{S}_z(Y;\Omega))$ de l'ensemble criblé.[5]

Cette question est alors une variante des problème de crible. Pour le voir, on définit

$$n(y) = \prod_{\substack{p\in\mathcal{P}\\ y \pmod p\in\Omega_p}} p$$

pour $y \in Y$, avec $n(y) = 0$ par convention si le produit est infini. C'est un entier $\geqslant 0$, tel que la propriété « d'adjonction »

$$(p \mid n(y)) \Longleftrightarrow (y \pmod p \in \Omega_p)$$

est valide pour tout $p \in \mathcal{P}$ si $n(y) \geqslant 1$.

Le cas où $n(y) = 0$ est, généralement, exceptionnel,[6] mais il peut se produire. On pose

$$Y^0 = \{y \in Y \mid n(y) = 0\}, \qquad Y^+ = Y - Y^0,$$

pour en tenir compte.

---

[5] Il ne devrait pas y avoir de confusion avec la fonction de Möbius.

[6] Dans les questions de comptage considérées dans ce survol, il représentera une contribution négligeable.

On définit alors la suite $\mathcal{F} = (a_n)$ en posant[7]

$$a_n = \mu(\{y \in Y \mid n(y) = n\}), \tag{13}$$

et il en découle que

$$S(\mathcal{F}) = \sum_{n \geqslant 1} a_n = \mu(Y^+),$$

tandis que

$$S(\mathcal{F}, z) = \sum_{(n,P(z))=1} a_n = \mu\Big(\{y \in Y \mid (n(y), P(z)) = 1\}\Big) = \mu(\mathcal{S}_z(Y^+; \Omega)).$$

Exemple 3.5. — On peut facilement interpréter l'Exemple 3.1 de cette manière. Ici, on prend pour Y l'ensemble des entiers naturels, μ est la mesure de comptage restreinte aux entiers $1 \leqslant m \leqslant X$, les applications de réduction modulo p sont les applications évidentes dans $Y_p = \mathbf{Z}/p\mathbf{Z}$. Si l'on choisit

$$\Omega_p = \{\alpha \in \mathbf{Z}/p\mathbf{Z} \mid f(\alpha) = 0\},$$

l'ensemble des zéros de f modulo p, il est clair que

$$\mu(\mathcal{S}_z(Y; \Omega)) = S(\mathcal{F}, z)$$

est la quantité définie par (9).[8]

Revenant au cas général, les sommes de congruences $S_d(\mathcal{F})$ sont données par

$$S_d(\mathcal{F}) = \mu(\{y \in Y^+ \mid y \pmod p \in \Omega_p \text{ pour tout } p \mid d\})$$

pour d sans facteurs carrés divisant $P(z)$. C'est aussi la mesure de l'ensemble

$$\Omega_d = \prod_{p|d} \Omega_p \subset \prod_{p|d} Y_p,$$

calculée à l'aide de l'image de la mesure μ par l'application

$$Y^+ \longrightarrow Y_d = \prod_{p|d} Y_p$$

de réduction simultanée modulo tout les $p \mid d$.

Cette interprétation suggère de considérer la condition de crible (5) et le fait que le reste $r_d(\mathcal{F})$ soit sensé être « petit » comme l'expression d'une propriété *d'equirépartition locale*, et *d'indépendance* des réductions de Y modulo les nombres premiers : on s'attend d'abord à ce que, pour p fixé, on puisse écrire

$$\mu(\{y \in Y \mid y \pmod p = \alpha\}) \approx \mu(Y)\nu_p(\alpha)$$

pour tout $\alpha \in Y_p$, pour une mesure de probabilité ν_p sur l'ensemble fini Y_p; puis, on s'attend à ce que les réductions modulo $p \mid d$ soient approximativement indépendantes, ce qui implique

$$\mu(\{y \in Y \mid y \pmod p = \alpha_p \text{ pour tout } p \mid d\}) \approx \mu(Y) \prod_{p|d} \nu_p(\alpha_p). \tag{14}$$

En comparant avec (5), on en déduit que l'on doit prendre

$$g(p) = \nu_p(\Omega_p), \qquad g(d) = \prod_{p|d} \nu_p(\Omega_p),$$

---

[7] On suppose évidemment que les ensembles $\{y \in Y \mid y \pmod p = \alpha\}$ sont tous mesurables.

[8] Ici, Y^+ est l'ensemble des entiers $m \leqslant X$ tels que $f(m) \neq 0$; en particulier, Y^0 est un ensemble fini.

ce qui correspond bien à l'idée intuitive que $g(d)$ donne la « densité » de la suite restreinte aux entiers divisibles par d, la multiplicativité de la fonction g étant alors pratiquement équivalence à la propriété d'indépendance asymptotique (14).

Nous donnons maintenant une définition précise des conditions d'approximation (14) et du niveau de distribution dans ce cadre. Il est alors préférable de considérer explicitement une situation asymptotique, et on supposera donc que l'on a une suite (μ_n) de mesures finies sur Y, non-triviales ($\mu_n(Y) > 0$) et l'intérêt principal sera la limite $n \to +\infty$ (cela correspond au paramètre $n = X \to +\infty$ dans l'Exemple 3.1).

Pour tout d sans facteurs carrés (divisible seulement par des nombres premiers $p \in \mathcal{P}$), on définit alors la mesure de probabilité $\tilde{\mu}_{n,d}$ sur

$$Y_d = \prod_{p|d} Y_d,$$

comme étant l'image de la mesure de probabilité

$$\tilde{\mu}_n = \mu_n/\mu_n(Y) \tag{15}$$

sous l'application naturelle $Y \longrightarrow Y_d$.

Définition 3.6 (Hypothèses de crible). — *Les hypothèses du crible avec niveau $D_n \geqslant 1$ sont satisfaites pour Y et la suite (μ_n) de mesures sur Y si les conditions suivantes sont vérifiées :*

(1) [Équirépartition locale et indépendance] *Pour tout d sans facteurs carrés comme ci-dessus, les mesures $\tilde{\mu}_{n,d}$ convergent vers une mesure de probabilité ν_d, telle que*

$$\nu_d = \prod_{p|d} \nu_p.$$

Autrement dit, il existe des mesures de probabilité ν_d sur Y_d telles que

$$\mu_n(\{y \in Y \mid y \pmod p = \alpha_p\}) = \mu_n(Y)(\nu_d(\alpha) + r_{d,n}(\alpha))$$

pour tout d et $\alpha = (\alpha_p)_{p|d} \in Y_d$, avec

$$\lim_{n\to+\infty} r_{d,n}(\alpha) = 0$$

pour tout d fixé et $\alpha \in Y_d$.

(2) [Niveau de distribution] *Étant donnés des ensembles $\Omega_p \subset Y_p$, et*

$$\Omega_d = \prod_{p|d} \Omega_p,$$

pour d sans facteurs carrés, on a

$$\sum_{d<D_n} |\Omega_d| \max_\alpha |r_{d,n}(\alpha)| \ll (\log D_n)^{-A}, \tag{16}$$

$$\mu_n(Y^0) \ll \mu_n(Y)(\log D_n)^{-A} \tag{17}$$

pour tout $n \geqslant 1$ et $A \geqslant 1$, les constantes implicites dépendant de A et des Ω_p.

Ces hypothèse reflètent des propriétés d'équirépartition quantitative et uniforme pour les réductions des objets globaux de Y. La difficulté dans le crible en orbites (par exemple dans le cas de l'exemple de la Section 2.1 ou plus généralement tel qu'il sera décrit dans la prochaine section) se situe au niveau de la vérification que ces conditions sont valides (avec un niveau

de distribution suffisamment grand). Dans la suite de ce texte, on présentera certaines des idées et des techniques qui permettent de les obtenir.

Quoi qu'il en soit, si l'on admet que les Hypothèses de crible sont valides, on peut les combiner avec le théorème fondamental du crible, et en déduire le fait général suivant. Étant donnés les ensembles de conditions $\Omega_p \subset Y_p$, tels que

$$\nu_p(\Omega_p) = \frac{\kappa}{p} + O(p^{-1-\delta}) \tag{18}$$

(ce qui est une condition locale, indépendante de Y) pour tout $p \in \mathcal{P}$ et un certain $\delta > 0$ fixé, on obtient en sommant sur $\alpha \in \Omega_p$ que les sommes de congruence vérifient

$$\mu_n(y \in Y \mid y \pmod p \in \Omega_p \text{ pour } p \mid d) = \mu_n(Y)\nu_d(\Omega_d) + r_{d,n}(\Omega)$$

avec

$$r_{d,n}(\Omega) \ll |\Omega_d| \max_{\alpha \in Y_d} |r_{d,n}(\alpha)|.$$

D'après la propriété d'indépendance, $g(d) = |\Omega_d|$ est une fonction multiplicative de d. Affaiblissant la conclusion du Théorème 3.2 pour obtenir un énoncé plus simple, on trouve que

$$\mu_n(\{y \in Y \mid y \pmod p \notin \Omega_p \text{ pour tout } p < D_n^{1/s}\}) \asymp \frac{\mu_n(Y)}{(\log D_n)^\kappa} \tag{19}$$

pour $n \geqslant 1$, lorsque s est fixé et est assez grand (en terme de κ).

Exemple 3.7. — Cela s'applique sans difficultés aux Exemples 3.1 et 3.5, en prenant la suite (μ_X) de mesures de comptage sur $1 \leqslant m \leqslant X$. La mesure ν_p est alors simplement la mesure de probabilité uniforme sur $\mathbf{Z}/p\mathbf{Z}$, reflétant la formule

$$|\{m \leqslant X \mid m \equiv \alpha \pmod p\}| = \frac{X}{p} + O(1),$$

et l'indépendance (qui passe presque inaperçue ici) est valide, et revient plus ou moins au Théorème des Restes Chinois : si l'on connaît la réduction modulo un nombre premier p_1 d'un entier « générique » n, on ne peut en déduire aucune information particulière concernant la réduction de n modulo $p_2 \neq p_1$. Quantitativement, comme

$$|\{m \leqslant X \mid m \equiv \alpha \pmod d\}| = \frac{X}{d} + O(1),$$

on a (avec les notations de la Définition 3.6) la borne uniforme

$$r_{d,X}(\alpha) \ll X^{-1},$$

et donc on retrouve le niveau de distribution $D \leqslant X^{1-\delta}$ avec $\delta > 0$ fixé de l'Exemple 3.4. La condition (17) est ici triviale, puisque Y^0 est l'ensemble fini des racines de f qui sont des entiers positifs. La situation est ici la meilleure que l'on puisse espérer avoir, et dans les exemples de crible en expansion, on sera loin d'avoir un niveau de distribution aussi grand.

Remarque 3.8. — La majoration (17) est, dans tout les cas présentés ici, obtenue comme conséquence de (16). Il sera en effet toujours vrai (comme dans l'exemple précédent) que $n(y) = 0$ correspond à $y \pmod p \in \Omega_p$ pour *tout* p. On peut alors majorer

$$\mu_n(Y^0) \leqslant \mu_n(\{y \in Y \mid y \pmod p \in \Omega\})$$

pour tout p, et sous les hypothèses ci-dessus, on trouve pour tout $p \leqslant D_n$ que

$$\mu_n(Y^0) \leqslant \mu_n(Y)\Big\{\nu_p(\Omega_p) + O(|\Omega_p| \max_{\alpha\in\Omega_p} |r_{p,n}(\alpha)|)\Big\}$$
$$\ll \mu_n(Y)\Big\{\frac{1}{p} + O((\log D_n)^{-A})\Big\}$$

et on peut prendre p de taille comparable à $(\log D_n)^A$ pour conclure.

4. CRIBLE EN ORBITES

On peut maintenant décrire la version générale du problème de crible développé par Bourgain, Gamburd et Sarnak (qu'on appellera « crible en orbites »), dont la Section 2.1) est un cas particulier. Comme le groupe $\mathcal{A}$, les entiers ou objets globaux concernés sont directement liés à des groupes discrets à croissance exponentielle. L'exemple de la Section 2.2 n'entre pas directement dans ce cadre ; il sera repris dans la Section 6.1.

4.1. Le cadre général

Soit $\Lambda \subset \mathrm{GL}_m(\mathbf{Z})$ un sous-groupe de type fini, pour un certain $m \geqslant 2$ (comme, $\mathcal{A} \subset \mathrm{GL}_4(\mathbf{Z})$, le groupe de Lubotzky L défini par (1) dans $\mathrm{SL}_2(\mathbf{Z})$, ou bien $\mathrm{SL}_m(\mathbf{Z})$, puisque il est bien connu que ce groupe est de type fini).

Étant donné un vecteur non-nul $x_0 \in \mathbf{Z}^m$, on forme l'orbite

$$\mathcal{O}(x_0) = \Lambda \cdot x_0 \subset \mathbf{Z}^m$$

de x_0 sous l'action linéaire de Λ, on fixe une fonction polynômiale $f \in \mathbf{Q}[X_1, \dots, X_m]$ telle que f prenne seulement des valeurs entières sur $\mathcal{O}(x_0)$ (par exemple, $f \in \mathbf{Z}[X_1, \dots, X_m]$, qui pourrait être le produit des coordonnées). La question sous-jacente est alors

« Les $f(x) \in \mathbf{Z}$, où $x \in \mathcal{O}(x_0)$, sont-ils des entiers typiques ? »

Puisqu'il s'agit ici d'utiliser le crible, la question sera plus exactement : est-ce que les propriétés multiplicatives (nombre et distribution des facteurs premiers) des $f(\gamma x_0)$ est différente de celle des entiers en général ?[(9)]

Dans l'approche de la Section 3.2, on considère donc l'ensemble

$$Y = \mathcal{O}(x_0),$$

et les applications de réduction

$$Y \to Y_p = \mathcal{O}(x_0 \pmod p),$$

modulo les nombres premiers, l'image étant l'orbite de l'image de $x_0 \pmod p$ sous l'action du sous-groupe

$$\Lambda_p \subset \mathrm{GL}_m(\mathbf{Z}/p\mathbf{Z})$$

qui est l'image de Λ par réduction modulo p. (Il peut être utile de rappeler d'emblée que si $\Lambda = \mathrm{SL}_m(\mathbf{Z})$, on a $\Lambda_p = \mathrm{SL}_m(\mathbf{Z}/p\mathbf{Z})$ pour tout nombre premier p, ce que l'on voit par exemple en utilisant les matrices élémentaires comme générateurs.)

