Habilitation à Diriger des Recherches

en Sciences Mathématiques

présentée à

l'Université des Sciences et Technologies de Lille

par

Gautami Bhowmik

FONCTIONS DIVISEURS DE MATRICES

Soutenue le 28 Octobre 1997 devant le jury composé de :

Paula COHEN,	Université de Lille I, rapporteur
Jean-Claude DOUAI,	Université de Lille I, directeur de recherche
Aloys KRIEG,	RWT Hochschule, Aachen , rapporteur
Thomas LAFFEY,	University College, Dublin
Hervé QUEFFELEC,	Université de Lille I
Marc REVERSAT,	Université de Toulouse
Michel WALDSCHMIDT,	Université de Paris VI-Jussieu, rapporteur

Fonctions diviseurs de matrices

Plan

I. Introduction.

L'étude des propriétés arithmétiques des matrices à coefficients dans un corps de nombres algébrique a été commencée par Siegel dans les années 30, dans le contexte des formes quadratiques et des fonctions modulaires de degré supérieur, cf [S1] et [S2]. Les spécificités de cette arithmétique sont d'une part la non-commutativité, l'existence de diviseurs de zéro et celle d'éléments non-inversibles et d'autre part la décomposition par blocs qui est souvent un avantage.

Les matrices rectangulaires apparaissent naturellement lorsque l'on opère avec des formes modulaires, précisément lorsque l'on souhaite utiliser une décomposition par blocs. Le développement de Fourier d'une forme modulaire de Siegel peut s'écrire à partir de la décomposition $Z = \begin{pmatrix} Z_0 & Z_1 \\ {}^tZ_1 & Z_2 \end{pmatrix}$ où Z_0 se situe dans le demi-plan hyperbolique $\mathbb{H}_m$ (constitué des matrices $m \times m$ symétriques complexes de partie imaginaire définie positive), Z_2 est dans $\mathbb{H}_{n-m}$ et Z_1 dans $\mathbb{C}^{(m,n-m)}$. Il vient

$$f(Z) = \sum_{T_2} \phi_{T_2}(Z_0, Z_1) \exp i\pi \operatorname{tr}(T_2 Z_2)$$

où les ϕ_{T_2} sont des fonctions holomorphes appelées coefficients de Fourier-Jacobi et qui sont données par

$$\phi_{T_2}(Z_0, Z_1) = \sum_{T = \begin{pmatrix} T_0 & T_1 \\ {}^tT_1 & T_2 \end{pmatrix}} a(T) \exp i\pi \operatorname{tr}(T_0 Z_0 + 2\,{}^tT_1 Z_1).$$

Ceci nous amène directement à considerer aussi l'arithmétique des matrices rectangulaires si l'on souhaite tirer partie de la décomposition par blocs. A ce niveau nous rencontrons les matrices "primitives" qui généralisent la notion de matrices unimodulaires (voir [Fr] par exemple) et qui sont définies dans ce contexte comme la troncature de matrices de $\mathrm{GL}_r(\mathbb{Z})$. De façon plus prosaïque, Kohnen, Böcherer ou Dabrowski ([Ko], [Bo] et [Da]) parmis d'autres, lorsqu'ils cherchent à calculer les séries de Poincaré du groupe modulaire de Siegel $\mathrm{Sp}_m(\mathbb{Z})$, ont directement à utiliser des matrices primitives et l'arithmétique afférante.

Les bases de cette arithmétique ont été établies par Siegel. Il a introduit les concepts d'unités, d'équivalence unilatérale et bilatérale et de classes de congruence pour des matrices rectangulaires. Maass [Ma] a continué cette étude et Kaplansky [Ka] s'est intéressé à plusieurs propriétés arithmétiques. Plus récemment, Newmann et Thompson ([Ne], [T1–3]) ont travaillé sur les classes de matrices, étudié les notions de pgcd et de ppcm, etc (voir aussi Hua [H]). Koecher [Koe] dans le manuscript non-publié de son livre examine les propriétés des matrices entières d'un point de vue plus algébrique. Nanda [N1–4] a travaillé à mettre les notions proprement arithmétiques en place. Dans un livre en préparation [BN], nous systématisons cette étude.

La notion de fonction arithmétique a été formellement introduite par Nanda [N4] comme étant des fonctions χ à valeurs complexes des doubles classes d'équivalence satisfaisant de plus à $\chi \begin{pmatrix} 1 & 0 \\ 0 & M \end{pmatrix} = \chi(M)$. Ces fonctions incluent notamment les fonctions de diviseurs, la fonction de Möbius, les fonctions constantes et les fonctions généralisées d'Euler et de Ramanujan. Cette dernière fonction apparaît au niveau

des coefficients de Fourier des séries d'Eisenstein associées à $\mathrm{Sp}_m(\mathbb{Z})$. Des résultats partiels concernant son évaluation ont été obtenus par Ramanathan & Subbarao [RS], et l'évaluation complète par Nanda [N3]. Elles sont souvent multiplicatives, ce par quoi nous entendons qu'elles vérifient $\chi(MN) = \chi(M)\chi(N)$ dès que M et N ont des discriminants premiers entre eux. Muni du produit de convolution $\star$ défini par

$$(\chi_1 \star \chi_2)(M) = \sum_{M_1 \text{ une classe de diviseurs de } M} \chi_1(M_1)\chi_2(M_1^{-1}M)$$

l'ensemble des fonctions arithmétiques forme une algèbre commutative.

Mes travaux ont pour but la compréhension de ce produit de convolution. A partir de maintenant, nous opérons avec des matrices à coefficients entiers bien que presque tous les résultats restent vrais sur des anneaux principaux dont chaque idéal a un anneau résiduel fini et peuvent de plus s'étendre aux anneaux de Dedekind.

Afin de comprendre ce produit de convolution, je me suis intéressée aux fonctions pondérées de diviseurs définies par $\sigma_a(M) = \sum_{M_1} (\det M_1)^a$ où M_1 est une classe de diviseurs de M, communément M_1 est en forme normale d'Hermite (voir partie II). Si les fonctions arithmétiques sont souvent difficiles à évaluer ponctuellement, les fonctions de diviseurs se sont révélées particulièrement résistantes. Ce n'est que récemment que j'ai réussi cette évaluation, et ce en utilisant principalement une formule de récurrence reliant trois valeurs de $\sigma_a(M)$, a et M variant.

Parallèlement et avec un co-auteur, nous avons exhibé une bijection naturelle entre classes de diviseurs d'une matrices et diviseurs d'un réseau associé à cette matrice, qui à son tour permet d'identifier une classe de diviseurs de M avec un sous-groupe d'un groupe abélien fini associé à M : à l'écriture $M = M_1M_2$, nous pouvons associé une suite exacte

$$0 \to \mathcal{C}_1(M_2) \to \mathcal{C}_1(M) \to \mathcal{C}_1(M_1) \to 0$$

où $\mathcal{C}_1(M)$ est le conoyau d'un endomorphisme de $\mathbb{Z}^r$ dont la matrice est M. Cette suite complète un résultat partiel de Thompson [T2]. La combinaison de ces résultats donne alors une façon simple de compter le nombre de sous-groupes d'un groupe abélien donné. Par ailleurs cette bijection nous a permis d'établir une bijection entre l'algèbre des fonctions arithmétiques et la complétion d'une algèbre de Hecke abstraite. Les avantages sont alors double : d'une part nous donnons une définition naturelle du produit de Hecke et d'autre part la structure de l'algèbre de Hecke nous permet d'en déduire celle de l'algèbre des fonctions arithmétiques.

La p-composante de cette algèbre de Hecke est aussi connue en combinatoire sous le nom d'algèbre de Hall, algèbre dont les polynômes de Hall $g^{\lambda}_{\mu,\nu}(p)$ sont les constantes de multiplication. Le polynôme $g^{\lambda}_{\mu,\nu}(p)$ donne le nombre de sous-groupes de type μ et cotype ν d'un p-groupe abélien fini de type λ (voir partie IV). Cet objet combinatoire est difficile à évaluer et notre approche nous permet d'en donner des propriétés via l'arithmétique matricielle. Dans l'autre sens, nous avons utilisé cette correspondance pour calculer l'indice d'une matrice, i.e. le nombre de formes normales d'Hermite équivalentes à une forme normale de Smith donnée, répondant ainsi à une question de Koecher [Koe] (l'argument utilisé dans [Kr] permettrait de montrer qu'il s'agit d'un polynôme en p, mais ne donne par exemple pas son degré).