[(9)] Un Appendice à ce rapport donne un rappel rapide de ce que sont ces propriétés « typiques » pour les entiers eux-mêmes.

Remarque 4.1. — Il est possible d'étudier d'autres actions de Λ ; par exemple, il est tout aussi naturel – et en fait souvent plus pratique – de se ramener à prendre $Y = \Lambda$, avec $Y_p = \Lambda_p$ comme précédemment, et la fonction sur Λ donnée par

$$\gamma \mapsto f(\gamma \cdot x_0).$$

Mais si l'on considère l'image de Λ dans $\mathrm{GL}_{m^2}(\mathbf{Z})$ donnée par l'action de multiplication à gauche de Λ sur $M_m(\mathbf{Z}) \simeq \mathbf{Z}^{m^2}$, on peut noter que Λ s'identifie naturellement avec l'orbite du vecteur x_0 qui est la matrice identité dans $M_m(\mathbf{Z})$, et de même pour les réductions modulo p.

On décrira dans la section suivante comment « compter » les éléments de Y pour appliquer les méthodes de crible. Suivant [4], il existe auparavant une manière qualitative élégante de présenter l'énoncé (attendu dans beaucoup de cas) qu'il existe « beaucoup » de $x \in \mathcal{O}(x_0)$ tels que $f(x)$ ait peu de facteurs premiers. Pour $r \geqslant 1$, soit

$$\mathcal{O}_f(x_0; r) = \{x \in \mathcal{O}(x_0) \mid \Omega(f(x)) \leqslant r\}$$

et définissons (suivant [4]) le « nombre de saturation » de l'orbite par

$$r(f, \Lambda) = \min\{r \geqslant 1 \mid \mathcal{O}_f(x_0; r) \text{ et } \mathcal{O}(x_0) \text{ ont la même adhérence de Zariski}\},$$

ou, en d'autres termes, le plus petit $r \geqslant 1$ (s'il existe) tel que les éléments de $\mathcal{O}_f(x_0; r)$ ne satisfont à aucune identité poynômiale autre que celles qui sont valides pour toute l'orbite $\mathcal{O}(x_0)$. La question naturelle devient :

Question 4.2. — *Le nombre de saturation est-il fini ? Si oui, quelle est sa valeur ?*

Exemple 4.3. — Pour $m = 1$, un ensemble d'entiers dans $\mathbf{Z}$ est soit fermé au sens de la topologie de Zariski, s'il est fini, soit dense (en ce sens) dans la droite affine entière. La finitude du nombre de saturation pour une orbite infinie $\mathcal{O} \subset \mathbf{Z}$ revient donc simplement à dire qu'il existe $r \geqslant 1$, tel que $\mathcal{O}$ contienne *une infinité d'entiers* ayant au plus r facteurs premiers, avec multiplicité.

Par contre, dès que $m \geqslant 2$, la condition de saturation devient plus subtile et donc plus intéressante. L'exemple suivant est détaillé dans [4, §6,Ex. C] : soit $\mathcal{O}$ l'orbite de $x_0 = (3, 4, 5)$ sous l'action du groupe orthogonal $\Lambda = \mathrm{SO}(2, 1)(\mathbf{Z})$. Cette orbite est l'ensemble des triplets Pythagoriciens entiers, et son adhérence de Zariski est le cône $\{x^2 + y^2 - z^2 = 0\}$. Si l'on considère alors la fonction $f(x, y, z) = xy/2$ (l'aire du triangle rectangle associé à (x, y, z)), Bourgain, Gamburd et Sarnak montrent à l'aide des résultats quantitatifs de Green et Tao [25] concernant le nombre de progressions arithmétiques de longueur 4 parmi les nombres premiers, que le nombre de saturation est 6 dans ce cas. Cependant, il est extrêmement probable (ce découlerait en particulier de certaines des conjectures de Hardy et Littlewood) qu'il existe une infinité de triangle rectangles à côtés entiers dont l'aire ait au plus 5 facteurs premiers. Mais les longueurs des côtés de ces triangles satisfont des relations polynômiales supplémentaires...

Il semble intéressant de renforcer un peu la condition de saturation en remplaçant la condition de densité pour la topologie de Zariski par la condition, plus forte, que $\mathcal{O}_f(x_0; r)$ *ne soit pas mince*. Rappelons la définition (voir [57, §3.1]) :

Définition 4.4 (Ensemble mince). — *Soit V/k une variété algébrique irréductible définie sur un corps k de caractéristique* 0. *Un ensemble $A \subset V(k)$ est* mince *s'il existe un morphisme k-rationnel $W \xrightarrow{f} V$ de variétés algébriques avec* $\dim(W) \leqslant \dim(V)$, *tel que*

$$A \subset f(W(k)),$$

et tel que f n'ait pas de section k-rationnelle.

Exemple 4.5. — Il existe beaucoup d'ensembles infinis (donc dense pour la topologie de Zariski) dans $\mathbf{Z}$ qui sont cependant minces (dans la droite affine). On peut toutefois montrer qu'un tel ensemble (noté $\mathcal{T}$) vérifie nécessairement une estimation

$$|\{n \in \mathcal{T} \mid |n| \leqslant X\}| \ll X^{1/2}(\log X)$$

pour $X \geqslant 2$ (un résultat de S.D. Cohen, voir, par exemple, [57, Th. 3.4.4]). Ainsi, les bornes élémentaires de Chebychev (ou même l'étude quand $\sigma \to 1$ de la fonction zêta

$$\prod_p (1 - p^{-\sigma})^{-1} = \sum_{n \geqslant 1} \frac{1}{n^\sigma} \sim \frac{1}{\sigma - 1}$$

dans l'esprit d'Euler) suffisent à montrer que l'ensemble des nombres premiers n'est pas mince dans la droite affine. L'exemple de l'ensemble des carrés parfaits montre que l'exposant $1/2$ est le meilleur possible dans une telle borne.

Le Théorème 1.1 signifie donc, pour certains groupes Λ et leurs orbites, que le nombre de saturation est fini, même avec la condition que $\mathcal{O}_f(x_0; r)$ ne soit pas mince (dans l'adhérence de Zariski de l'orbite entière). On présentera ci-dessous l'esquisse de la preuve de ce résultat, y compris pour des groupes plus généraux. Il est intéressant de noter que, bien que [4] ne considère que la condition de saturation initiale, les valeurs de r qu'ils obtiennent telles que $\mathcal{O}_f(x_0; r)$ soit Zariski-dense ont également la propriété que cet ensemble n'est pas mince.

4.2. Comment compter ?

Le crible en orbites donne de nombreux exemples d'ensembles Y avec des applications de réduction $Y \to Y_p$ pour lesquelles il est souhaitable de pouvoir appliquer le crible (par exemple pour montrer qu'un certain nombre de saturation est fini). Ainsi que la Section 3.2 l'a montré, il faut pour cela préciser comment compter les éléments de Y, plus précisément, pour quelles mesures finies μ_n sur Y on va s'efforcer de vérifier les hypothèses de crible (Définition 3.6).

Contrairement au crible classique, où le comptage ne pose guère de problèmes, une caractéristique du crible en expansion est qu'il existe deux ou trois (ou plus) manières naturelles de compter les éléments de Y. Nous illustrons cela dans le cas où $Y = \Lambda$ est un sous-groupe de type fini de $\mathrm{GL}_m(\mathbf{Z})$. On peut en effet alors utiliser:

– [Boules archimédiennes] On peut fixer une norme $\|\cdot\|$ sur $\mathrm{GL}_m(\mathbf{R})$, et définir μ_X comme la mesure de comptage sur l'ensemble fini

$$B_\Lambda(X) = \{g \in \Lambda \subset \mathrm{GL}_m(\mathbf{R}) \mid \|g\| \leqslant X\},$$

pour $X \geqslant 1$ (qui ensuite tendra vers l'infini).

– [Boules combinatoires] On peut aussi fixer à la place un ensemble fini de générateurs S, souvent symétrique (c'est-à-dire que $s \in S$ implique $s^{-1} \in S$), et l'utiliser pour définir une norme combinatoire par la longueur minimale des mots représentant un élément :

$$\|g\|_S = \min\{k \geqslant 0 \mid g = s_1 \cdots s_k \text{ pour certains } s_1, \ldots, s_k \in S\}.$$

Cela permet de considérer la mesure de comptage μ_k sur la boule combinatoire finie

$$B_S(k) = \{g \in \Lambda \mid \|g\|_S \leqslant k\}$$

où le paramètre asymptotique est maintenant un entier $k \geqslant 1$. Bien entendu, cet ensemble dépend de S, mais on peut s'attendre à ce que certaines propriétés robustes soient indépendantes du choix de S.

– [Marches aléatoires] Au lieu de la mesure de probabilité uniforme sur la boule combinatoire ci-dessus, il peut être pratique d'utiliser un poids approprié sur ses éléments, qui prend en compte la multiplicité des représentations d'un élément comme mot de longueur k. Plus précisément, on suppose que $1 \in S$ (on peut remplacer S par $S \cup \{1\}$ si besoin est), et on considère le mesure de probabilité μ_k sur Λ définie par

$$\mu_k(g) = \frac{1}{|S|^k} \sum_{\substack{(s_1,\dots,s_k)\in S^k \\ s_1\cdots s_k = g}} \cdots \sum 1$$

(la condition $1 \in S$ assure que le support de cette mesure est bien la boule combinatoire de rayon k, et non pas seulement la sphère combinatoire).

L'intérêt de cette pondération est qu'elle permet de simplifier toute moyenne sur $B_S(k)$ en rendant *indépendantes* les variables de sommations $s_1, \dots, s_k \in S$: on a

$$\sum_{g\in\Lambda} \varphi(g)\mu_k(g) = \frac{1}{|S|^k} \sum_{s_1,\dots,s_k\in S} \cdots \sum \varphi(s_1 \cdots s_k),$$

pour toute fonction φ sur Λ, où les variables de sommation à droite sont « libres »: aucune relation n'intervient entre elles.

Remarque 4.6. — Cette troisième mesure a une interprétation probabiliste naturelle : la mesure μ_k est la loi du k-ème pas de la marche au hasard $(X_k)_{k\geqslant 0}$ sur Λ définie par

$$X_0 = 1 \in \Lambda \quad X_{k+1} = X_k\xi_{k+1},$$

où $(\xi_k)_{k\geqslant 1}$ est une suite de variables aléatoires indépendantes et uniformément distribuées (sur un espace probabilisé fixé $(\Omega, \Sigma, \mathbf{P})$ convenable) à valeurs dans S, telles que

$$\mathbf{P}(\xi_k = s) = \frac{1}{|S|} \quad \text{pour tout } k \geqslant 1 \text{ et } s \in S.$$

Revenant au cas général, une fois fixée la façon de compter, c'est-à-dire une suite de mesures. notée (μ_X), la forme plus précise de la Question 4.2 est de borner (par excès ou par défaut) la fonction

$$\pi_f(X; r) = \mu_X(\gamma \in \Lambda \mid \Omega(f(\gamma \cdot x_0)) \leqslant r)$$

lorsque $X \to +\infty$. L'idée est de prouver une minoration asymptotique de $\pi_f(X; r)$ (pour r convenable et $X \to +\infty$) qui soit suffisante pour garantir que la densité de l'ensemble $\mathcal{O}_f(x_0; r)$ (pour la topologie de Zariski, ou le fait qu'il ne soit pas mince), par comparaison avec une *majoration* pour la fonction

$$\mu_X(\gamma \in \Lambda \mid f(\gamma \cdot x_0) \in W)$$

associée à une sous-variété fermée propre $W \subset V = \overline{\mathcal{O}(x_0)}$ (ou à un ensemble mince $W \subset V(\mathbf{Q})$).

5. LES HYPOTHÈSES FONDAMENTALES

Considérons un groupe Λ et une orbite $\mathcal{O}(x_0)$ comme dans le crible en orbites de la section précédente, et supposons choisie une manière de compter (donc une suite (μ_X) de mesures sur Y). Nous essayons maintenant de vérifier si les Hypothèses Fondamentales du crible (au sens de la Définition 3.6) sont satisfaites.

Pour cela, nous ferons d'abord l'hypothèse suivante, qui sera raffinée plus bas, au moment d'énoncer un résultat crucial (Théorème 5.4, qui expliquera sans doute mieux la nature de cette hypothèse pour certains lecteurs):

HYPOTHÈSE 5.1. — *L'adhérence de Zariski $G/\mathbf{Q}$ du groupe $\Lambda \subset \mathrm{GL}_m(\mathbf{Z})$ est un* groupe semisimple*, par exemple, SL_m, ou Sp_{2g}, ou un groupe orthogonal, ou un produit de tels groupes.*

Par exemple, cela signifie que l'on exclut entièrement des considérations ci-dessous un groupe tel que celui engendré par l'élément unique $2 \in \mathrm{GL}_1(\mathbf{Z}[1/2])$ et son orbite $\{2^n\} \subset \mathbf{Z}[1/2]$ (ici l'anneau de base est $\mathbf{Z}[1/2]$, au lieu de $\mathbf{Z}$). On peut comprendre pourquoi: trouver des entiers n tels que, par exemple, la fonction $f(2^n) = 2^n - 1$, soit un nombre premier ou presque premier, est un problème très mal compris, même du point de vue heuristique. Le crible est inapplicable, tout simplement parce que les résultats de base qui sont absolument nécessaires pour comprendre les informations locales provenant des applications de réduction $\Lambda \to \Lambda_p$ ne sont pas valides dans ce cas ! (Voir la Remarque 5.6 ci-dessous, et voir aussi dans [4, §2] d'autres exemples qui montrent pourquoi on ne peut pas s'attendre à une bonne théorie de crible lorsque l'adhérence de Zariski de Λ est un groupe réductif non-semisimple, par exemple).

Pour la même raison, les groupes résolubles (par exemple, Λ dense dans le groupe des matrices triangulaires supérieures) doivent être évités ; les groupes nilpotents, par contre, sont bien souvent accessibles à des méthodes plus classiques, et leur croissance polynômiale est plus facile à contrôler, et ne requiert pas les résultats d'expansion mentionnés ci-dessous. On peut donc voir le cas semisimple comme étant le cas critique.

5.1. Mesures limites locales

Conformément à la recette de la Section 3.2, on commence par vérifier si, pour un entier d fixé (sans facteurs carrés), les mesures images $\tilde{\mu}_{X,d}$ (définies par (15)) sur

$$\Lambda_d = \prod_{p|d} \Lambda_p,$$

convergent, et si oui, si la mesure limite ν_d est la mesure produit des mesures ν_p, $p \mid d$. Cette dernière condition est cruciale, et il est parfois nécessaire d'effectuer des arrangements préliminaires pour s'assurer qu'elle puisse être vérifiée. La difficulté est illustrée par la situation suivante : supposons que, pour un certain ensemble Z, il existe des applications (non constantes)

$$N : Y \to Z, \qquad N_p : Y_p \to Z,$$

telles que

$$N(y) = N_p(y \pmod p)$$

pour tout nombre premier p. Alors, la réduction $y \pmod p$ révèle la valeur de $N(y)$, et par conséquent, la réduction modulo p ne peut être asymptotiquement indépendante de celle

modulo un autre nombre premier : il n'est pas possible que $y \pmod{p_1 p_2}$ soit équiréparti avec une mesure limite qui soit une mesure produit.

Exemple 5.2. — La situation décrite peut se produire dans le crible en orbites, en particulier lorsque des groupes orthogonaux sont concernés. Ainsi, le groupe $\mathcal{A}$ n'est pas contenu dans $\mathrm{SO}(Q, \mathbf{Z})$, et on a

$$\det(\gamma) = \det(\gamma \pmod{p}) \in \{\pm 1\}$$

pour tout p, de sorte que l'on peut prendre $Z = \{\pm 1\}$ et $N(\gamma) = \det(\gamma)$. Et même pour $\mathcal{A} \cap \mathrm{SO}(Q, \mathbf{Z})$, il existe une obstruction à l'indépendance, due à la « norme spinorielle ».

La présence de tels obstacles ne doit pas être interprétée comme un problème sérieux dans une tentative de crible. Ils signifient plutôt que le problème doit être reformulé d'une manière ou d'une autre. Au lieu de Y, par exemple, il peut être préférable d'essayer de cribler les fibres de l'application N. Et comme il peut effectivement se passer que différentes fibres aient des propriétés différentes, et ne puissent pas être traitées uniformément, cela n'est pas étonnant.[10]

Dans le cas du crible en orbites pour un groupe Λ, Zariski-dense dans le groupe semisimple $G/\mathbf{Q}$, l'indépendance désirée est obtenue en se ramenant d'abord à la composante connexe de l'élément neutre G^0 de G (en remplaçant Λ par $\Lambda \cap G^0(\mathbf{Q})$ ou une classe à gauche de ce groupe dans Λ) et ensuite au *revêtement simplement connexe* G^{sc} de G^0 à l'aide de l'application de projection

$$\pi : G^{sc} \to G^0,$$

avec laquelle on remplace Λ par son image inverse Λ^{sc} dans $G^{sc}(\mathbf{Q})$, et la fonction f par la composée $\tilde{f} = f \circ \pi$. En général, ces opérations peuvent rendre nécessaire de passer à un corps de base différent du corps $\mathbf{Q}$, mais cela ne pose pas de difficultés de principe. Pour une analyse détaillée dans le cas du groupe Apollonien $\mathcal{A}$, où $G = O(Q)$ n'est pas connexe, et où la composante connexe $\mathrm{SO}(Q)$ n'est pas simplement connexe, voir [4, §6] ou [17].

Exemple 5.3. — Dans l'énoncé du Théorème 1.1, on a $G = \mathrm{SL}_m$, qui est connexe et simplement connexe, et ces préliminaires ne sont pas nécessaires. Il en est de même lorsque G est un groupe symplectique $G = \mathrm{Sp}_{2g}$, ou si G est un produit fini de groupes de ces deux types.

C'est le résultat suivant qui montre qu'un sous-groupe Zariski-dense dans un groupe simplement connexe a une propriété forte d'indépendance des réductions modulo les nombres premiers, et qui fournit (dans un cas au moins) la propriété d'équirépartition locale nécessaire au crible.

Théorème 5.4 (Approximation forte et indépendance). — *Soit $G/\mathbf{Q}$ un groupe algébrique linéaire, connexe, simplement connexe et absolument presque simple, plongé dans $\mathrm{GL}_m/\mathbf{Q}$ pour un certain $m \geqslant 1$, et soit $\Lambda \subset G(\mathbf{Q}) \cap \mathrm{GL}_m(\mathbf{Z})$ un sous-groupe de type fini Zariski-dense.*[11] *Il existe un ensemble fini de nombres premiers $\Sigma = \Sigma(\Lambda)$ tel que G a un modèle sur $\mathbf{Z}[1/\Sigma]$, encore noté G pour simplifier, et tel que:*

(1) *Pour tout nombre premier $p \notin \Sigma$, l'application de réduction*

$$\Lambda \to G(\mathbf{F}_p)$$

[10] On peut penser au nombre de saturation pour une fonction comme $f(\gamma) = (2 + \det(\gamma)) \operatorname{Tr}(\gamma)$ dans le cas du groupe $\mathcal{A}$.

[11] Par exemple, cela s'applique à $G = \mathrm{SL}_m$ ou Sp_{2g}.

est surjective, c'est-à-dire, l'image Λ_p de la réduction modulo p est « aussi grande que possible », et donc $\Lambda_p = G(\mathbf{F}_p)$.

(2) *Pour tout entier d sans facteurs carrés premier à Σ, l'application de réduction*

$$\Lambda \to \prod_{p|d} G(\mathbf{F}_p) = G(\mathbf{Z}/d\mathbf{Z})$$

est surjective, c'est-à-dire, on a $\Lambda_d = G(\mathbf{Z}/d\mathbf{Z})$ et $\Lambda \to \Lambda_d$ est également surjective.

(3) *Soit μ_k la mesure de comptage pondérée de la Section 4.2 associée à un ensemble de générateur fini S, symétrique et tel que $1 \in S$. Alors, pour tout entier d sans facteurs carrés et premier à Σ, les mesures de probabilité $\tilde{\mu}_{k,d}$ sur*

$$\Lambda_d = \prod_{p|d} \Lambda_p = G(\mathbf{Z}/d\mathbf{Z})$$

convergent, quand $k \to +\infty$, vers la mesure de probabilité uniforme sur $\nu_d = \prod \nu_p$, c'est-à-dire, vers la mesure telle que

$$\nu_d(\gamma) = \frac{1}{|G(\mathbf{Z}/d\mathbf{Z})|}, \qquad \textit{pour tout } \gamma \in G(\mathbf{Z}/d\mathbf{Z}).$$

Les énoncés (1) et (2) sont des résultats difficiles, qui ont été prouvés, sous diverses formes, par Hrushovski et Pillai [30], Nori [47], Matthews-Vaserstein-Weisfeiler [44], la version la plus générale étant celle due à Weisfeiler [60].

Exemple 5.5. — Bien que ces résultats soient difficiles, on peut remarquer que lorsque le groupe Λ est donné « concrètement », on peut espérer vérifier directement ses conclusions, et cela peut même être nécessaire si l'on souhaite avoir un énoncé complètement explicite (c'est-à-dire connaître précisément l'ensemble exceptionnel Σ).

Par exemple, pour le groupe Apollonien $\mathcal{A}$, Fuchs [17] a déterminé explicitement l'image modulo d de l'image inverse dans le revêtement universel du groupe $\mathcal{A}$. Pour le groupe $L \subset \mathrm{SL}_2(\mathbf{Z})$ (voir (1)) qui est d'indice infini dans $\mathrm{SL}_2(\mathbf{Z})$, on voit clairement que la réduction modulo p de L est surjective pour $p \neq 3$, et est triviale pour $p = 3$. Pour $\Lambda = \mathrm{SL}_m(\mathbf{Z})$ ou $\mathrm{Sp}_{2g}(\mathbf{Z})$ (entre autres), la surjectivité modulo tout les nombres premiers est élémentaire si l'on utilise les générateurs « standards » de ces groupes et de leur analogues modulo p.

L'énoncé (3), par contre, ne fait pas partie de ce que l'on appelle traditionnellement la propriété « d'approximation forte ». Il est connu, dans beaucoup de cas, pour les autres méthodes de comptage (boules archimédiennes et combinatoires non pondérées), mais il est alors vu en général comme un corollaire évident des énoncés d'équirépartition quantitative et uniforme qui sont nécessaires de toute manière pour les hypothèses fondamentales du crible. Nous en dirons plus à ce sujet dans la section suivante. Notons cependant que les mesures locales obtenues à la limite, étant les mesures uniformes sur les groupes finis $G(\mathbf{Z}/d\mathbf{Z})$, sont les plus naturelles que l'on puisse espérer trouver une fois qu'il est établi que $\Lambda_d = G(\mathbf{Z}/d\mathbf{Z})$.

Voici la preuve de (3), qui est très simple. Plus généralement, elle montre – sans hypothèse sur G ou sur d – que les mesures $\tilde{\mu}_{k,d}$, pour le comptage pondéré, convergent vers la mesure de probabilité uniforme sur l'image Λ_d de la réduction modulo d (indépendamment du fait que Λ_d soit $G(\mathbf{Z}/d\mathbf{Z})$ ou un autre groupe).[12]

[12] Ce fait est aussi une propriété de la théorie élémentaire des chaînes de Markov finies.

Soit $\varphi : \Lambda_d \to \mathbf{C}$ une fonction quelconque. L'intégrale de φ par rapport à $\tilde{\mu}_{k,d}$ est

$$\sum_{y\in\Lambda_d} \varphi(y)\frac{1}{|S|^k}\sum_{\substack{s_1,\dots,s_k\in S\\ s_1\cdots s_k=y}}\cdots\sum 1 = \frac{1}{|S|^k}\sum_{s_1,\dots,s_k\in S}\cdots\sum \varphi(s_1\cdots s_k) = (M^k\varphi)(1),$$

où M désigne l'opérateur de moyenne de Markov associé à (la réduction modulo d de) S, agissant sur les fonctions sur Λ_d, autrement dit, pour $f : \Lambda_d \to \mathbf{C}$ et $x \in \Lambda_d$, on a

$$(Mf)(x) = \frac{1}{|S|}\sum_{s\in S} f(xs).$$

Les fonctions constantes sont fonctions propres de M pour la valeur propre 1. Parce que S engendre Λ (et donc Λ_d), on voit facilement que cette valeur propre a multiplicité 1. Ainsi, si l'on écrit

$$\varphi = \frac{1}{|\Lambda_d|}\sum_{y\in\Lambda_d}\varphi(y) + \varphi_0,$$

avec φ_0 de moyenne nulle sur Λ_d (pour la mesure uniforme), on trouve

$$M^k\varphi = \frac{1}{|\Lambda_d|}\sum_{y\in\Lambda_d}\varphi(y) + M^k\varphi_0,$$

d'où il découle que

$$\left|(M^k\varphi)(1) - \frac{1}{|\Lambda_d|}\sum_{y\in\Lambda_d}\varphi(y)\right| \leqslant \max_{y\in\Lambda_d}|(M^k\varphi_0)(y)| \leqslant \sqrt{|\Lambda_d|}\rho_0(M)^k\|\varphi\|_2, \tag{20}$$

ρ_0 étant le rayon spectral de l'opérateur M restreint à l'espace des fonctions sur de moyenne 0 sur Λ_d, équipé de la norme L^2 correspondante, notée $\|\cdot\|_2$.

Comme on a supposé que $1 \in S$, -1 n'est *pas*[13] une valeur propre de M. Comme M est symétrique et a un spectre dans $[-1, 1]$, cela signifie que $\rho_0(M) < 1$. Ainsi, on a

$$\int_{\Lambda_d}\varphi(y)d\tilde{\mu}_{k,d} \to \frac{1}{|\Lambda_d|}\sum_{y\in\Lambda_d}\varphi(y)$$

quand $k \to \infty$, qui correspond à la propriété d'équirépartition locale par rapport à la mesure de probabilité uniforme sur Λ_d.