Une autre façon d'aborder le sujet consiste à associer une série de Dirichlet à une fonction arithmétique et à essayer d'analyser comment cette série réagit au produit

de convolution (voir partie VI, VII et IX). A l'heure actuelle, nous n'avons pas élucidé ce comportement. Pour ce qui est de matrices 2×2, nous présentons une étude complète. La fonction de diviseurs est justifiable d'un traitement particulier, et il est raisonnable de penser que la compréhension de cette fonction devrait donner accès à la compréhension d'un produit de convolution quelconque (au moins de fonctions positives ou nulles). Avec plusieurs co-auteurs, nous avons traité de ce sujet et nous donnons ici les fonctions zéta associées, à un facteur "plus convergent" près.

Ces résultats nous permettent de déterminer le nombre moyen de sous-groupes des groupes abéliens finis de rang $\leq r$ et de cardinal $\leq x$ (voir partie VII). Nous donnons des résultats fins pour les termes d'erreurs, résultats que nous obtenons en utilisant des méthodes d'analyse réelle (sommes d'exponentielles) ou complexe. Par ailleurs nous avons aussi étudié l'ordre normal de $\mathrm{Log}\,\sigma_0$ à l'aide d'une généralisation de l'inégalité de Turàn-Kubilius qui englobent plusieurs résultats précédents (cf [Ell], [Hi] et [Ho]). Cet ordre normal ressemble à celui de la fonction de diviseurs sur $\mathbb{Z}$ alors que l'ordre moyen en est lui très loin.

Afin de comprendre comment nos séries de Dirichlet se comportent vis-à-vis du produit de convolution, nous avons émis l'hypothèse que si les facteurs locaux des séries associées à deux fonctions sont rationnels, alors il en est de même du facteur local du produit de convolution. Nous avons obtenu des résultats partiels en dimension 2 et le premier exemple en dimension r est celui de la fonction de diviseurs. Des questions similaires ont été abordées au niveau des sous-groupes de groupes abéliens sans torsion (cf [Lu]). En utilisant le principe de dualité, nous avons obtenue une seconde formule de récurrence (ce qui nous montre l'importance de la non-commutativité dans ce contexte) et la conjugaison des deux formules obtenues nous donne une troisième récurrence qui est elle très efficace, bien qu'elle fasse intervenir des dénominateurs et des termes positifs et négatifs (voir partie IX). A l'aide de ce nouvel outil, nous avons montré que la fonction zéta associée à la fonction de diviseurs est rationnelle. Cet outil donne par ailleurs un moyen très efficace pour calculer numériquement le nombre de sous-groupes de cardinalité fixée d'un groupe abélien fini, ce qui n'existait pas jusqu'à présent. A l'heure actuelle nous n'avons pas d'interprétation du numérateur.

Signalons pour finir que les idées développées ici, interprétées sur des matrices à coefficients dans un anneau de Dedekind doivent trouver un cadre naturel au niveau des formes modulaires de Hilbert ou de Hilbert-Siegel.

Pour conclure, je remercie Jean-Claude Douai d'avoir accepté d'être mon directeur de recherches ; Paula Cohen, Aloys Krieg et Michel Waldschmidt d'avoir accepté d'être rapporteurs ; Hervé Queffelec, Marc Reversat et Thomas Laffey pour leur participation au jury ; Olivier Ramaré pour le soutien mathématique, moral et éditorial !

Lille, le 30 Août 1997

II. Arithmétique matricielle.

Nous présentons ici les idées de base de l'arithmétique matricielle telle qu'elle a été pensée initialement par Siegel [S1], par Maass [Ma] puis développée notamment par Kaplansky [Ka]. Il n'existe à l'heure actuelle aucun livre reprenant de façon systématique ces notions ; il s'agit là de l'objet de [BN]. Nous ne considérons que des matrices sur $\mathbb{Z}$, mais toutes les notions introduites ici s'étendent au cas d'un anneau principal (sauf éventuellement le caractère fini de certaines quantités). Plus intéressant, ces notions et résultats ont des analogues sur les anneaux de Dedekind. Le lecteur trouvera une introduction élémentaire dans les livres de Hua [H] et de Newman [Ne].

Les unités.

En raison de la non-commutativité de la multiplication et de l'existence de matrices singulières, les unités pour la multiplication sont unilatérales et dépendent du rang. Une matrice idempotente G de même rang qu'une matrice donnée A et qui satisfait la condition $AG = A$ est appelée une unité à droite pour A. Si les coefficients de G appartiennent à $\mathbb{Q}$, nous dirons que G est une unité fractionnaire à droite, mais si ces coefficients appartiennent à $\mathbb{Z}$, nous l'appellerons une unité entière à droite, souvent écourté en unité à droite. Comme exemple, nous constatons que $G = \begin{pmatrix} 1 & 0 & 8 \\ 0 & 1 & -13 \\ 0 & 0 & 0 \end{pmatrix}$ est une unité à droite de la matrice $A = \begin{pmatrix} 2 & 1 & 3 \\ 5 & 3 & 1 \end{pmatrix}$. De façon similaire, si ${G^*}^2 = G^*$, si $\mathrm{rang}(G^*) = \mathrm{rang}(A)$ et si $G^*A = A$, nous dirons que G^* est une unité à gauche pour A. Elle est fractionnaire ou entière selon que ses coefficients appartiennent à $\mathbb{Q}$ ou à $\mathbb{Z}$.

En ce qui concerne les matrices non-singulières, leurs seules unités sont l'identité usuelle, c'est à dire $E_r = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ où r est le nombre de lignes (ou de colonnes).

Décomposition en produit.

Nous considérons une décomposition $A = MN$ comme licite si le nombre de colonnes de M égale le nombre de lignes de N et si il existe une unité (entière) à droite pour M qui soit aussi une unité à gauche pour N. Nous dirons alors que M et N admettent une unité simultanée (attention cette notion n'est pas symétrique !). Cette condition, qui n'apparaît pas sur des anneaux intègres, est nécessaire ici pour tenir compte des diviseurs de 0. A partir des idées développées dans la partie IV, il est possible de montrer que, si une unité simultanée existe, alors elle est unique. Deux matrices de même rang ayant une unité fractionnaire simultanée peuvent ne pas avoir d'unité simultanée et la factorisation résultante n'est pas considérée comme étant licite. Par exemple, $A = \begin{pmatrix} 6 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 1 & 0 \end{pmatrix} = MN$ mais il n'y a aucunes unités entières simultanées entre M et N (Il est facile de voir que les unités à droite de M sont de la forme $\begin{pmatrix} 1 & 0 \\ x & 0 \end{pmatrix}$; si cette matrice doit aussi être une unité à gauche pour N, alors il faut prendre $x = 1/3$). Laffey a montré [La] que toute matrice singulière s'écrit comme produit d'idempotents sur un anneau euclidien, ce qui montre clairement qu'une condition est nécessaire pour que le produit MN soit arithmétiquement intéressant. Remarquons finalement que dans

le cas de matrices non-singulières, la condition d'existence d'une unité simultanée est automatiquement satisfaite.

Inverses de Siegel et matrices primitives.

Nous nous tournons maintenant vers une notion assez courante en mathématiques, qui est celle d'inverse généralisé. L'inverse généralisé de Moore-Penrose par exemple est bien connu [Na]. Nous considérons un inverse bien adapté à notre situation : l'inverse de Siegel. Cet inverse dépend d'un choix d'unités à droite et à gauche. Plus précisément, supposons que les deux matrices entières A et X aient une unité simultanée G et que X et A aient une unité simultanée G^*. Supposons en outre que $XA = G$ et que $AX = G^*$. Alors nous appelons X l'inverse de Siegel de A (relativement aux unités G et G^*). Remarquons que la liste suivante d'égalités est satisfaite : $G^2 = G$, $G^{*2} = G^*$, $AG = A$, $G^*A = A$, $XG^* = X$, $GX = X$, $AX = G^*$ et $XA = G$. Si A admet un inverse de Siegel, A est dite primitive. Bien que X dépende de G et de G^*, son existence et le fait qu'elle soit entière sont eux indépendants des unités choisis. En ce qui concerne les matrices non-singulières, l'inverse de Siegel est l'inverse usuel et les matrices primitives sont les matrices unimodulaires.