Remarque 5.6. — L'indépendance des réductions modulo p, au sens du Théorème 5.4, n'est valide que lorsque G est simplement connexe. Cela signifie que les conclusions (1) et (2) peuvent être considérées comme une caractérisation alternative de cette propriété, dans le cadre du crible au moins.

Considérons de nouveau l'exemple du groupe cyclique Λ engendré par $2 \in \mathrm{GL}_1(\mathbf{Z}[1/2])$, déjà mentionné après l'Hypothèse 5.1. L'image de Λ modulo un nombre premier $p \geqslant 3$ est cyclique d'ordre égal à l'ordre de 2 dans $(\mathbf{Z}/p\mathbf{Z})^\times$. Il s'agit là d'une quantité mystérieuse; en particulier, il n'est pas vrai que 2 engendre $(\mathbf{Z}/p\mathbf{Z})^\times$ pour tout p assez grand (bien que, d'après une conjecture classique d'Artin, cela devrait être le cas pour une proportion strictement positive des nombres premiers). De plus, les différentes réductions modulo p ne sont pas indépendantes. Ceci montre comment les principes les plus élémentaires du crible sont en défaut. (Le mieux qu'il semble possible de faire avec les techniques actuelles est d'utiliser le

[13] Soit $S' = S - \{1\}$, $|S| = s \geqslant 1$; l'opérateur M s'écrit $(1 - 1/s)M' + 1/s$, M' étant l'opérateur associé à S', et puisque le spectre de M' est dans $[-1, 1]$, celui de M est dans $[-1 + 2/s, 1]$.

fait que tout nombre premier ℓ assez grand est l'ordre de 2 modulo un certain $p = p(\ell)$, pour en déduire que $2^n - 1$ a, en moyenne pour $n \leqslant N$, à peu près autant de « petits » facteurs premiers que les entiers d'une taille comparable – voir [35, Exercise 4.2]).

5.2. Équirépartition quantitative : aspects combinatoires

On considère ici un sous-groupe $\Lambda \subset \mathrm{GL}_m(\mathbf{Z})$ de type fini dont l'adhérence de Zariski G est simple, connexe et simplement connexe, avec un ensemble de générateurs symétrique fixé S. (Plus concrètement, Λ est tel que les conclusions (1) et (2) du Théorème 5.4 sont valides).

Si l'on utilise la méthode de comptage combinatoire pondérée (avec la condition $1 \in S$), le théorème en question montre que pour vérifier les hypothèse fondamentales du crible (Définition 3.6) avec un niveau de distribution D_k, il « suffit » de vérifier la condition correspondante (16), si l'on restreint l'attention au crible avec des nombres premiers p n'appartenant pas à l'éventuel ensemble exceptionnel Σ, et donc aux entiers d sans facteurs carrés et premiers à Σ.

L'inégalité (20), appliquée à la fonction caractéristique φ d'un point $\alpha \in \Lambda_d$, montre que l'on a un énoncé d'équirépartition quantitatif pour d fixé, premier à Σ, à savoir

$$|r_{d,k}(\alpha)| \leqslant \rho_d^k,$$

pour tout $\alpha \in \Lambda_d$, où $\rho_d < 1$ est comme ci-dessus le rayon spectral de l'opérateur de moyenne sur les fonctions de moyenne nulle sur Λ_d.

Il est donc clair *qu'obtenir un niveau de distribution pour cribler Λ revient alors à avoir un contrôle uniforme sur ρ_d pour d variable.*

Le mieux que l'on puisse espérer[(14)] est d'avoir une majoration

$$\rho_d \leqslant \rho < 1$$

pour tout $d \geqslant 1$, avec ρ fixé et indépendant de d. L'équirépartition modulo d se produit alors à vitesse exponentielle et uniforme par rapport à d. Cette condition équivaut à demander que la famille de graphes de Cayley des Λ_d (par rapport aux générateurs S) soit un *graphe expanseur*. Nous renvoyons à [28] pour un traitement détaillé des propriétés et définitions équivalentes des expanseurs, et nous nous contentons ici de la définition qui est apparue naturellement :

Définition 5.7 (Famille de graphes expanseurs, définition par les marches au hasard)

Soit $k \geqslant 1$ un entier fixé. Une famille $(\Gamma_i)_{i\in I}$ de graphes connexes k-réguliers, éventuellement avec des arêtes multiples ou des boucles, est une famille de graphes expanseurs s'il existe $\rho < 1$, indépendant de i, tel que

$$\rho_i \leqslant \rho < 1$$

pour tout i, où ρ_i désigne le rayon spectral de l'opérateur de moyenne de Markov agissant sur l'espace des fonctions de moyenne nulle sur Γ_i munies du produit scalaire

$$\langle f_1, f_2\rangle = \frac{1}{|\Gamma_i|}\sum_{x\in\Gamma_i} f_1(x)\overline{f_2(x)}.$$

(14) Il est bien entendu permis d'envisager des cas où le niveau de distribution est obtenu par une estimation en moyenne, comme le permet le théorème de Bombieri-Vinogradov, ou les théorèmes de Fouvry-Iwaniec et Bombieri-Friedlander-Iwaniec, pour les nombres premiers en progressions arithmétiques.

Si l'on suppose que les graphes de Cayley de Λ_d forment un expanseur, avec constante d'expansion $\rho < 1$, et que

$$|\Omega_p| \leqslant p^{\Delta}, \quad |\Lambda_p| \leqslant p^{\Delta_1}$$

on obtient immédiatement la majoration

$$\sum_{d<D} |\Omega_d| \max_{\alpha\in\Lambda_d} |r_{d,k}(\alpha)| \leqslant D^{\Delta+1}\rho^k \leqslant D^{\Delta_1+1}\rho^k$$

pour $k \geqslant 1$. Cela permet de garantir un niveau de distribution (comme dans la Définition 3.6) du type

$$D_k = \beta^k, \quad \text{pour tout} \quad 1 < \beta < \rho^{-1/(1+\Delta)}. \tag{21}$$

Ces arguments portent sur la méthode de comptage pondérée. On peut quand même espérer avoir un niveau de distribution comparable pour les boules combinatoires, sous l'hypothèse d'expansion des graphes de Cayley. Cela ne semble connu à l'heure actuelle que sous l'hypothèse supplémentaire que Λ soit un groupe libre (nécessairement de rang au moins 2). Quand c'est le cas, Bourgain, Gamburd et Sarnak [4, §3.3, (3.29), (3.32)] montrent, à l'aide de la théorie spectrale classique des groupes libres, que pour les boules combinatoires de rayon k, il existe $\tau < 1$, qui dépend explicitement de la constante d'expansion ρ de la famille (Λ_d), tels que les mesures $\tilde{\mu}_{d,k}$ correspondantes convergent vers la mesure uniforme ν_d sur Λ_d (pour d premier à un ensemble fini de nombres premiers), avec une erreur bornée par

$$|r_{d,k}(\alpha)| \ll |B_S(k)|^{\tau-1}$$

pour tout $k \geqslant 1$.

La restriction aux groupes libres peut être gênante pour certaines applications. Cependant, on peut noter (par exemple) que l'image inverse de $\mathcal{A}$ dans le revêtement simplement connexe de $\mathrm{SO}(Q)$ est libre, ce qui permet d'utiliser cette méthode sans difficultés pour les empilements de cercles Apolloniens. De plus, comme indiqué dans [4], il est possible pour beaucoup d'applications (par exemple pour borner le nombre de saturation) d'utiliser le fait (l'alternative de Tits) que, sous les hypothèses données sur G, tout sous-groupe Λ de G qui est Zariski-dense contient un sous-groupe libre Λ_Z qui est encore Zariski-dense dans G. On peut alors appliquer le crible à Λ_Z (ou à l'orbite de x_0 sous Λ_Z seulement).

Quoi qu'il en soit, il devient essentiel de savoir si la propriété d'expansion est valide. Oubliant l'ensemble possible de nombres premiers exceptionnels, on peut poser la question pour tout les graphes de Cayley de $G(\mathbf{Z}/d\mathbf{Z})$, lorsque $d \geqslant 1$ est sans facteurs carrés, par rapport à des ensembles de générateurs convenables.

Cette question a une assez longue histoire. Jusqu'aux derniers développements, cependant, les cas connus étaient tous des réseaux dans des groupes semisimples.[15] En effet, la propriété d'expansion peut être énoncée comme le fait que le groupe Λ ait la propriété (τ) de Lubotzky pour des représentations se factorisant par un quotient de congruence $\Lambda \to \Lambda_d = G(\mathbf{Z}/d\mathbf{Z})$. Ainsi, elle est connue, d'après les travaux de Clozel [11], pour tout sous-groupe d'indice fini Λ de $G(\mathbf{Z})$. En fait, dans beaucoup de cas très intéressants, comme les sous-groupes d'indice fini de $\mathrm{SL}_m(\mathbf{Z})$ pour $m \geqslant 3$ ou de $\mathrm{Sp}_{2g}(\mathbf{Z})$ pour $g \geqslant 2$, le résultat découle directement de la Propriété (T) de Kazhdan.

[15] À des exceptions isolées près, dues à Shalom [58, Th. 5.2] et implicitement à l'exception du travail de Gamburd [19] du côté spectral, décrit dans la section suivante. (Pour p premier seulement dans les deux cas).

Lorsque Λ est, éventuellement, d'indice infini dans $G(\mathbf{Z})$, il y a eu très récemment des progrès rapides,[16] motivés en partie par les applications au crible. Le théorème suivant a été annoncé :

THÉORÈME 5.8 (Expansion dans les groupes linéaires finis). — *Soit $G/\mathbf{Q}$ un groupe algébrique absolument presque simple, connexe et simplement connexe, plongé dans GL_m pour un certain $m \geqslant 1$, par exemple, $G = \mathrm{SL}_m$, $m \geqslant 2$, ou Sp_{2g}, $g \geqslant 1$, $m = 2g$. Soit $\Lambda \subset G(\mathbf{Q}) \cap \mathrm{GL}_m(\mathbf{Z})$ un sous-groupe de type fini, Zariski-dense dans G. Soit S un ensemble fini symétrique de générateurs de Λ. Alors la famille des graphes de Cayley des groupes $\Lambda_d \subset \mathrm{GL}_m(\mathbf{F}_p)$ obtenus par réduction modulo d de Λ, par rapport aux générateurs S modulo d, est une famille de graphes expanseurs lorsque d parcourt l'ensemble des entiers sans facteurs carrés.*

Ceci s'applique, en particulier, au groupe $L \subset \mathrm{SL}_2(\mathbf{Z})$ de (1), ce qui répond à une question de Lubotzky.

Beaucoup de mathématiciens ont contribué (et contribuent encore) à la preuve de ce résultat et de ses variantes, extensions, etc. Les remarques qui suivent ne prétendent pas donner une histoire détaillée, ni même l'esquisse d'une preuve, mais il semble utile de présenter rapidement la stratégie qui est employée :

– [1ère étape : Croissance] La première étape est la preuve d'un théorème de croissance dans les groupes finis $G(\mathbf{F}_p)$ pour p premier : il existe $\delta > 0$, dépendant seulement de G, tel que pour tout sous-ensemble $A \subset G(\mathbf{F}_p)$ qui engendre $G(\mathbf{F}_p)$, on a

$$|A \cdot A \cdot A| = |\{abc \mid a, b, c \in A\}| \gg \min(|G(\mathbf{F}_p)|, |A|^{1+\delta}), \tag{22}$$

où la constante implicite dépend seulement de G.

Un tel résultat, quand il est connu, implique que le diamètre des graphes de Cayley est $\ll (\log p)^C$ pour une certaine constante $C \geqslant 1$. Des résultats standards concernant les graphes permettent d'en déduire une majoration explicite de ρ_p, mais celle-ci est plus faible que la condition d'expansion : elle est de la forme $1 - \rho_p \gg (\log p)^{-D}$ pour une constante $D \geqslant 0$. Notons en passant que bien que cela ne suffise pas pour les applications au crible, il existe des applications de telles inégalités, y compris, de manière peut-être surprenante, en géométrie arithmétique [14].

Les premiers cas de résultats de croissance sont dus à Helfgott [26] pour $G = \mathrm{SL}_2$ et SL_3 [27]. Après ce progrès décisif, de tels énoncés ont été prouvés par Gill et Helfgott [20] (pour SL_m, avec une restriction sur A) et, indépendamment et simultanément, par Breuillard-Green-Tao [8] et par Pyber-Szabó [51, Th. 4], dans la généralité nécessaire pour notre propos (et même plus). Il semble important de mentionner aussi un article intermédiaire de Hrushovski [29], car celui-ci a mis en valeur une prépublication assez ancienne de Larsen et Pink [36], de laquelle a émergé une inégalité générale très utile (voir, par exemple, [8, Th. 4.1]) concernant la taille de l'intersection d'un sous-ensemble de $G(\mathbf{F}_p)$ « qui ne croit pas » et d'une sous-variété algébrique propre de G.

– [2ème étape : Expansion modulo p] Comme il a été mentionné, le théorème de croissance ne suffit pas à démontrer immédiatement que les graphes de Cayley forment un graphe expanseur. Bourgain et Gamburd [3] ont donné la première preuve de ce fait pour le cas de

[16] Ces progrès méritent amplement leur propre discussion ; l'excellent survol de B. Green [24], bien que lui-même très récent, ne couvre pas les nouveaux résultats les plus remarquables.