Voici deux exemples : la matrice $A = \begin{pmatrix} 2 & 2 & 1 \\ 2 & 1 & 1 \end{pmatrix}$ est primitive ; en prenant $G^* = E_2$ et $G = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}$ qui sont des unités respectivement à gauche et à droite de A, la matrice $X = \begin{pmatrix} 0 & 0 \\ 1 & -1 \\ -1 & 2 \end{pmatrix}$ est son inverse de Siegel. Par contre la matrice $B = \begin{pmatrix} 2 & 0 \\ 0 & 2 \\ 0 & 0 \end{pmatrix}$ n'est pas primitive car, étant données des unités $G = E_2$ et $G^* = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, il n'y a aucun inverse entier bien qu'un inverse fractionnaire $X = \begin{pmatrix} 1/2 & 0 & 0 \\ 0 & 1/3 & 0 \end{pmatrix}$ existe. Nous pouvons établir que les matrices primitives ont un discriminant égal à 1 et que les matrices primitives de rang maximal sont précisément celles qui peuvent être complétées en des matrices unimodulaires, i.e. $P \in \mathbb{Z}^{(m,n)}$ de rang maximal est primitive si il existe une matrice $M \in \mathbb{Z}^{(m,m-n)}$ (ou dans $\mathbb{Z}^{(n-m,n)}$ selon que $m \geq n$ ou que $m < n$) telle que la matrice $\begin{pmatrix} P \\ M \end{pmatrix}$ (ou $\begin{pmatrix} P & M \end{pmatrix}$) soit dans $\mathrm{GL}_m(\mathbb{Z})$ (resp. dans $\mathrm{GL}_n(\mathbb{Z})$). Dans les exemples précédents, nous remarquons que $\begin{pmatrix} A \\ M \end{pmatrix}$ avec $M = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$ est unimodulaire, mais il n'y a aucune matrice M entière telle que $\begin{pmatrix} B & M \end{pmatrix}$ soit dans $\mathrm{GL}_3(\mathbb{Z})$.

Souvent (voir par exemple [Fr], [Ko], [Ma]), la condition de rang maximal n'est pas signalée et les matrices primitives sont alors définies comme troncature de matrices unimodulaires : un certain nombre de lignes ou de colonnes sont ôtées mais pas des deux. Si cette définition suffit pour exprimer les coefficients de Fourier-Jacobi de formes modulaires, elle a le défaut de ne pas préserver les propriétés arithmétiques : par exemple le produit de deux matrices primitives en ce sens n'est

plus nécessairement primitif en ce même sens, comme c'est le cas pour $A = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \end{pmatrix}$. De plus les matrices idempotentes ne sont pas primitives en ce sens.

Classes primitives unilatérales.

Nous disposons à présent de la notion de matrice primitive et nous nous tournons vers les propriétés proprement arithmétiques des matrices entières, propriétés qui se doivent d'être invariantes lorsque nous multiplions notre matrice par une matrice primitive (moyennant l'existence d'une unité simultanée). La non-commutativité du produit complique quelque peu les choses. Deux matrices A et B sont dites équivalentes à droite si il existe deux matrices entières M et N telles que $AM = B$ et $BN = A$. Si, en particulier, M et N sont primitives, nous disons que A et B sont primitivement équivalentes à droite. Il se trouve que dans le cas des anneaux de Dedekind, l'équivalence et l'équivalence primitive sont synonymes. Dans le cas de matrices non-singulières, nous pouvons remplacer l'équivalence primitive par l'équivalence unimodulaire.

Comme représentant particulier d'une classe d'équivalence primitive unilatérale, nous choisissons la forme normale d'Hermite. Un résultat classique de Hermite (1851) dit que chaque matrice est primitivement équivalente à droite, et ce de façon unique, à une matrice triangulaire $H = (h_{i,j})$ caractérisée par les conditions : $h_{i,i} \geq 0$, $h_{i+k,i} = 0$ pour $k \geq 0$, et $0 \leq h_{i,i+k} < h_{i,i}$. En particulier, si A est non-singulière, alors $h_{i,i} > 0$. La matrice H s'appelle la forme normale d'Hermite de la classe considérée et nous notons $H = \mathrm{FNH}(M)$.

Classes primitives bilatérales.

Nous nous tournons ensuite vers l'équivalence bilatérale. Deux matrices A et B sont bilatéralement équivalentes si il existe quatre matrices entières M_1, M_2, N_1 et N_2 telles que $M_1AM_2 = B$ et $N_1BN_2 = A$. Si M_1 et M_2 sont primitives, A et B sont dites primitivement équivalentes et nous définissons bien une relation d'équivalence de cette façon. Comme représentant particulier d'une classe bilatérale primitive, noux choisissons la célèbre forme normale de Smith. En 1861, Smith a établi que chaque matrice A est (unimodulairement et bilatéralement) équivalente, et ce de façon unique, à une matrice diagonale $S = \mathrm{diag}(s_i)$ telle que $s_i \geq 0$ et s_i divise s_{i+1} pour tout i. La matrice S s'appelle aussi un diviseur élémentaire et nous notons $S = \mathrm{FNS}(M)$. Pour une interpretation des invariants de Smith en termes du conoyau de A, voir par exemple [LR]. Le calcul des invariants de Smith repose en général sur la notion de "module discriminantaux" qui sont souvent malaisés à manipuler, mais Gerstein a introduit dans [Ge] une approche locale très souple. Signalons que chaque classe bilatérale contient un nombre fini de classes unilatérales. Koecher dans le manuscript de son livre [Koe] posait la question de calculer ce nombre. Nous répondrons à cette question plus loin.

Décomposition en facteurs premiers.

Une façon d'obtenir une écriture unique pour la décomposition d'une matrice consiste à utiliser les matrices P_r de $\mathbb{Z}^{(r,r)}$ telles que $P_r = \begin{pmatrix} E_j & 0 \\ 0 & pE_{r-j} \end{pmatrix}$ où p est un nombre premier. Par pré- ou post-multiplication par des matrices primitives si nécessaire, nous pouvons exprimer chaque matrice A, de façon unique, comme un produit de matrices P_r. Par exemple nous avons

$$A = \begin{pmatrix} 6 & 2 \\ 6 & 6 \end{pmatrix} = U \begin{pmatrix} 2 & 0 \\ 0 & 12 \end{pmatrix} V = U \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} V$$

où U et V sont unimodulaires. Notons qu'il est difficile de lire la décomposition d'un produit moyennant la connaissance de la décomposition de chacun des facteurs, ce qui rend marginale l'utilité de cette factorisation. Obtenir la forme normale de Smith de AB à partir de celles de A et de B est a priori impossible puisque plusieurs possibilités existent. Il est toutefois possible d'obtenir des renseignements sur la forme normale du produit (voir [Pr], [T1] et [T2]). Nous parlerons plus avant de ce sujet dans la partie V.

Classes de congruence.

Nous nous tournons maintenant vers la notion de classes de congruence. Donnons-nous une matrice non-singulière N et une de ses unités à gauche G^*. Deux matrices de même taille A et B vérifiant $G^*A = A$ et $G^*B = B$ sont dites congruentes modulo N (relativement à G^*) s'il existe une matrice D telle que $A - B = ND$. Remarquons que, contrairement à ce qui a été notre habitude jusqu'à présent, nous ne supposons pas qu'il y ait une unité simultanée entre N et D ; il s'agit là de l'un des rares cas où nous ne suivons pas cette convention. Nous écrivons $A \equiv B[N]$ et nous notons $\mathcal{C}_t(N, G^*)$ le groupe additif formé à partir des classes de congruence de matrices admettant t colonnes. Nous remarquons tout d'abord que si G_2^* est une autre unité à gauche de N les groupes $\mathcal{C}_t(N, G^*)$ et $\mathcal{C}_t(N, G_2^*)$ sont égaux, ce qui nous permet d'adopter la notation $\mathcal{C}_t(N)$. En outre les groupes $\mathcal{C}_t(N)$ et $\mathcal{C}_t(UNV)$ sont naturellement isomorphes dès que U et V sont unimodulaires. En prenant alors N en forme normale de Smith, nous constatons qu'il s'agit d'un groupe fini dont nous pouvons facilement déterminer la structure en fonction des invariants de Smith.

Nous disposons d'un théorème chinois reliant $\mathcal{C}_t(A)$ et $\mathcal{C}_t(B)$ dès que A et B sont de même taille et ont des déterminants premiers entre eux. Ce théorème dit qu'étant donnés X et Y ayant t colonnes, nous pouvons trouver Z satisfaisant à $Z \equiv X\ [A]$ et $Z \equiv Y\ [B]$. Si de plus A et B commutent, alors Z est déterminé de façon unique modulo AB.

Définissons à présent le sous-ensemble $\mathcal{R}_t(N)$ des classes premières à N. Deux matrices M et N sont dites premières entre elles si, dès qu'un triplet (D, H, K) vérifie $M = DH$ et $N = DK$, alors D est primitive. Une classe est dite première à N si il existe une matrice dans cette classe qui est première à N et nous vérifions qu'alors toute matrice dans cette classe est première à N.

Classes de congruence symétriques.

Les définitions précédentes ont des équivalents "symétriques" qui apparaissent au niveau des formes modulaires de Siegel (cf [Ma]). Pour ces définitions, il nous faut une matrice non-singulière N et deux unités de N, soit G une unité à droite et G^* une unité à gauche. Nous disons qu'une classe de congruence est symétrique par rapport à N si il existe une matrice B dans cette classe telle que $B\,{}^tN = N\,{}^tB$ et $B\,{}^tG = B$. Notons que cette définition n'a de sens que si B est carrée et de même taille que N. Nous disons alors que B et N forment une paire symétrique. Si r est le rang de N, nous dénotons par $\mathcal{C}(N)$ le sous-groupe de $\mathcal{C}_r(N)$ constitué des classes symétriques par rapport à N. Ce sous-groupe dépend à priori de G et de G^* mais nous montrons qu'il n'en est rien. Enfin nous dénotons par $\mathcal{R}(N)$ l'ensemble des classes de congruence modulo N qui sont symétriques par rapport à N et premières avec N. Il s'agit là de notions naturelles lorsque l'on étudie le groupe symplectique : dire que B forme une paire symétrique avec N et est premier à N équivaut tout simplement à dire que $\begin{pmatrix} N & B \end{pmatrix}$ est la moitié inférieure d'une

matrice symplectique.

Diviseurs.

Une idée centrale en arithmétique est celle de diviseurs. Nous avons déjà vu que, pour qu'une décomposition soit licite, nous avions besoin de l'existence d'unités simultanées. De plus, afin d'avoir un nombre fini de diviseurs, nous nous restreignons à compter les classes unilatérales de diviseurs. Par conséquent nous considérons des décompositions $A = BC$ où B est un représentant d'une classe d'équivalence primitive à droite. Communément nous prenons B en forme normale d'Hermite. Dans ce cas, nous appelons la classe primitive à droite de B une classe de diviseurs de A. Rappelons que cette definition tient bien compte des décompositions de A en produits de matrices singulières. Nous voyons par exemple que $A = \begin{pmatrix} 8 & 0 & 2 \\ 5 & 2 & 3 \\ 19 & 6 & 10 \end{pmatrix}$ est le produit de $M_1 = \begin{pmatrix} 2 & 0 \\ 1 & 1 \\ 4 & 3 \end{pmatrix}$ et de $M_2 = \begin{pmatrix} 4 & 0 & 1 \\ 1 & 2 & 2 \end{pmatrix}$ et vérifions qu'il existe une unité simultanée entre ces deux facteurs. Mais nous avons aussi $A = N_1 N_2$ où $N_1 = M_1 T$ et $N_2 = X M_2$ où T est une matrice primitive et X son inverse au sens de Siegel. En prenant par exemple

$$T = \begin{pmatrix} 1 & 2 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix} \quad \text{et} \quad X = \begin{pmatrix} 1 & -2 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

nous obtenons

$$A = N_1 N_2 = \begin{pmatrix} 2 & 4 & 0 & 0 & 0 \\ 1 & 3 & 1 & 0 & 0 \\ 4 & 11 & 3 & 0 & 0 \end{pmatrix} \begin{pmatrix} 2 & -4 & 0 \\ 1 & 2 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Fonctions arithmétiques et produit de convolution.

Pour détecter les propriétés arithmétiques, nous introduisons, en suivant [N4], la notion de fonction arithmétique. Une fonction χ sur l'ensemble des matrices entières et à valeurs dans $\mathbb{C}$ est dite arithmétique si d'une part $\chi(M)$ ne dépend que de la classe primitive bilatérale de M et si d'autre part $\chi \begin{pmatrix} 1 & 0 \\ 0 & M \end{pmatrix} = \chi(M)$. Parmi les exemples classiques, nous disposons de la fonction de diviseurs τ qui compte le nombre de classes diviseurs d'une matrice donnée, la fonction $\mathbb{1}$ constante égale à 1, son inverse la fonction de Möbius μ, diverses fonctions d'Euler, etc.

Nous définissons le produit de Dirichlet $\star$ sur l'ensemble des fonctions arithmétiques par

$$(\chi_1 \star \chi_2)(M) = \sum_{M = M_1 M_2} \chi_1(M_1)\chi_2(M_2)$$

où M_1 représente une classe de diviseurs de M, c'est à dire que nous le prenons en forme normale d'Hermite. L'ensemble des fonctions arithmétiques muni de

l'addition et du produit de convolution forme une algèbre commutative dont le groupe des inversibles est constitué des fonctions qui ne s'annulent pas sur E. L'identité pour le produit est bien sûr la fonction η qui vaut 1 sur toute matrice primitive et 0 ailleurs.

Les fonctions que l'on rencontrent naturellement sont presque toutes multiplicatives ce par quoi nous entendons qu'elles vérifient $\chi(MN) = \chi(M)\chi(N)$ dès que M et N sont multipliables et ont des discriminants premiers entre eux. L'ensemble des fonctions multiplicatives muni de convolution est un groupe abelien.

Il nous faut mentionner que les fonctions que nous rencontrons s'expriment souvent sous forme de produit de convolution. Par exemple on a $\tau = \mathbb{1} \star \mathbb{1}$ et $\mu \star \mathbb{1} = \eta$.

Pour évaluer une fonction arithmétique, il nous suffit de considérer sa valeur sur les matrices en forme normale de Smith puisque cette valeur ne dépend que de la classe d'équivalence primitive bilatérale. Nous pouvons ne considérer que des matrices non-singulières parce que les matrices $\begin{pmatrix} 0 & 0 \\ 0 & M \end{pmatrix}$ et M sont primitivement bilatéralement équivalentes. Lorsque nous opérons avec des fonctions multiplicatives, nous pouvons qui plus est nous restreindre aux formes normales de Smith dont le déterminant est la puissance d'un nombre premier. Typiquement nous considérons les matrices $F_r = \operatorname{diag}(p^{f_1}, \ldots, p^{f_1+\cdots+f_r}) = \langle f_1, \ldots, f_r \rangle_p$ où $f_1, \ldots, f_r$ sont des entiers positifs ou nuls et p un nombre premier.

Fonctions arithmétiques associées aux classes de congruence.

Parmi ces fonctions, nous avons les fonctions de norme, les fonctions d'Euler-Jordan et les fonctions de Ramanujan. Nous donnons un aperçu de ces fonctions.

La norme ν_t est tout simplement le cardinal de $\mathcal{C}_t(N)$, et l'on découvre que $\nu_t(N) = (\det N)^t$.

Sur $\mathbb{Z}$, Jordan a introduit et évalué la fonction qui compte le nombre de t-uplets qui sont incongruents modulo n et dont chaque composante est première à n. Le cardinal $\phi_t(N)$ de $\mathcal{R}_t(N)$ en est une généralisation en dimension r. Pour $t \geq r$, la valeur ponctuelle est donnée par

$$\phi_t(F_r) = |F_r|^t \left(1 - \frac{1}{p^t}\right)\left(1 - \frac{1}{p^{t-1}}\right) \cdots \left(1 - \frac{1}{p^{t-r+1}}\right),$$

ce qui étend bien le résultat classique $t = r = 1$. Remarquons que $\phi_t = \nu_t \star \mu$.

Nous définissons la norme symétrique comme étant le cardinal de $\mathcal{C}(N)$ et il est possible d'en donner une expression satisfaisante à partir de $\nu(p^g E_s) = p^{gs(s+1)/2}$. La fonction d'Euler symétrique a été introduite par Siegel et évaluée par Christian [Ch]. Il s'agit bien sûr du cardinal de $\mathcal{R}(N)$ et nous avons encore $\phi = \nu \star \mu$.