$\mathrm{SL}_2(\mathbf{F}_p)$. Leur méthode est fondée sur une idée qui remonte au moins à Sarnak et Xue [56] et qui consiste à comparer une majoration et une minoration pour le nombre de boucles dans le graphe de Cayley, basées à l'identité et de longueur $\ell \approx \log p$. Comme dans [56], la minoration (où apparaît ρ_p) est facile à obtenir par une expansion spectrale et une application du fait – remontant, lui, à Frobenius ! – que la plus petite dimension d'une représentation linéaire non-triviale de $\mathrm{SL}_2(\mathbf{F}_p)$ est « grande » (à savoir égale à $(p-1)/2$). La majoration, par contre, est obtenue à l'aide d'un nouvel ingrédient très ingénieux (maintenant appelé « flattening lemma », voir [3, Prop. 2]), qui est utilisé pour montrer que la propriété d'avoir un grand tour de taille (« girth »), qui est assez facile à vérifier, suffit pour démontrer qu'après $\gg \log p$ pas, la marche au hasard sur le graphe est très proche d'être uniformément répartie, et donc qu'il ne peut y avoir trop de boucles de telle longueur basée en 1. Ce lemme d'aplatissement, quand à lui, est obtenu *in fine* par une application – dans ce cas – du théorème de croissance (22) de Helfgott dans $\mathrm{SL}_2(\mathbf{F}_p)$. (Pourquoi ? Très approximativement, on peut dire que Bourgain et Gamburd montrent que si doubler le nombre de pas $\gg \log p$ de la marche au hasard n'aboutit pas à une amélioration considérable de son uniformité, c'est que celle-ci doit être largement concentrée sur un ensemble $A \subset \mathrm{SL}_2(\mathbf{F}_p)$ qui ne croit pas, c'est-à-dire tel que (22) ne soit pas valide ; d'après le théorème de Helfgott, il en découlerait donc que A serait contenu dans un sous-groupe propre, et il est relativement facile de vérifier que cette alternative n'est pas possible pour la marche au hasard qui est basée sur des générateurs de $G(\mathbf{F}_p)$).

Après la preuve des théorèmes de croissance généraux, cette seconde étape a été étendue aux autres groupes (par exemple, c'est annoncé par Breuillard, Green et Tao dans [8]).

– [3ème étape : Expansion pour d sans facteurs carrés] Cette étape, qui d'après la discussion précédente est indispensable pour le crible, a d'abord été obtenue par Bourgain, Gamburd et Sarnak pour SL_2 dans [4], par une démonstration inspirée de celle de Bourgain-Gamburd, mais significativement plus complexe. La difficulté essentielle est de contrôler le trou spectral lorsque le nombre de facteurs premiers de d augmente (si d a un nombre borné de facteurs premiers, il n'y a pas de difficulté majeure en plus du cas des nombres premiers). Varjú [59] a trouvé une preuve plus simple et conceptuelle, qui peut être adaptée à des groupes plus généraux, en particulier à SL_m, dès qu'un théorème de croissance est connu pour $G(\mathbf{F}_p)$.[(17)] Un résultat optimal, en un certain sens, a été annoncé par Salehi Golsefidy et Varjú [53] ; il s'applique à n'importe quel groupe G dont la composante connexe de l'identité est *parfaite*.

5.3. Équirépartition quantitative : aspects spectraux et ergodiques

Revenons au crible en orbite pour un sous-groupe Λ, dont l'adhérence de Zariski est $G/\mathbf{Q}$, mais avec l'idée d'utiliser les mesures de comptage sur des boules archimédiennes. Dans ce cas, les résultats sont plus fragmentaires. Bien évidemment, le point essentiel est d'étendre l'énoncé d'équirépartition quantitatif à cette méthode de comptage (la partie (3) du Théorème 5.4). Notons que les parties (1) et (2) restent valables (si les hypothèses sont vérifiées par G). Comme on a

$$\mu_X(\gamma \in \Lambda \mid \gamma \equiv \gamma_0 \pmod d) = \sum_{\substack{\|\gamma\| \leqslant X \\ \gamma \equiv \gamma_0 \pmod d}} 1$$

(17) On peut noter que Bourgain et Varjú [7] ont aussi démontré la propriété d'expansion pour $\mathrm{SL}_m(\mathbf{Z}/d\mathbf{Z})$ pour tout $d \geqslant 1$, pas seulement les entiers sans facteurs carrés.

pour $d \geqslant 1$ et $\gamma_0 \in \Lambda_d$, et que cela peut aussi s'écrire

$$\sum_{\substack{\|\tau\gamma_0\| \leqslant X \\ \tau \in \Lambda(d)}} 1$$

où $\Lambda(d) = \ker(\Lambda \to \Lambda_d)$ est un sous-groupe de congruence de Λ, on peut voir que cela revient à des questions d'uniformité et d'effectivité dans des problèmes de comptage de points dans un réseau, précisément dans le quotient $X_\Lambda = \Lambda\backslash G(\mathbf{R})$ et ses revêtements de congruence $X_\Lambda(d) = \Lambda(d)\backslash G(\mathbf{R})$. (Si l'on désire compter directement sur l'orbite $\mathcal{O}(x_0)$, le problème est encore différent suivant la nature du stabilisateur de x_0, et des difficultés supplémentaires peuvent surgir).

Dans le cas le plus simple où $G(\mathbf{R}) = \mathrm{SL}_2(\mathbf{R})$, $\Lambda \subset \mathrm{SL}_2(\mathbf{Z})$ et X_Λ est de volume fini, un résultat célèbre de Selberg (voir, par exemple, [31, Th. 15.11]), dont la démonstration originale dépend de la décomposition spectrale de l'opérateur de Laplace sur X_Λ, prouve l'énoncé d'équirépartition locale avec un terme de reste qui dépend directement de la première valeur propre non-nulle $\lambda_1(d)$ du laplacien de la surface hyperbolique $\Lambda(d)\backslash\mathbf{H}$. Cela permet de constater encore une fois que l'existence d'un trou spectral est, d'une manière ou d'une autre, l'outil crucial pour l'équirépartition quantitative. La différence frappante avec l'argument complètement élémentaire qui mène à la formule (10) devient claire : au lieu de compter les entiers dans un (grand) intervalle, où la contribution du bord (qui sert essentiellement de terme de reste) est facile à contrôler et souvent négligeable, on a ici un problème de comptage hyperbolique, où le bord peut contribuer une proportion positive de la masse.

En général, on peut distinguer deux cas : Λ est, ou n'est pas, un réseau dans le groupe $G(\mathbf{R})$ des points réels de son adhérence de Zariski G (que l'on suppose de nouveau être simple, connexe et simplement connexe), autrement dit, Λ est d'indice fini, ou pas, dans un tel réseau fixé. En terme de X_Λ, la dichotomie a une signification géométrique évidente : X_Λ a un volume fini ou infini par rapport à une mesure induite à partir d'une mesure de Haar sur $G(\mathbf{R})$. (Noter que l'on requiert toujours que le Théorème 5.4 soit valide, ce qui signifie que $G(\mathbf{R})$ n'est pas compact).

(1) [Volume fini] Bien qu'il semble naturel d'appliquer ici les méthodes d'analyse harmonique similaires à celles de Selberg, il y a des difficultés techniques assez sérieuses. C'est particulièrement vrai lorsque X_Λ n'est pas compact, puisque la décomposition spectrale complète de $L^2(X_\Lambda)$ fait alors intervenir la théorie générale des séries d'Eisenstein (voir l'article de Duke, Rudnick et Sarnak [12] pour les premiers résultats de ce type).

Mais, à partir des travaux de Eskin et McMullen [15], des méthodes issues de la théorie ergodique ont été découvertes, permettant d'obtenir des résultats très généraux concernant le problème de comptage dans les réseaux. Dans l'esprit du problème d'équirépartition local uniforme (comme dans le Théorème 5.4), on peut mentionner d'abord un article de Maucourant [45]; les résultats les plus généraux ont été développés par Gorodnik et Nevo [21], [22] (voir aussi [46]). Sans en dire davantage, par manque de compétences, on peut cependant dire que le trou spectral apparaît dans cette méthode par l'intermédiaire de l'exposant $p_\Lambda > 2$ tel que les coefficients matriciels de représentations unitaires de $G(\mathbf{R})$ apparaissant dans $L^2_0(\Lambda(d)\backslash G(\mathbf{R}))$ sont dans $L^{p+\varepsilon}$ pour tout $\varepsilon > 0$. L'existence d'un tel exposant > 2 est une conséquence connue de la Propriété (τ) pour Λ par rapport aux quotients de congruence. Lorsque $G(\mathbf{R})$ a la Propriété (T), cette constante dépend seulement de $G(\mathbf{R})$, et des valeurs explicites sont connues (dues à Li [38] pour les groupes classiques et Oh en général [48]). Pour

certains groupes comme SL_m, $m \geqslant 3$ ou Sp_{2g}, $g \geqslant 2$, ces travaux donnent même l'exposant optimal (du point de vue des représentations générales du groupe $G(\mathbf{R})$). Pour les sous-groupes de congruence, l'exposant optimal est lié directement aux formes généralisées de la conjecture de Ramanujan ; on peut consulter le survol [55] de Sarnak pour ces aspects).

(2) [Volume infini[18]] Ce cas, pour la méthode de comptage archimédienne, est le plus délicat. Ainsi, seuls des exemples de sous-groupes des groupes d'isométrie des espaces hyperboliques ont été considérés avec succès (c'est-à-dire des sous-groupes de $O(n,1)$). En effet, dans ce cas, l'approche spectrale de Lax-Phillips est disponible pour le comptage de points [37], du moins quand la dimension de Hausdorff de l'ensemble limite du sous-groupe discret $\Lambda \subset \mathrm{SO}(n,1)(\mathbf{R})$ est assez grande.[19] C'est le cas, par exemple, du groupe Apollonien $\mathcal{A}$ (qui est isomorphe à un sous-groupe de $O(3,1)(\mathbf{R})$, puisque la forme quadratique Q a signature $(3,1)$), dont l'ensemble limite a dimension de Hausdorff > 1.30, alors que la borne inférieure pour la méthode de Lax-Phillips dans l'espace hyperbolique de dimension 3 est $\delta > 1$.

Encore une fois, il ne sera pas dit plus concernant les techniques utilisées, par manque d'expertise. Cependant, on peut répéter que c'est l'existence d'un trou spectral du laplacien pour les revêtements de congruence qui joue un rôle crucial. Le premier cas où cela a été établi est dans l'article [19] de Gamburd. On peut aussi aujourd'hui espérer obtenir un tel résultat en étendant au cas de volume infini les théorèmes de comparaison entre laplaciens combinatoire et hyperbolique (voir par exemple [9, Ch. 6]), et en appliquant alors les propriétés d'expansion des graphes de Cayley discutés dans la section précédente (Théorème 5.8) ; voir [5] pour cette approche. Dans la Section 5.5, on trouvera l'énoncé de certains résultats de cribles obtenus par Kontorovich et Oh [33], et nous référons au survol de Oh [49] (ICM 2010) pour plus de détails.

5.4. Nombre de saturation

Nous expliquons maintenant comment s'applique le crible pour démontrer le Théorème 1.1, en utilisant la méthode de comptage pondérée (c'est-à-dire, implicitement, des marches au hasard). Il devrait être clair que la méthode est extrêmement générale.

Soit Λ, x_0 et f comme dans l'énoncé, ou bien Λ dont l'adhérence de Zariski G est simple, connexe et simplement connexe (et pas seulement $G = \mathrm{SL}_m$, $m \geqslant 2$). Pour simplifier, on va cribler dans $Y = \Lambda$ au lieu de le faire dans l'orbite $\mathcal{O}(x_0)$: il est élémentaire de déduire la finitude du nombre de saturation pour l'orbite à partir de ce cas. On va aussi supposer, pour simplifier, que les composantes irréductibles de l'hypersurface donnée par l'équation $\{f(\gamma x_0) = 0\}$ dans G sont absolument irréductibles.[20] Fixons un ensemble symétrique de générateurs de Λ avec $1 \in S$.

On va étudier l'ensemble criblé (12) pour l'ensemble de nombres premiers $\mathcal{P}$ formé par ces p qui ne sont pas dans l'ensemble exceptionnel fini Σ fournit par le Théorème 5.4, avec le choix

[18] Bourgain, Gamburd et Sarnak parlent, dans ce cas, d'un sous-groupe Λ « mince » (« thin » en anglais) ; cette terminologie entre malheureusement en conflit avec la notion d'ensemble « mince » dans la Définition 4.4 – un sous-groupe Zariski-dense $\Lambda \subset \mathrm{GL}_m(\mathbf{Z})$ de G n'est jamais « mince », en ce sens, dans $G(\mathbf{Q})$.

[19] Très récemment, Bourgain, Gamburd et Sarnak [5] ont abordé le problème pour des sous-groupes Zariski-dense de $\mathrm{SL}_2(\mathbf{R})$ dont l'ensemble limite a n'importe quelle dimension > 0.

[20] Comme expliqué dans [4, p. 562], lorsque G est simplement connexe, l'anneau $\mathbf{Q}[G]$ des fonctions sur G est factoriel, et l'hypothèse est que les facteurs irréductibles de f dans $\mathbf{Q}[G]$ sont encore irréductibles dans $\bar{\mathbf{Q}}[G]$.

des conditions de crible

$$\Omega_p = \{\gamma \in Y_p = G(\mathbf{F}_p) \mid f(\gamma \cdot (x_0 \pmod p)) = 0 \in \mathbf{Z}/p\mathbf{Z}\}.$$

D'après les arguments décrits précédemment (les Théorèmes 5.4 et 5.8), les hypothèses fondamentales du crible sont satisfaites.