Jusqu'à présent nous n'avons évalué que des cardinaux et nous nous tournons à présent vers des sommes oscillantes. La première de ces sommes apparaît comme coefficient de Fourier de séries d'Einsenstein (pour les formes modulaires de Siegel, cf [Bo]) et il s'agit d'une généralisation de la somme de Ramanujan. Nous définissons, pour $M \in \mathbb{Z}^{(t,r)}$ et $N \in \mathbb{Z}^{(r,r)}$ non-singulière (avec $t \geq r$) la fonction

$$\rho(M, N) = \sum_{H \in \mathcal{R}(N)} e^{2i\pi \operatorname{tr}(HMN^{-1})}$$

et son t-analogue

$$\rho_t(M, N) = \sum_{H \in \mathcal{R}_t(N)} e^{2i\pi \operatorname{tr}(HMN^{-1})}.$$

Dans le cas $r = 2$, Ramanathan et Subbarao [RS] ont évalué $\rho(M, N)$ mais leur méthode (traduction des conditions en termes des coefficients des matrices) ne pouvaient s'étendre que difficilement au cas général. En utilisant les notions décrites ici, Nanda [N3] a pu procéder à l'évaluation complète de ces deux fonctions et comme pour les sommes de Ramanujan sur $\mathbb{Z}$, il exprime ρ_t en termes de la fonction d'Euler ϕ_t et de la fonction de Möbius pour obtenir ce que l'on appelle parfois la relation de Hölder. Si M et N sont deux matrices, nous disons que la matrice L est un pgcd à droite de M et N si il existe un triplet (L, H, K) tel que $M = HL$ et $N = KL$ et si pour tout autre triplet (L_2, H_2, K_2) vérifiant ces égalités, nous pouvons déterminer une matrice J satisfaisant $L = JL_2$. La classe primitive à gauche de ce pgcd est unique. Avec ces notations, nous avons

$$\rho_t(M, N) = \mu(NL^{-1})\phi_t(N)/\phi_t(NL^{-1}).$$

Remarquons que les fonctions de Ramanujan sont des fonctions de deux variables et que, à M fixé et N variable, la fonction obtenue n'est pas arithmétique au sens que nous prenons ici. Nous avons aussi les formules classiques

$$\rho_t(M, N) = \sum_{D|L} \mu(ND^{-1})\nu_t(D) \quad \text{et} \quad \rho(M, N) = \sum_{D|L} \mu(ND^{-1})\nu(D).$$

Si nous nous intéressons aux coefficients de Fourier-Jacobi de séries de Poincaré (pour les formes modulaires de Siegel, cf [Bo], [Da], [Ko]), nous obtenons des séries beaucoup plus compliquées sur lesquelles nous n'avons que peu de résultats jusqu'à présent. Pour en décrire un prototype, il nous faut définir l'inverse d'une classe de $\mathcal{R}(N)$. Si B et N forment une paire symétrique avec B premier à N, alors il existe X et Y telles que $BX + NY = E$. Nous définissons alors l'inverse de la classe de B, soit $\overline{B}$, comme étant la classe de ${}^tX$. Nous constatons que cette définition est cohérente et que nous définissons une involution sur $\mathcal{R}(N)$. Un exemple type de sommes à évaluer pour appréhender ces coefficients de Fourier-Jacobi est alors donné par

$$f(N) = \sum_{H \in \mathcal{R}(N)} e^{2i\pi \operatorname{tr}(N^{-1}(H+\overline{H}))}.$$

Il s'agit là d'une extension des sommes de Kloosterman.

III. Fonctions de diviseurs.

Pour comprendre et utiliser le produit de convolution, il est impératif de connaître la fonction τ qui donne le nombre de classes de diviseurs d'une matrice donnée. Depuis que l'étude systématique des fonctions arithmétiques a commencé, cette fonction est l'une des plus simples à exprimer et des plus difficiles à évaluer. Elle est simple à exprimer en termes de produit de convolution ($\tau = \mathbb{1} \star \mathbb{1}$), mais la difficulté est alors cachée dans le fait que l'on ne sait pas contrôler ce produit de convolution. En utilisant la multiplicativité de τ, une approche naïve nous dit qu'il s'agit de compter le nombre de solutions de l'équation

$$\begin{pmatrix} p^{f_1} & 0 & \dots & 0 \\ 0 & p^{f_1+f_2} & & \\ \vdots & & \ddots & \\ 0 & 0 & & p^{f_1+\dots+f_r} \end{pmatrix} = \begin{pmatrix} p^{a_1} & m_{1,2} & \dots & m_{1,r} \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & 0 & & p^{a_r} \end{pmatrix} M_2$$

avec $0 \leq m_{i,i+k} < p^{a_i}$.

Dans le cas $r = 2$, Narang en 1979 a donné une formule explicite pour τ. Nanda [N2] a aussi réussi en 1981 à évaluer τ si $f_1 = 1$ et $f_2 = \dots = f_r = 0$. Ces deux formules sont relativement simples. Dans le cas $r = 3$, nous avons établi dans [B1] une relation de récurrence entre $\tau\langle f_1, f_2, f_3\rangle_p$, $\tau\langle f_1, f_2, f_3 - 1\rangle_p$ et $\sigma_1\langle f_1, f_2\rangle_p$ où $\sigma_a(M)$ est le nombre pondéré de classes de diviseurs de M défini par

$$\sigma_a(M) = \sum_{M_1 M_2 = M} (\det M_1)^a$$

pour a dans $\mathbb{C}$. Cette relation permettait d'évaluer $\tau(F_3)$, mais sa démonstration était extrêment longue. Deux ans plus tard, nous avons obtenu [B3] une preuve beaucoup plus simple et plus générale basée sur la décomposition en blocs suivante : $F_r = \begin{pmatrix} F_{r-1} & 0 \\ 0 & p^{f_1+\dots+f_r} \end{pmatrix}$. La formule de récurrence obtenue s'écrit

$$\sigma_a\langle f_1, \dots, f_r\rangle_p = p^a \sigma_a\langle f_1, \dots, f_r - 1\rangle_p + \sigma_{a+1}\langle f_1, \dots, f_{r-1}\rangle_p.$$

Bien que cette formule nous a permis pour la première fois d'évaluer numériquement la fonction τ sur des matrices de rang 4, son utilisation récursive systématique rencontre l'obstacle que voici : dans notre formule, il est possible d'avoir $f_r - 1 = -1$, ce qui détruit la structure de forme normale de Smith nécessaire dans le membre de gauche de notre relation ; pour pouvoir la réappliquer, il faut alors retrouver la forme normale de Smith de la matrice correspondante. Il nous a fallu encore deux ans pour obtenir une bonne représentation graphique de cette récurrence et pour démontrer le résultat intermédiaire suivant :

$$\begin{aligned} \sigma_a\langle f_1, \dots, f_{r-k+1}, 0_{k-1}\rangle_p = \sum_{t=0}^{k-1} \begin{bmatrix} k \\ t \end{bmatrix}_p p^{a(k-t)} \sigma_{a+t}\langle f_1, \dots, f_{r-k+1} - 1, 0_{k-t-1}\rangle_p \\ + \sigma_{a+k}\langle f_1, \dots, f_{r-k}\rangle_p \end{aligned}$$

où $\begin{bmatrix} k \\ t \end{bmatrix}_p$ désigne le polynôme de Gauss en p. Notons que dans cette formule, la structure de forme normale de Smith n'est plus détruite puisque l'on peut supposer

$f_{r-k+1} \geq 1$. Ce résultat nous a permis dans [B5] de donner enfin une formule exacte pour $\sigma_a(F_r)$. Cette formule est assez compliquée bien qu'elle ne fasse intervenir que des polynômes de Gauss. Si a est un entier ≥ 0, $\sigma_a(F_r)$ est un polynôme entier en p, dont les coefficients sont positifs ou nuls et dépendent de $f_1, \ldots, f_r$ et de a. A titre d'exemple, nous avons

$$\begin{aligned}\sigma_0\langle 2,3,3,4\rangle_p =& 20p^{17} + 58p^{16} + 118p^{15} + 154p^{14} + 174p^{13} + 190p^{12} + 184p^{11} + 192p^{10} \\ &+ 176p^9 + 176p^8 + 150p^7 + 142p^6 + 106p^5 + 90p^4 + 72p^3 + 50p^2 + 26p + 28\end{aligned}$$

et

$$\begin{aligned}\sigma_2\langle 1,1,1,1\rangle_p =& 2p^{21} + 6p^{20} + 7p^{19} + 10p^{18} + 10p^{17} + 11p^{16} + 10p^{15} + 11p^{14} + 8p^{13} \\ &+ 9p^{12} + 7p^{11} + 6p^{10} + 5p^9 + 5p^8 + 3p^7 + 3p^6 + 2p^5 + 2p^4 + p^3 + p^2 + 1\end{aligned}$$