En effet, $\mathcal{S}_z(\Lambda;\Omega)$ est l'ensemble des $\gamma \in \Lambda$ tels que $f(\gamma \cdot x_0)$ n'a pas de facteurs premiers $< z$ (en dehors de Σ).

Au prix d'un agrandissement éventuel de l'ensemble Σ (qui reste cependant fini), les estimations de type Lang-Weil pour le nombre de solutions d'équations polynômiales sur un corps fini permettent d'obtenir l'asymptotique

$$|\Omega_p| = \kappa p^{\dim(G)-1} + O(p^{\dim(G)-3/2})$$

pour $p \notin \Sigma$, où κ est le nombre de composantes (absolument) irréductibles de l'hypersurface de G déjà mentionnée, définie par $\{f(\gamma x_0) = 0\}$. Puisque on a

$$|G(\mathbf{F}_p)| = p^{\dim(G)} + O(p^{\dim(G)-1/2}),$$

ce qui peut se vérifier à l'aide des formules pour l'ordre des groupes finis de type Lie, par exemple

$$|\operatorname{SL}_m(\mathbf{F}_p)| = q^{m(m-1)/2} \prod_{2 \leqslant i \leqslant m} (q^i - 1),$$

il en découle que la densité de Ω_p vérifie

$$\nu_p(\Omega_p) = \frac{|\Omega_p|}{|G(\mathbf{F}_p)} = \frac{\kappa}{p} + O(p^{-3/2})$$

pour tout $p \notin \Sigma$. Cela donne la condition (18) et montre que le crible en orbite est alors de « dimension » κ dans la terminologie classique. D'après (21),[(21)] on voit aussi que (19) est valide avec

$$D_k = \beta^k$$

pour un certain $\beta > 1$ (en fait, β peut être n'importe quel nombre réel $< \rho^{-1/\dim(G)}$, où $\rho < 1$ est la constante d'expansion pour les graphes de Cayley concernés, voir la Définition 5.7).

On peut alors conclure qu'il existe « beaucoup » de $\gamma \in \Lambda$ tels que $f(\gamma \cdot x_0)$ ne soit pas divisible par des nombres premiers $< z = \beta^{k/s}$ (hormis ceux dans Σ) ; précisément la μ_k-mesure de cet ensemble, noté $\mathcal{S}_k$, vérifie

$$\mu_k(\mathcal{S}_k) \gg \frac{1}{(\log z)^\kappa} \asymp \frac{1}{k^\kappa},$$

lorsque k est assez grand.[(22)] Pour en déduire que le nombre de saturation est fini, il faut ajouter deux ingrédients assez simples :

(1) Si $\gamma \in \mathcal{S}_k$, l'entier $n = f(\gamma \cdot x_0)$ n'a qu'un nombre *borné* de facteurs premiers (sauf si $n = 0$, ce qui ne se produit qu'avec une probabilité très inférieure, comme dans la Remarque 3.8). En effet, on sait que

$$n = f(s_1 \cdots s_n x_0)$$

[(21)] La Remarque 3.8 s'applique ici pour vérifier (17).

[(22)] Et la majoration correspondante $\mu_k(\mathcal{S}_k) \ll k^{-\kappa}$ est également valide.

avec $s_i \in S$. Puisque la fonction f est un polynôme, il existe évidemment une constante $\lambda \geqslant 1$ telle que

$$f(\gamma \cdot x_0) \ll \lambda^k \tag{23}$$

pour tout $\gamma \in \mathcal{S}_k$ (la constante implicite dépendant de S). Un entier de cette taille qui n'a pas de facteurs premiers $< \beta^{k/s}$ hors de Σ, doit nécessairement satisfaire

$$\Omega(f(\gamma \cdot x_0)) \leqslant r = \frac{s \log \lambda}{\log \beta} + |\Sigma|.$$

Remarque 5.9. — Si les graphes de Cayley vérifient une propriété d'expansion plus faible, il reste possible de cribler, mais les conclusions sont plus faibles : on obtient alors des points dans l'orbite dont le nombre de facteurs premiers a un ordre de grandeur plus petit que celui d'un entier typique de sa taille (voir l'Appendice pour ce nombre de facteurs premiers typique).

(2) Il faut encore vérifier que la borne inférieure obtenue pour les points avec $\leqslant r$ facteurs premiers est incompatible avec la possibilité que cet ensemble soit trop petit, c'est-à-dire, qu'il ne soit pas Zariski-dense, ou qu'il soit mince au sens de la Définition 4.4. Pour le premier cas, il est très facile de voir que tout sous-ensemble W de Λ contenu dans une hypersurface propre $\{g = 0\}$ de G vérifie la majoration

$$\mu_k(W) \ll \delta^{-k} \tag{24}$$

pour un certain $\delta > 1$, ce qui est clairement incompatible avec la minoration ci-dessus pour $\mu_k(\mathcal{S}_{+k})$. Pour voir cela, on choisit un nombre premier convenable $p \notin \Sigma$ tel que $\{g = 0\}$ soit une hypersurface modulo p, et on majore

$$\mu_k(W) \leqslant \mu_k(\gamma \mid g(\gamma) = 0 \pmod p)$$

à l'aide de l'équirépartition locale modulo p et des bornes de Lang-Weil (par exemple).

Une telle majoration (24) est aussi valide pour un ensemble mince, mais il faut appliquer une inégalité de grand crible pour le vérifier (voir la Section 6.2).

5.5. Autres résultats concernant le crible en orbites

Nous énonçons ici un certain nombre de résultats obtenus dans le cadre du crible en orbite.

Exemple 5.10. — On commence avec le groupe Apollonien et les empilements de cercles associés...

- Fuchs [17] a étudié très précisément l'image du groupe $\mathcal{A}$ par réduction modulo un entier.
- À l'aide des informations ainsi obtenues, une conjecture (qui semble difficile) prédit un principe local-global pour les entiers qui apparaissent dans l'ensemble de courbures $\mathcal{C}(\boldsymbol{c})$; Bourgain et Fuchs [2] ont dores et déjà démontré que le nombre d'entiers $\leqslant T$ qui apparaissent (comptés sans multiplicité) est $\gg T$.
- Kontorovich et Oh ont appliqué les méthodes spectrales et ergodiques de comptage de points dans le cas de volume infini pour déduire, tout d'abord, une formule asymptotique pour le nombre de courbures $\leqslant T$ (avec multiplicité ; cette dernière, en moyenne, est grande, de taille $T^{\delta-1}$, où $\delta > 1.3$ est la dimension de l'ensemble limite) puis, à l'aide du crible, ils ont obtenu des majorations et minorations pour le nombre de courbures premières, ou le nombre de paires de courbures premières de deux cercles tangents dans l'empilement (comme 11 et 23 dans la Figure 1). Il est à noter que, le comptage ayant lieu sur l'orbite, au lieu du groupe, la théorie de Lax-Phillips ne s'applique pas, et de

nouvelles idées sont nécessaires. Kontorovich et Oh [34] ont aussi appliqué des méthodes semblables pour l'orbite de sous-groupes d'indice infini Λ dans $\mathrm{SO}(2,1)(\mathbf{Z})$ agissant sur le cône des triplets pythagoriciens (voir la Remarque 4.3). Par exemple, à l'aide du trou spectral explicite de Gamburd [19], ils prouvent que si l'ensemble limite a dimension assez grande (mais pas seulement lorsqu'elle vaut 1), les triplets pythagoriciens dans une telle orbite dont l'hypoténuse a au plus $\leqslant 14$ facteurs premiers forment un ensemble Zariski-dense.

Exemple 5.11. — L'ensemble $V_{m,n}$ des points entiers de l'espace homogène

$$\mathcal{V}_{m,n} = \{\gamma \in \mathrm{GL}_m \mid \det(\gamma) = n\}$$

sous $\mathrm{SL}_m(\mathbf{Z})$ ont été étudiés par Nevo et Sarnak [46], dans le cadre des boules archimédiennes, à l'aide de méthodes basées sur la théorie ergodique (en particulier, propriétés de mélange). Ils démontrent, par exemple, que si $f \in \mathbf{Q}[\mathcal{V}_{m,n}]$ prend des valeurs entières sur $V_{m,n}$, est absolument irréductible, et qu'il n'existe pas d'obstruction de congruence pour que $f(\gamma)$ soit premier (c'est-à-dire, pour tout p premier, il existe $\gamma \in V_{m,n}$ tel que $p \nmid f(\gamma)$), alors le nombre de saturation de $V_{m,n}$ vérifie

$$r \leqslant 1 + 18m_e^3 \deg(f),$$

où m_e est le plus petit entier pair $\geqslant m-1$, sous la forme quantitative

$$|\{\gamma \in V_{m,n} \mid \|\gamma\| \leqslant T \text{ et } \Omega(f(\gamma)) \leqslant r\}| \gg \frac{|\{\gamma \in V_{m,n} \mid \|\gamma\| \leqslant T\}|}{(\log T)}, \tag{25}$$

pour $r > 18m_e^3 \deg(f)$.

Exemple 5.12. — Ainsi qu'il est expliqué dans [46], des bornes comme (25) ne peuvent s'adapter immédiatement à des espaces homogènes non-principaux (c'est-à-dire, des orbites d'un groupe arithmétique tel que le stabilisateur soit non-trivial), quoique la seule finitude du nombre de saturation ne pose pas de problème. Gorodnik et Nevo [21, 22] ont obtenu des résultats qui étendent de telles minorations dans de nombreuses situations. Par exemple, ils considèrent les orbites

$$\mathcal{O}(g_0) = \{g \in M_m(\mathbf{Z}) \mid g = {}^t\gamma g_0 \gamma \text{ pour un } \gamma \in \mathrm{SL}_m(\mathbf{Z})\}$$

pour g_0 fixée, matrice symétrique non-dégénérée à coefficients entiers, si $m \geqslant 3$. Ainsi, pour f convenable, et pour κ et r explicites, ils obtiennent

$$|\{g \in \mathcal{O}(g_0) \mid \|g\| \leqslant T \text{ et } \Omega(f(g)) \leqslant r\}| \gg \frac{|\{g \in \mathcal{O}(g_0) \mid \|g\| \leqslant T\}|}{(\log T)^\kappa}$$

(ici, le stabilisateur qui intervient est un groupe orthogonal).

6. AUTRES PROBLÈMES DE CRIBLE ET AUTRES RÉSULTATS

Dans cette section, nous présentons quelques autres développements du crible en expansion, ainsi que certains problèmes analogues sur les corps finis.

6.1. Exemples géométriques

Dans l'esprit de la Section 2.2, il y a un certain nombre de situations géométrique qui suggèrent des questions de crible pour des groupes discrets qui ne sont pas donnés comme sous-groupes de $\mathrm{GL}_m(\mathbf{Z})$. Il est parfois possible d'attaquer ces problèmes en utilisant le crible dans des quotients arithmétiques de ces groupes, comme on l'a déjà vu pour l'homologie des variétés de Dunfield-Thurston.

Dans ce cas, le groupe discret concerné est le groupe modulaire (« mapping class group ») Γ_g d'une surface Σ_g (connexe compacte sans bord) de genre g. Ce groupe est de type fini, et il est naturel (comme dans [13]) d'utiliser une méthode de comptage pondérée pour étudier le crible sur Γ_g.

Les formules (2) et (3) pour l'homologie des variétés M_ϕ ne dépendent que de l'image du difféomorphisme ϕ dans $\mathrm{Sp}_{2g}(\mathbf{Z})$ ou $\mathrm{Sp}_{2g}(\mathbf{F}_p)$, ce qui signifie qu'en pratique, il s'agit de faire une marche au hasard (avec des pas qui ne sont pas nécessairement équiprobables) sur le groupe discret $\mathrm{Sp}_{2g}(\mathbf{Z})$. Pour $g \geqslant 2$ (une condition qui n'est pas très restrictive, car le cas $g = 1$ n'est pas très intéressant ici), ce groupe a la Propriété (T), et donc les conditions fondamentales du crible sont vérifiées.

Il n'est pas difficile de vérifier par ailleurs que

$$\Omega_p = \{\gamma \in \mathrm{Sp}_{2g}(\mathbf{F}_p) \mid \langle J_p, \gamma J_p\rangle \neq \mathbf{F}_p^{2g}\},$$

est de cardinal $p^{-1} + O(p^{-2})$ pour $p \geqslant 2$ (avec g fixé ; intuitivement, un certain déterminant dans $\mathbf{Z}/p\mathbf{Z}$ doit être nul pour que cette propriété soit vraie, et la probabilité de cet événement est environ $1/p$). On peut donc voir l'homologie des variétés de Dunfield-Thurston comme contrôlée par un crible de dimension 1.

Si ϕ_k est le k-ème pas d'une marche au hasard sur Γ_g, avec les notations de la Section 3.2, l'ensemble Y^0 correspond précisément aux variétés telles que $H^1(M_{\phi_k}, \mathbf{Z})$ soit infini. Comme dans la Remarque 3.8, cet événement a une probabilité qui tend vers 0 (ce qui est prouvé dans [13]), exponentiellement vite quand $k \to +\infty$ ([35, Pr. 7.19 (1)]).

On peut alors aussi conclure que

$$\mathbf{P}(H_1(M_{\phi_k}, \mathbf{Z}) \text{ n'a pas de partie } p\text{-primaire pour } p < z = \beta^k) \asymp \frac{1}{k},$$

pour un certain $\beta = \beta(g) > 1$. La formule (2) montre aussi que si $H_1(M_{\phi_k}, \mathbf{Z})$ est fini, son ordre est de taille contrôlée : précisément, il existe $\lambda \geqslant 1$ tel que le produit Δ_k des p tels que

$$H_1(M_{\phi_k}, \mathbf{F}_p) \neq 0,$$

vérifie $\Delta_k \leqslant \lambda^k$ (encore parce que Δ_k divise un déterminant, non-nul dans $\mathbf{Z}$, et borné par λ^k). En comparant comme pour la finitude du nombre de saturation, on en déduit qu'il existe r (dépendant de g et du système de générateurs S) tel que

$$\mathbf{P}(H_1(M_{\phi_k}, \mathbf{Z}) \text{ est fini et est d'ordre divisible par au plus } r \text{ nombres premiers}) \gg \frac{1}{k}.$$

Une application du grand crible (voir ci-dessous) montre que, toujours avec probabilité qui tend vers 1 quand $k \to +\infty$, l'ordre de $|H_1(M_{\phi_k}, \mathbf{Z})|$ est fini mais divisible par « beaucoup » de nombres premiers $< z$. Cela signifie que $|H_1(M_{\phi_k}, \mathbf{Z})|$ est en général fini, mais de grande taille (voir [35, Pr. 7.19 (2)]).

Un autre exemple de groupe où le crible peut être appliqué est fourni par le groupe des automorphismes extérieurs d'un groupes libre non-abélien (l'action sur l'abélianisation donne

un quotient $\mathrm{SL}_m(\mathbf{Z})$). Cela montre que le crible donne une nouvelle illustration des analogies qui existent entre ces groupes discrets (voir le rapport récent [50] de F. Paulin dans ce séminaire pour beaucoup d'autres exemples profonds, et voir aussi les travaux de Rivin [52] et Maher [42]).

6.2. Le grand crible

Le « grand crible » a déjà été mentionné brièvement, et nous donnons quelques détails ici (voir [35] pour ce sujet). Dans le contexte de la Section 3.2, beaucoup de conditions de crible (Ω_p) vérifiant

$$\nu_p(\Omega_p) \geqslant \delta > 0 \tag{26}$$

pour un certain $\delta > 0$ et tout $p \in \mathcal{P}$ apparaissent naturellement (pour la première fois dans des travaux de Linnik). On parle de *grand crible* parce que, dans le cas classique, cela revient à exclure beaucoup de classes modulo p (une proportion positive des classes modulo p).

Les inégalités de grand crible mènent, sous les hypothèses d'équirépartition uniforme et quantitative et d'indépendance, comme dans la Définition 3.6, à deux types d'énoncés[(23)] :

(1) Une majoration pour la mesure $\mu_n(\mathcal{S}_z(Y;\Omega))$ de l'ensemble criblé qui est de la forme

$$\mu_n(\mathcal{S}_z(Y;\Omega)) \ll \mu_n(Y)H^{-1}, \qquad H = \sum_{d<z} \mu(d)^2 \prod_{p|d} \frac{\nu_p(\Omega_p)}{1-\nu_p(\Omega_p)}$$

(avec z de taille similaire au niveau de distribution, voir [35, Prop. 2.3, Cor. 2.13]). Dans le crible en orbites, on peut appliquer cette borne pour montrer qu'il existe $\delta > 1$ tel que

$$\mu_n(W) \ll \delta^{-k}$$

lorsque $W \subset G(\mathbf{Q}) \cap \mathrm{GL}_m(\mathbf{Z})$ est un ensemble mince, en utilisant le fait (voir [57, Th. 3.6.2]) que le *complément* Ω_p de W (mod p) vérifie une condition de grand crible

$$|\Omega_p| \gg 1$$

pour p assez grand. Cela donne la finitude du nombre de saturation pour les ensembles non-minces.

(2) Une majoration pour la moyenne de

$$\Big(\sum_{\substack{p<z \\ y \pmod p \in \Omega_p}} 1 - \sum_{p<z} \nu_p(\Omega_p) \Big)^2$$

calculée par rapport à μ_n (voir [35, Prop. 2.15]). Ceci permet de démontrer qu'il existe une grande probabilité que le nombre de $p < z$ tels que y (mod p) appartient à Ω_p soit proche de la valeur heuristique attendue, qui est

$$\sum_{p<z} \nu_p(\Omega_p)$$

C'est cette inégalité qui permet, par exemple, de vérifier que l'homologie d'une variété de Dunfield-Thurston M_{ϕ_k} est typiquement de grande taille (croissant plus vite que tout polynôme en k, quand $k \to +\infty$).

Une autre application du grand crible, dans un contexte lié aux groupes discrets, consiste à déterminer le groupe de Galois « typique » du corps de décomposition du polynôme

[(23)] Où il n'est pas nécessaire de supposer a priori que (26) est valide.

caractéristique d'un élément d'un sous-groupe $\Lambda \subset \mathrm{GL}_m(\mathbf{Z})$. L'idée (qui est classique) est d'utiliser les classes de conjugaisons de Frobenius associées aux nombres premiers pour produire des classes de conjugaison dans ce groupe de Galois. Par exemple, si Λ est Zariski-dense dans SL_m, le type de factorisation du polynôme caractéristique modulo p donne une partition de m, et donc une classe de conjugaison c dans le groupe symétrique $\mathfrak{S}_m$, qui est le plus grand groupe de Galois possible. Puisqu'il est assez facile de vérifier que

$$|\{g \in \mathrm{SL}_m(\mathbf{F}_p) \mid \text{la classe de conjugaison associée à } g \text{ est } c\}| \sim \frac{|c|}{|\mathrm{SL}_m(\mathbf{F}_p)|}$$

quand $p \to +\infty$, pour m fixé et toute classe de conjugaison c, c'est une situation où (26) est vérifié avec la mesure de probabilité uniforme ν_p sur $\mathrm{SL}_m(\mathbf{F}_p)$. On peut alors prouver que le groupe de Galois est aussi grand que possible avec probabilité tendant exponentiellement vite vers 1 (voir [52], [35, Th. 7.12] et un travail récent avec F. Jouve et Zywina [32], pour un énoncé très général, où le groupe de Weyl de l'adhérence de Zariski de Λ joue le rôle de groupe de Galois typique).

Et pour conclure, très récemment, Lubotzky et Meiri [41] ont utilisé le grand crible (avec le résultat d'expansion de Salehi Golsefidy et Varjú [53]) pour prouver que si Γ est un sous-groupe de type fini de $\mathrm{GL}_m(\mathbf{C})$ qui n'est pas virtuellement résoluble, on a

$$\mathbf{P}(X_k \text{ est de la forme } \gamma^m \text{ pour un } \gamma \in \Gamma \text{ et un } m \geqslant 2) \ll \exp(-\beta k)$$

pour toute marche au hasard (X_k) sur Γ définie à l'aide d'un système de générateurs S de Γ (symétrique et avec $1 \in \Gamma$), où $\beta > 0$ dépend de S. Cet énoncé n'a pas d'analogue évident dans le crible classique, et est une réciproque (forte) à un théorème de Mal'cev. La preuve fait appel a beaucoup de résultats profonds de théorie des groupes, en plus du crible, et on peut donc voir ce théorème comme une excellente illustration de l'utilité potentielle des idées de crible, *en tant qu'outil*, dans l'étude des groupes discrets.

6.3. Crible pour Frobenius sur les corps finis

Le crible en orbites de la Section 4 présente aussi certaines analogies avec des questions d'arithmétique sur les corps finis, concernant les propriétés de l'action d'automorphismes de Frobenius associés à des familles de variétés algébriques sur les corps finis. Dans ce contexte, le rôle de la propriété d'expansion des graphes de Cayley est joué par l'hypothèse de Riemann sur les corps finis, utilisée (avec des estimations de nombres de Betti ad-hoc) pour obtenir une forme quantitative et uniforme du théorème d'équirépartition de Chebotarev (qui est analogue au Théorème 5.8). On renvoie à [35, §8, App. A] pour une description précise et certaines applications, en particulier via les inégalités de grand crible (qui remontent implicitement à un article de Chavdarov [10]). Mentionnons juste une question typique qui peut être traitée : étant donné un polynôme $f \in \mathbf{F}_p[X]$ de degré $2g \geqslant 2$ sans facteur multiple, et la famille de courbes hyperelliptiques définies par

$$C_t \,:\, y^2 = f(x)(x-t)$$

où t est le paramètre, combien y a-t-il de $t \in \mathbf{F}_{p^\nu}$ tels que $|C_t(\mathbf{F}_{p^\nu})|$ soit un nombre premier, ou presque premier ?

On peut aussi considérer le cas d'une variété algébrique fixée, définie sur un corps de nombre, et la variation avec p de ses réductions modulo p. Les principes du « crible pour Frobenius »

(dans une direction horizontale) sont applicables, mais souffrent de l'absence de l'Hypothèse de Riemann, et les résultats inconditionnels sont assez faibles (voir [10] et [61]).

7. REMARQUES, PROBLÈMES ET CONJECTURES

Finalement, voici quelques questions et problèmes ouverts qui semblent d'un grand intérêt.

(1) [Classes de conjugaison] Soit $\Lambda \subset \mathrm{SL}_m(\mathbf{Z})$ un sous-groupe Zariski-dense, d'indice infini. Les méthodes décrites ci-dessus permettent d'obtenir des informations – des théorèmes ou des conjectures étayées par des indices convaincants – concernant la distribution et certaines propriétés des éléments de Λ, qui peuvent être comparées à celles de tout les éléments de $\mathrm{SL}_m(\mathbf{Z})$. On peut alors demander : qu'en est-il de l'ensemble des *classes de conjugaison* de Λ ? Cela semble une question naturelle, mais même pour $m = 2$, il ne semble pas que l'on sache grand chose à ce sujet...

(2) [Équirépartition forte pour la métrique des mots] Il serait très intéressant de pouvoir obtenir une version de la partie (3) du Théorème 5.4 pour la métrique des mots (sans pondération), lorsque Λ est un groupe assez général à croissance exponentielle (en particulier, loin d'être libre).

(3) [Bornes explicites] Ce survol s'est concentré sur les aspects généraux du crible en expansion. On a pu voir que, du point de vue des énoncés de crible utilisés, les résultats obtenus sont relativement simples. On peut penser que des efforts importants seront maintenant consacrés à l'amélioration des énoncés généraux, en particulier pour obtenir des bornes *explicites*[(24)] pour les nombres de saturation dans diverses situations. Des exemples dus à Nevo-Sarnak et Gorodnik-Nevo ont été mentionnés, dans le cas des réseaux et du comptage archimédien. Clairement, atteindre cet objectif passe nécessairement d'abord par la preuve d'un énoncé d'expansion également explicite (comme le fameux $\lambda_1 \geqslant 3/16$ de Selberg). Ainsi, il serait très intéressant d'avoir, par exemple, une version complètement effective du Théorème 5.8 (pour commencer, par exemple, pour SL_2) dans lequel la constante d'expansion pour les quotients de congruence est une fonction explicite, disons, des coefficients des matrices de l'ensemble de générateurs S. E. Breuillard a fait remarquer que les méthodes menant au théorème d'expansion sont, en principe, effective : il n'y a pas ici, a priori, de difficulté similaire aux hypothétiques zéros de Landau-Siegel dans la théorie des nombres premiers en progression arithmétique. Mais dans un cadre aussi général que [53], il y a tout de même des questions délicates de géométrie algébrique effective.

(4) [Raffinements] Lorsqu'un trou spectral explicite est connu, on peut envisager l'application de formes hautement raffinées de crible ; pour un exemple, voir l'article de Liu et Sarnak [39] concernant le crible appliqué aux points entiers sur des quadriques en trois variables.

Dans cet ordre d'idée, il serait extrêmement intéressant d'avoir des exemples où la forme bilinéaire du terme de reste dans le crible de dimension un, découverte par Iwaniec, serait exploitée (voir [16, §12.7]). De même, il serait remarquable d'avoir des applications où le niveau de distribution serait obtenu, ou amélioré, par une exploitation non-triviale de la

(24) C'est-à-dire, de « vrais nombres », comme 10, 100 ou 1000, dans une situation concrète, comme le groupe L et le polynôme $f(\gamma) =$ produit des coordonnées.

moyenne sur d des termes de reste r_d (rappelons que c'est là le cœur du théorème de Bombieri-Vinogradov).

(5) [Nombres premiers ?] Dans beaucoup de cas, lorsqu'aucune obstruction de congruence ne se présente, on peut s'attendre à ce que le nombre de saturation soit 1, c'est-à-dire, qu'une orbite contienne un ensemble Zariski-dense de points x tels que $f(x)$ soit (au signe près) un nombre premier.[(25)]. Bourgain, Gamburd et Sarnak proposent [4, Conjecture 1.4] une conjecture assez générale dans ce sens, concernant même la valeur exacte du nombre de saturation. L'article de Fuchs et Sanden [18, Conj. 1.2, 1.3] donne deux versions quantitatives précises pour les courbures premières dans un empilement de cercle Apollonien. Leurs arguments illustrent que de telles conjectures sont plutôt subtiles.

On connaît quelques résultats, mais ceux-ci sont obtenus par des méthodes qui sont plus directement comparables avec celles de Vinogradov et avec la méthode du cercle, qu'avec les méthodes de crible. Nevo et Sarnak [46, Th. 1.4] trouvent un ensemble Zariski-dense de $V_{m,n}$ (voir (5.11)) où toutes les coordonnées de la matrice sont des nombres premiers (au signe près), sous la condition – nécessaire – que $n \equiv 0 \pmod{2^{m-1}}$. Bourgain et Kontorovich [6] montrent (entre autres) que l'ensemble des entiers apparaissant comme (valeur absolue) du coefficient en bas à droite d'un élément d'un sous-groupe Zariski-dense de $\mathrm{SL}_2(\mathbf{Z})$ dont l'ensemble limite a une dimension assez proche de 1, contient tout les entiers positifs $\leqslant N$, avec $\ll N^{1-\delta}$ exceptions, lorsque N est assez grand ; en particulier, cet ensemble contient une infinité de nombres premiers.