Remarquons que la suite des coefficients de σ_a n'est pas unimodale. Bien que qu'il soit difficile de donner une formule explicite pour chaque terme de ce polynôme, nous déterminons dans [BW2] son terme principal lorsque a est un entier. Plus précisément, le terme principal de $\sigma_a(F_r)$ s'écrit $\alpha(a,r)p^{\theta(a,r)}$ avec

$$\alpha(a,r) = \prod_{k=0}^{[(r-a)/2]} (f_{r-a-2k} + 1)$$

et

$$\theta(a,r) = \sum_{k=0}^{r-a-1} \left[\frac{(a+r-k)^2}{4}\right] f_{k+1} + a \sum_{k=r-a}^{r-1} (r-k) f_{k+1}$$

où $[n]$ représente la partie entière de n et où $f_t = 0$ si $t \leq 0$ (De plus la somme vide vaut 0 et le produit vide 1).

Nous connaissons aussi la somme des coefficients du polynôme $\sigma_a(F_r)$. Cette somme, très simple, est égale à $(f_1+1)(f_1+f_2+1)\ldots(f_1+\cdots+f_r+1)$, somme à laquelle nous nous réfèrerons en parlant de la valeur en $p=1$.

Ce sont ces deux renseignements (associés au fait que $\sigma_a(F_r)$ n'a pas de coefficients négatifs) qui nous permettent de construire une fonction zéta associée à $\sigma_a(F_r)$ et d'en déterminer l'abscisse de convergence. (En fait dans [BR1], nous ne disposions que de résultats moins précis mais qui suffirent). Nous reviendrons sur ce point plus loin.

IV. Diviseurs de réseaux et classes de diviseurs de matrices.

Jusqu'à présent, tous les résultats obtenus sur la fonction de diviseurs proviennent de la relation de récurrence. Avant d'en obtenir une formule complète, nous avions élaboré avec Ramaré une approche différente qui s'est révélée très fructueuse. Son point de départ consiste à étudier l'action de $\mathbb{Z}^{(r,r)}$ sur $\mathbb{Z}^r$. Il convient de signaler ici l'approche de Hua [H] qui consiste aussi à associer un module à une matrice ; si cette approche est duale de la nôtre, la différence est bien plus importante dans la mesure où toutes les constructions qui apparaissent naturelles ici (à commencer par l'invariance du module associé quand notre matrice parcourt une classe unilatérale) ne le sont plus lorsque l'on dualise.

Soit $\mathcal{B}$ une base de $\mathbb{Z}^r$ et soit ϕ_M l'endomorphisme de $\mathbb{Z}^r$ dont la matrice dans la base $\mathcal{B}$ soit M que nous supposons non-singulière. Nous remarquons tout d'abord que $V(M) = \phi_M(\mathbb{Z}^r)$ ne dépend que de la classe unimodulaire à droite de M, i.e. de sa forme normale d'Hermite. L'objet qui nous intéresse plus particulièrement est le conoyau de ϕ_M soit $\mathbb{Z}^r/V(M)$ dont nous constatons qu'il est déjà apparu sous le nom de $\mathcal{C}_1(M)$. Il s'agit d'un groupe abélien fini, qui ne dépend pas du choix de $\mathcal{B}$ et dont les facteurs invariants sont précisément ceux de M. Remarquons ici que, si M était singulière, le groupe qui nous intéresserait serait alors la partie de torsion du conoyau.

Donnons-nous à présent deux sous-réseaux (i.e. sous-module de rang maximal) W_1 et W_2 de $\mathbb{Z}^r$ et, en suivant [BR2], disons que W_1 est un diviseur à droite de W_2 si et seulement si $W_1 \supset W_2$. Nous remarquons que, bien que W_1 soit un diviseur de W_2, W_1 est plus grand au sens ensembliste que W_2. Considérons alors d'une part l'ensemble $RD(W)$ des diviseurs à droite du réseau W, qui est ordonné par l'inclusion, et d'autre part l'ensemble $RD(M)$ des classes de diviseurs à droite de M, ordonné par la division. Nous montrons dans [BR2] que l'application naturelle

$$\begin{array}{rcccc} \Theta & : & RD(M) & \to & RD(V(M)) \\ & & M_1 \cdot \mathrm{GL}_r(\mathbb{Z}) & \mapsto & \phi_{M_1}(\mathbb{Z}^r) \end{array}$$

est une bijection (et où $\mathrm{GL}_r(\mathbb{Z})$ désigne le groupe unimodulaire) d'ensembles ordonnés. Construire Θ^{-1} n'est d'ailleurs pas très difficile : tout réseau W s'écrit sous la forme $\phi_N(\mathbb{Z})$, et un petit calcul montre que $W \supset V(M)$ se traduit effectivement par $N|M$.

Il est possible de décrire un peu plus précisément cette situation. Si W_1 et W_2 sont deux sous-réseaux de $\mathbb{Z}^r$, nous appelons $\mathrm{GL}_r(\mathbb{Z})\cdot W_1$ un diviseur complémentaire de W_2 si il existe un épimorphisme de W_1 dans W_2. En notant $CD(W)$ l'ensemble des diviseurs complémentaires de W, nous pouvons construire une surjection Ψ de $RD(M)$ sur $CD(V(M))$ telle que $\Psi(M_1 \cdot \mathrm{GL}_r(\mathbb{Z})) = \mathrm{GL}_r(\mathbb{Z}) \cdot \phi_{M_1^{-1}M}(\mathbb{Z}^r)$. A termes, cela nous permet à partir d'une décomposition licite $M = M_1M_2$ d'obtenir une suite exacte

$$0 \to \mathcal{C}_1(M_2) \to \mathcal{C}_1(M) \to \mathcal{C}_1(M_1) \to 0.$$

Nous établissons ainsi une bijection entre le nombre de classes de diviseurs M_1 de M telles que $\mathrm{FNS}(M_1) = S_1$ et $\mathrm{FNS}(M_1^{-1}M) = S_2$ et le nombre de sous-groupes Γ de $\mathcal{C}_1(M)$ tels que $\Gamma \simeq \mathcal{C}_1(S_1)$ et $\mathcal{C}_1(M)/\Gamma \simeq \mathcal{C}_1(S_2)$. Nous avons découvert plus tard que Thompson avait déjà tenté une telle approche en 1985 (cf [T2]). Avec nos notations, il montre que si il existe une décomposition $M = M_1M_2$ avec $\mathrm{FNS}(M_1) = S_1$ et $\mathrm{FNS}(M_1^{-1}M) = S_2$, alors il existe un sous-groupe Γ de $\mathcal{C}_1(M)$

tel que $\Gamma \simeq \mathcal{C}_1(S_1)$ et $\mathcal{C}_1(M)/\Gamma \simeq \mathcal{C}_1(S_2)$. Notre résultat est donc plus complet dans la mesure où nous établissons une condition nécessaire et suffisante et où nous sommes de plus capables de le quantifier.

Nous détaillons un petit exemple. Considérons $M = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}$. Nous avons $\mathcal{C}_1(M) \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ et

$$RD(M) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}, \begin{pmatrix} p & x \\ 0 & 1 \end{pmatrix} (0 \leq x < p), \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} \right\}.$$

En prenant $\mathcal{B} = \{e_1, e_2\}$, nous obtenons

$$RD(V(M)) = \{\mathbb{Z}^2, \mathbb{Z} \cdot e_1 \oplus \mathbb{Z} \cdot pe_2, \mathbb{Z} \cdot (pe_1 + xe_2) \oplus \mathbb{Z} \cdot e_2 \ (0 \leq x < p), V(M)\}.$$

Nous vérifions alors que le nombre de classes de diviseurs de $\langle 1, 0 \rangle_p$ est $3+p$ et qu'il s'agit du nombre de sous-groupes de $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$.

Notre évaluation de $\sigma_0(F_r)$ donne donc une autre méthode, relativement simple, de compter le nombre de sous-groupes de

$$\mathbb{Z}/p^{f_1}\mathbb{Z} \oplus \mathbb{Z}/p^{f_1+f_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{f_1+f_2\cdots+f_r}\mathbb{Z}.$$

Nous détaillerons ce point plus avant dans les parties V et IX.