On peut aussi se demander *quelle est la force de tels énoncés ?* Que disent-ils au sujet des nombres premiers ? Le seul indice dont l'auteur ait connaissance dans cette direction est le fait suivant, qui est assez indirect : Friedlander et Iwaniec ont démontré (voir [16, §14.7]) que l'on peut obtenir la proportion attendue de matrices

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$$

avec

$$a^2 + b^2 + c^2 + d^2 = p \text{ premier}, \ p \leqslant X,$$

sous l'hypothèse d'une forme convenable de la conjecture d'Elliott-Halberstam (précisément, il faut un niveau de distribution $Q = X^{1/2+\delta}$, avec un certain $\delta > 0$, pour les nombres premiers $p \leqslant X$). Il s'agit là, évidemment, d'un type – particulier – de crible en orbite. L'hypothèse ainsi faite est considérée comme très probablement valide, mais elle est également entièrement hors de portée. On sait, par exemple, après les travaux de Goldston, Pintz et Yıldırım, qu'une telle hypothèse implique aussi l'existence d'une infinité d'écarts bornés entre nombres premiers successifs (voir, par exemple, [16, Th. 7.17]).

APPENDICE: À QUOI RESSEMBLE UN ENTIER « TYPIQUE »

On rappelle ici très brièvement les estimations les plus fondamentales concernant la structure multiplicative des entiers. Ceux-ci servent de point de comparaison pour tout énoncé concernant la distribution des facteurs premiers des éléments d'un ensemble d'entier. Bien

[(25)] Il est expliqué dans [4, §2.3] pourquoi on ne peut pas espérer distinguer le signe en toute généralité.

entendu, tout les résultats ci-dessous sont connus sous des formes beaucoup plus fines et plus fortes.

- Le nombre de nombres premiers $p \leqslant X$ est asymptotiquement équivalent à $X/(\log X)$ quand $X \to +\infty$ (le Théorème des Nombres Premiers).
- Plus généralement, pour $k \geqslant 1$ (fixé), le nombre d'entiers $n \leqslant X$ qui sont produit de k (ou d'au plus k) facteurs premiers est asymptotiquement équivalent à
$$\frac{1}{(k-1)!}\frac{X(\log\log X)^{k-1}}{(\log X)}.$$
- Par contre, pour $k \geqslant 1$ (fixé), le nombre d'entiers $n \leqslant X$ qui n'ont *pas de facteur premier* $p \leqslant X^{1/k}$ est d'ordre de grandeur $\asymp X/(\log X)$. Cet ensemble est évidemment un sous-ensemble du précédent (lorsque ce dernier est défini avec $\leqslant k$ facteurs premiers), mais la restriction concernant la taille des facteurs est plus forte que celle concernant leur nombre, et en particulier l'ordre de grandeur[(26)] devient insensible à la valeur de k.
- Le nombre « typique » de facteurs premiers d'un entier $n \leqslant X$ est $\log\log X$; plus précisément, on a la majoration de Hardy-Ramanujan
$$\sum_{n\leqslant X}\Big(\Omega(n) - \log\log X\Big)^2 \ll X\log\log X,$$
qui implique, par exemple, qu'il y a seulement
$$\ll \frac{X}{\log\log X}$$
entiers $\leqslant X$ avec $|\Omega(n) - \log\log X| \geqslant (\log\log X)/2$.

RÉFÉRENCES

[1] N. BOURBAKI – *Fonctions d'une variable réelle*, Paris, Hermann, 1976.

[2] J. BOURGAIN et E. FUCHS – *A proof of the positive density conjecture for integer Apollonian circle packing*, prépublication (2010), `arXiv:1001.3894`

[3] J. BOURGAIN et A. GAMBURD – *Uniform expansion bounds for Cayley graphs of* $\mathrm{SL}_2(\mathbf{F}_p)$, Ann. of Math. 167 (2008), 625–642.

[4] J. BOURGAIN, A. GAMBURD et P. SARNAK – *The affine linear sieve*, Invent. math. 179 (2010), 559–644.

[5] J. BOURGAIN, A. GAMBURD et P. SARNAK – *Generalization of Selberg's* 3/16 *Theorem and affine sieve*, prépublication (2010), `arXiv:0912.5021`

[6] J. BOURGAIN et A. KONTOROVICH – *On representations of integers in thin subgroups of* $\mathrm{SL}(2,\mathbf{Z})$, prépublication (2010), `arXiv:1001.4534`.

[7] J. BOURGAIN et P. VARJÚ – *Expansion in* $\mathrm{SL}_d(\mathbf{Z}/q\mathbf{Z})$, *q arbitrary*, prépublication (2010), `arXiv:1006.3365`.

[8] E. BREUILLARD, B. GREEN et T. TAO – *Linear approximate groups*, prépublication (2010), `arXiv:1005.1881`.

[9] M. BURGER – *Petites valeurs propres du Laplacien et topologie de Fell*, PhD Thesis (1986), Econom Druck AG (Basel).

(26) Mais pas la formule asymptotique que l'on peut démontrer !

[10] N. CHAVDAROV – *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy*, Duke Math. J. 87 (1997), 151–180.

[11] L. CLOZEL –*Démonstration de la conjecture τ*, Invent. math. 151 (2003), 297–328.

[12] W. DUKE, Z. RUDNICK et P. SARNAK – *Density of integer points on affine homogeneous varieties*. Duke Math. J. 71 (1993), 143–179.

[13] N. DUNFIELD et W. THURSTON – *Finite covers of random: 3-manifolds*, Invent. math. 166 (2006), 457–521.

[14] J. ELLENBERG, C. HALL et E. KOWALSKI – *Expander graphs, gonality and variation of Galois representations*, prépublication (2010), `arXiv:1008.3675`.

[15] A. ESKIN et C. McMULLEN – *Mixing, counting, and equidistribution in Lie groups*, Duke Math. J. 71 (1993), 181–209.

[16] J. FRIEDLANDER et H. IWANIEC – *Opera de cribro*, Colloquium Publ. 57, A.M.S, 2010.

[17] E. FUCHS – *Strong approximation in the Apollonian group*, prépublication (2009).

[18] E. FUCHS et K. SANDEN – *Some experiments with integral Apollonian circle packings*, J. Experimental Math., to appear.

[19] A. GAMBURD – *On the spectral gap for infinite index « congruence » subgroups of* $\mathrm{SL}_2(\mathbf{Z})$, Israel J. Math. 127 (2002), 157-–200.

[20] N. GILL et H. HELFGOTT – *Growth of small generating sets in* $\mathrm{SL}_n(\mathbf{Z}/p\mathbf{Z})$, prépublication (2010); `arXiv:1002.1605`

[21] A. GORODNIK et A. NEVO – *The ergodic theory of lattice subgroups*, Annals of Math. Studies 172, Princeton Univ. Press, 2009.

[22] A. GORODNIK et A. NEVO – *Lifting, restricting and sifting integral points on affine homogeneous varieties*, prépublication (2010).

[23] R. GRAHAM, J. LAGARIAS, C. MALLOWS, A. WILKS et C. YAN – *Apollonian circle packings: number theory*, J. Number Theory 100 (2003), 1–45, `arXiv:math/0009113v2`.

[24] B. GREEN – *Approximate groups and their applications: work of Bourgain, Gamburd, Helfgott and Sarnak*, Current Events Bulletin of the AMS, 2010.

[25] B. GREEN et T. TAO – *Linear equations in primes*, Annals of Math. 171 (2010), 1753-–1850.

[26] H. HELFGOTT – *Growth and generation in* $\mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z})$, Ann. of Math. 167 (2008), 601–623.

[27] H. HELFGOTT – *Growth in* $\mathrm{SL}_3(\mathbf{Z}/p\mathbf{Z})$, J. European Math. Soc. (à paraître).

[28] S. HOORY, N. LINIAL et A. WIGDERSON – *Expander graphs and their applications*, Bull. A.M.S 43 (2006), 439–561.

[29] E. HRUSHOVSKI – *Stable group theory and approximate subgroups*, prépublication (2010), `arXiv:0909.2190`.

[30] E. HRUSHOVSKI et A. PILLAY – *Definable subgroups of algebraic groups over finite fields*, J. reine angew. Math 462 (1995), 69–91.

[31] H. IWANIEC et E. KOWALSKI – *Analytic Number Theory*, Colloquium Publ. 53, A.M.S, 2004.

[32] F. JOUVE, E. KOWALSKI et D. ZYWINA – *Splitting fields of characteristic polynomials of random elements in arithmetic groups*, prépublication, `arXiv:1008.3662`

[33] A. KONTOROVICH et H. OH – *Apollonian circle packings and closed horospheres on hyperbolic* 3*-manifolds*, prépublication (2008), `0811.2236v4`

[34] A. KONTOROVICH et H. OH – *Almost prime Pythagorean triples in thin orbits*, prépublication (2010), `arXiv:1001.0370`.

[35] E. KOWALSKI – *The large sieve and its applications*, Cambridge Tracts in Math. 175, Cambridge Univ. Press, 2008.

[36] M. LARSEN et R. PINK – *Finite subgroups of algebraic groups*, prépublication (1998), `http://www.math.ethz.ch/~pink/ftp/LP5.pdf`

[37] P. LAX et R. PHILIIPS – *The asymptotic distribution of lattice points in Euclidean and non-Euclidean spaces*, Journal of Functional Analysis 46 (1982), 280–350.

[38] J.S. LI – *The minimal decay of matrix coefficients for classical groups*, Math. Appl., 327, Kluwer, (1995), 146–169.

[39] J. LIU et P. SARNAK – *Integral points on quadrics in three variables whose coordinates have few prime factors*, Israel J. of Math, à paraître.

[40] A. LUBOTZKY – *Discrete groups, expanding graphs and invariant measures*, Progress in Math. 125, Birkaüser 1994.

[41] A. LUBOTZKY et C. MEIRI – *Sieve methods in group theory I: powers in linear groups*, prépublication (2010).

[42] J. MAHER – *Random Heegard splittings*, Journal of Topology, à paraître.

[43] O. MARFAING – *Sieve and expanders*, Rapport de stage de Master, ETH Zürich et Université Paris Sud, 2010.

[44] C. MATTHEWS, L. VASERSTEIN et B. WEISFEILER – *Congruence properties of Zariski-dense subgroups*, Proc. London Math. Soc. (3) 48 (1984), no. 3, 514–532.

[45] F. MAUCOURANT – *Homogeneous asymptotic limits of Haar measures of semisimple linear groups and their lattices*, Duke Math. J. 136 (2007), 357–399.

[46] A. NEVO et P. SARNAK – *Prime and almost prime integral points on principal homogeneous spaces*, prépublication (2010).

[47] M.V. NORI – *On subgroups of* $GL_n(\mathbf{F}_p)$, Invent. math. 88 (1987), 257–275.

[48] H. OH – *Uniform pointwise bounds for matrix coefficients of unitary representations and applications to Kazhdan constants*, Duke Math. J. 113 (2002), 133–192.

[49] H. OH – *Dynamics on geometrically finite hyperbolic manifolds with applications to Apollonian circle packings and beyond*, Proc. ICM Hyderabad, India, 2010, `arXiv:1006.2590`.

[50] F. PAULIN – *Sur les automorphismes de groupes libres et de groupes de surface*, Séminaire Bourbaki, Exp. 1023 (2010).

[51] L. PYBER et E. SZABÓ – *Growth in finite simple groups of Lie type of bounded rank* prépublication (2010), `arXiv:1005.1858v1`

[52] I. RIVIN – *Counting Reducible Matrices, Polynomials, and Surface and Free Group Automorphisms*, Duke Math. J. 142 (2008), 353–379.

[53] A. SALEHI GOLSEFIDY et P. VARJÚ – *Expansion in perfect groups*, prépublication (2010).

[54] P. SARNAK – *Affine sieve*, notes d'un exposé fait Juin 2010, `http://www.math.princeton.edu/sarnak/Affine crible summer 2010.pdf`

[55] P. SARNAK – *Notes on the generalized Ramanujan conjectures*, in « Harmonic Analysis, The Trace Formula, and Shimura Varieties », Clay Math. Proceedings, vol. 5, A.M.S 2005; edited by J. Arthur, D. Ellwood et R. Kottwitz; `http://www.math.princeton.edu/sarnak/FieldNotesCurrent.pdf`

[56] P. SARNAK et X. XUE – *Bounds for multiplicities of automorphic representations*, Duke Math. J. 64, (1991), 207–227.

[57] J-P. SERRE – *Topics in Galois theory*, Res. Notes in Math. 1, A.K. Peters, 2008.

[58] Y. SHALOM – *Expander graphs and invariant means*, Combinatorica 17 (1997), 555–575.

[59] P. VARJÚ – *Expansion in* $\mathrm{SL}_d(O_K/I)$*, I squarefree*, prépublication (2010), `arXiv:1001.3664`.

[60] B. WEISFEILER – *Strong approximation for Zariski-dense subgroups of semi-simple algebraic groups*, Annals of Math. 120 (1984), 271–315.

[61] D. ZYWINA – *The large sieve and Galois representations*, prépublication, `arXiv:0812.2222`.

Emmanuel KOWALSKI

ETH Zürich – DMATH
Rämistrasse 101
8092 Zürich, Switzerland
E-mail : `kowalski@math.ethz.ch`