Notons que sur le treillis des réseaux, les notions de pgcd et de ppcm sont simples à décrire : il s'agit respectivement de la somme et de l'intersection, ce qui permet de retrouver des résultats de Thompson et de Nanda ([T3] et [N1]).

Cette interprétation est aussi efficace au niveau des matrices singulières et les notions d'unité et d'unité simultanée se comprennent particulièrement bien dans ce contexte : une unité à gauche est la matrice d'un projecteur sur $(\phi_M(\mathbb{Z}^r) \otimes \mathbb{Q}) \cap \mathbb{Z}^r$ (ce module admet un supplémentaire), une unité à droite celle d'un projecteur sur un supplémentaire de $\operatorname{Ker} \phi_M$. Pour qu'il y ait une unité simultanée entre A et B, il faut en conséquence avoir

$$((\phi_A(\mathbb{Z}^r) \otimes \mathbb{Q}) \cap \mathbb{Z}^r) \oplus \operatorname{Ker} \phi_B = \mathbb{Z}^r.$$

Notre but à présent est de donner une preuve de la formule de récurrence (cf partie III) en termes de groupes abéliens. Cette réécriture de la preuve dans le contexte des groupes n'est pas du tout immédiate, mais l'effort fait nous permettra plus loin d'obtenir des résultats très intéressants.

Donnons-nous un p-groupe abélien fini F_r d'exposant (le maximum de l'ordre de ses éléments) p^ℓ. Il existe alors un élément e_ℓ d'ordre p^ℓ dans F_r et un sous-groupe F_{r-1} de F_r tels que

$$F_r = F_{r-1} \oplus \mathbb{Z}e_\ell.$$

Considérons alors $G_r = F_{r-1} \oplus \mathbb{Z}pe_\ell$. Soit maintenant H un sous-groupe de F_r. Ou bien $H \subset G_r$ et alors H est un sous-groupe de G_r. Nous avons donc triviallement

$$\sum_{\substack{H \subset F_r \\ H \subset G_r}} |F_r/H|^a = p^a \sum_{H \subset G_r} |G_r/H|^a.$$

Ou bien $H \not\subset G_r$ et dans ce cas H contient un élément de la forme $e_\ell + y$ où $y \in F_{r-1}$. Pour dénombrer convenablement le nombre de sous-groupes ainsi obtenus, nous nous donnons un sous-groupe K de F_{r-1} et considérons la fonction

$$\begin{aligned} \{H \not\subset G_r, H \cap F_{r-1} = K\} &\to F_{r-1}/K \\ H &\mapsto y \mod K. \end{aligned}$$

Nous vérifions qu'il s'agit d'une bijection, ce qui nous donne

$$\sum_{\substack{H \subset F_r \\ H \not\subset G_r}} |F_r/H|^a = \sum_{K \subset F_{r-1}} |F_{r-1}/K| \cdot |F_{r-1}/K|^a.$$

En additionnant les deux formules obtenues, nous retrouvons notre relation de récurrence.

V. Algèbre de Hecke et algèbre de Hall

L'algèbre des fonctions arithmétiques en tant que complétée d'une algèbre de Hecke...

Jusqu'ici, nous avons surtout rencontré des formes modulaires de Siegel. Il se trouve que le cadre algébrique naturel du produit de convolution a vu naissance au niveau de l'algèbre de Hecke qui agit sur les formes modulaires usuelles. La théorie de ces algèbres va nous permettre de décrire plus avant la structure algébrique liée au produit de convolution. Par exemple, Cashwell & Everett ont montré en 1959 que l'algèbre des fonctions arithmétiques sur $\mathbb{Z}$ (i.e. en dimension $r = 1$), le produit étant celui de convolution, est factoriel. Dans [BR2], nous étendons ce résultat au cas $r \geq 2$. De façon inverse, la définition (très naturelle) du produit de convolution permet de comprendre la définition (très technique) du produit dans une algèbre de Hecke.

En utilisant le fait que la valeur d'une fonction arithmétique est la même sur $\begin{pmatrix} 0 & 0 \\ 0 & A \end{pmatrix}$, sur A et sur $\begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix}$, ainsi que sur toute matrice bilatéralement primitivement équivalente à A, nous constatons que pour connaître une fonction arithmétique sur toutes les matrices de rang $\leq r$, il nous suffit d'étudier sa restriction au sous-ensemble $\mathcal{I}nv_r$ de $\mathbb{Z}^{(r,r)}$ constitué des matrices non-singulières. Considérons donc $\hat{\mathcal{H}}_r$ l'ensemble des fonctions sur $\mathcal{I}nv_r$ qui ne dépendent que de la forme normale de Smith d'une matrice, i.e.

$$\hat{\mathcal{H}}_r = \{f : \mathrm{GL}_r(\mathbb{Z})\backslash \mathcal{I}nv_r / \mathrm{GL}_r(\mathbb{Z}) \to \mathbb{C}\}.$$

Nous pouvons écrire le produit de convolution de deux fonctions f et g en fonctions de leurs valeurs sur des matrices en forme normale de Smith si nous ajoutons un poids qui "convertisse" les formes normales d'Hermite en formes normales de Smith. Plus précisément, soit S une matrice en forme normale de Smith (non-singulière) et H un représentant d'une classe de diviseurs, i.e. $S = H(H^{-1}S)$. Soit S_1 et S_2 les formes normales de Smith respectivement de H et de $H^{-1}S$. Définissons $\alpha(S_1, S_2; S)$ comme étant le nombre de H satisfaisant à ces conditions. Alors

$$(f \star g)(S) = \sum_{S = H(H^{-1}S)} f(H)g(H^{-1}S) = \sum_{S_1, S_2} f(S_1)g(S_2)\alpha(S_1, S_2; S).$$

Muni de ce produit nous avons déjà remarqué que $(\hat{\mathcal{H}}_r, +, \star)$ est une $\mathbb{C}$-algèbre commutative.

Nous retrouvons ce produit au niveau de l'algèbre de Hecke $\mathcal{H}_r$ associée à $\mathrm{GL}_r(\mathbb{Z})$ et $\mathcal{I}nv_r$ (voir [Kr]). Nous avons tout simplement

$$\mathcal{H}_r = \{f \in \hat{\mathcal{H}}_r, f(S) = 0 \quad \text{sauf sur un ensemble fini}\}.$$

La définition du produit de Hecke sur $\mathcal{H}_r$ est rendue opaque par la technique, mais nous vérifions qu'il s'agit effectivement du produit défini plus haut, i.e.

$$(\mathrm{GL}_r(\mathbb{Z}) \cdot S_1 \cdot \mathrm{GL}_r(\mathbb{Z})) \cdot (\mathrm{GL}_r(\mathbb{Z}) \cdot S_2 \cdot \mathrm{GL}_r(\mathbb{Z})) = \sum_{S \in \mathrm{GL}_r(\mathbb{Z})\backslash S_1 \cdot \mathrm{GL}_r(\mathbb{Z}) \cdot S_2 / \mathrm{GL}_r(\mathbb{Z})} \alpha(S_1, S_2; S)(\mathrm{GL}_r(\mathbb{Z}) \cdot S \cdot \mathrm{GL}_r(\mathbb{Z}))$$

Si l'associativité n'est par exemple pas du tout naturelle sur cette définition, elle est évidente en termes de matrices. Nous savons alors que $\mathcal{H}_r$ est un anneau de

polynômes en un nombre dénombrable d'indéterminées (algébriquement indépendantes). Toutefois sa structure peut-être précisée. Pour un nombre premier p, considérons $\mathcal{I}nv_{r,p}$ l'ensemble des matrices de $\mathcal{I}nv_r$ dont le déterminant est une puissance de p et la composante primaire

$$\mathcal{H}_{r,p} = \{f : \mathrm{GL}_r(\mathbb{Z})\backslash\mathcal{I}nv_{r,p}/\mathrm{GL}_r(\mathbb{Z}) \to \mathbb{C}, f(S) = 0 \text{ sauf sur un ensemble fini}\}.$$

Alors $\mathcal{H}_r$ est isomorphe au produit tensoriel des $(\mathcal{H}_{r,p})_p$ et chaque $\mathcal{H}_{r,p}$ est isomorphe à $\mathbb{C}[X_1, \dots, X_r]$. Il est alors facile de constater que

$$\hat{\mathcal{H}}_{r,p} = \{f : \mathrm{GL}_r(\mathbb{Z})\backslash\mathcal{I}nv_{r,p}/\mathrm{GL}_r(\mathbb{Z}) \to \mathbb{C}\}$$

est une algèbre de séries formelles en r indéterminées (algébriquement indépendantes) et que $\hat{\mathcal{H}}_r$ est une algèbre de séries formelles en un nombre dénombrable d'indéterminées (algébriquement indépendantes). Un tel anneau est factoriel d'après un résultat de Cashwell & Everett [CE]. Notons que les identités polynomiales décrites dans [N2] et [B1] trouvent ici leur cadre naturel.

Nous introduisons à présent la fonction indice qui est un homorphisme classique d'une algèbre de Hecke vers $\mathbb{C}$. La valeur de $\mathrm{ind}(\mathrm{GL}_r(\mathbb{Z}) \cdot S \cdot \mathrm{GL}_r(\mathbb{Z}))$ est tout simplement le nombre de simples classes (à droite ou à gauche grâce à l'anti-involution transposition) qui forment $\mathrm{GL}_r(\mathbb{Z}) \cdot S \cdot \mathrm{GL}_r(\mathbb{Z})$. En termes de matrices, il s'agit du nombre de FNH équivalents à la forme normale de Smith S.

Remarquons que nous aurions pu considérer l'ensemble des combinaisons linéaires formelles de doubles classes de l'ensemble de toutes les matrices à coefficients dans $\mathbb{Z}$ (de n'importe quelle taille et même rectangulaires) divisé à droite et à gauche par les matrices primitives. Il faut de plus ajouter le fait que nous ne considérons PAQ que si il existe une unité simultanée entre P et A et entre A et Q. Nous ne connaissons pas à l'heure actuelle la structure de cette algèbre.

...Ou de l'algèbre de Hall.

L'algèbre de Hecke $\mathcal{H}_{r,p}$ ci-dessus est bien connue en combinatoire sous le nom d'algèbre de Hall. Notre équivalence entre classes de diviseurs d'une matrice M et diviseurs du réseau $V(M)$ nous permet de lire directement beaucoup de nos résultats (et de nos problèmes) en termes d'algèbre de Hall.

Nous définissons (voir [G] et [Md]) le type d'un p-groupe abélien fini

$$G \simeq \mathbb{Z}/p^{f_1}\mathbb{Z} \oplus \mathbb{Z}/p^{f_1+f_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{f_1+f_2\cdots+f_r}\mathbb{Z}$$

comme étant la partition $(f_1 + \cdots + f_r, f_1 + \cdots + f_{r-1}, \dots, f_1)$. Ce même type est parfois aussi connu sous le nom de caractéristique de Segre [Z]. Etant donné un sous-groupe H de G, nous disposons de son type en tant que groupe abstrait et du type de G/H que nous appelons son cotype. Répondant à une conjecture de Hall, Klein en 1967 [K] a montré que le nombre de sous-groupes de type μ et cotype ν d'un p-groupe de type λ est un polynôme. Nous dénotons cette quantité par $g^{\lambda}_{\mu,\nu}(p)$: il s'agit des célèbres polynômes de Hall.

Nous remarquons alors que la suite exacte écrite partie IV nous garantit, via les fonctions arithmétiques de matrices, l'égalité $\alpha(S_1, S_2; S) = g^{\lambda}_{\mu,\nu}(p)$ où

$$\begin{cases} S = \mathrm{diag}(p^{\lambda_1}, p^{\lambda_2}, \dots) & , \quad \lambda = (\lambda_1, \lambda_2, \dots) \\ S_1 = \mathrm{diag}(p^{\mu_1}, p^{\mu_2}, \dots) & , \quad \mu = (\mu_1, \mu_2, \dots) \\ S_2 = \mathrm{diag}(p^{\nu_1}, p^{\nu_2}, \dots) & , \quad \nu = (\nu_1, \nu_2, \dots). \end{cases}$$

Notre évaluation des fonctions de classes de diviseurs nous donne en fait la possibilité d'évaluer $\sum_{\mu,\nu} g^{\lambda}_{\mu,\nu}(p)$ pour λ fixé. Nous signalons qu'il y avait déjà des résultats dans cette direction. Birkhoff par exemple a donné une expression pour $\sum_{\mu} g^{\lambda}_{\mu,\nu}(p)$ à ν et λ fixés en 1933 [B]. Sa formulation et sa démonstration sont assez compliquées. Butler en 1987 [Bu] redonne ce résultat sous la forme

$$\sum_{\mu} g^{\lambda}_{\mu,\nu}(p) = \prod_{i\geq 1} p^{\nu'_{i+1}(\lambda'_i-\nu'_i)} \begin{bmatrix} \lambda'_i - \nu'_{i+1} \\ \nu'_i - \nu'_{i+1} \end{bmatrix}_p$$

où λ' et ν' sont les partitions conjuguées des partitions λ et ν. En faisant la somme sur tous les ν, nous obtenons par conséquent une seconde expression pour τ.

Nous avons vu sur les exemples de la partie III que la suite des coefficients de $\sigma_a(F_r)$, en tant que polynôme en p, n'est pas unimodale. Mais si nous regardons $\sigma_a(F_r)$ comme un polynôme en p^a, i.e.

$$\sigma_a(F_r) = \sum_{k\geq 0} p^{ak} \alpha_{\lambda}(k;p)$$

où λ est le type du groupe abélien associé à F_r et où $\alpha_{\lambda}(k;p)$ est le nombre de ses sous-groupes d'ordre p^k, alors Butler [Bu] a montré que la suite de coefficients $(\alpha_{\lambda}(k;p))_k$ est elle unimodale. En fait, à partir des outils donnés à la partie III, nous pouvons donner une preuve très simple de ce résultat, preuve qui évite notamment tout recours au profond théorème de Lascoux & Schützenberger utilisé par Butler.

Nous avons déjà introduit le concept d'indice, une fonction très utilisée en algèbre de Hecke. En utilisant les idées de types et cotypes avec les diviseurs de réseaux, nous pouvons (cf [BR2]) obtenir une évaluation précise de $\mathrm{ind}(S)$, nommément

$$\mathrm{ind}(S) = \left[\begin{matrix} r \\ \lambda'_1 - \lambda'_2, \lambda'_2 - \lambda'_3, \ldots, \lambda'_{\lambda_1} \end{matrix} \right]_p p^{\sum_{i=1}^{\lambda_1} \lambda'_{i+1}(r-\lambda'_i)}$$

où $\lambda = (f_1 + \cdots + f_r, f_1 + \cdots + f_{r-1}, \ldots, f_1)$, λ' est sa partition conjuguée et $[\ ]_p$ sont les multinômes de Gauss en p.

L'argument de Krieg dans [Kr] peut être étendu pour montrer que l'indice est un polynôme en p. Notre argument donne qui plus est que son degré vaut $\sum_{j=1}^{r}(r+1-j)(j-1)f_j$.

Nous nous sommes intéressés aussi aux conditions pour qu'étant donnés trois groupes G, H et K abéliens finis, K soit un sous-groupe de G tel que $G/K \simeq H$. Une condition nécessaire et suffisante est que le polynôme de Hall associé soit non-nul. Thompson [T2] a donné des conditions nécessaires pour cette divisibilité en termes des facteurs invariants. Ces résultats utilisent des suites de Littlewood-Richardson que nous ne voulons pas détaillées ici.

VI. Fonctions Zéta associées.

Pour mieux comprendre le produit de convolution, nous avons décidé d'étudier la fonction zéta associée à un produit de convolution de deux fonctions arithmétiques χ_1 et χ_2. Bien que ces fonctions restent très mal connues, nous disposons à présent de bons renseignements dans le cas où $\chi_1 = \chi_2 = \mathbb{1}$. Comme conséquence nous pouvons obtenir par exemple l'ordre moyen du nombre de sous-groupes d'un groupe abélien fini et même avoir une version localisée de ce résultat.

La série de Dirichlet associée au produit de convolution de deux fonctions arithmétiques sur $\mathbb{Z}$ satisfait la propriété d'être égale au produit des séries de Dirichlet de chaque fonction. Ceci n'est plus vrai en dimension $r \geq 2$.

Définissons tout d'abord, en suivant [BR1], la série de Dirichlet formelle de simples classes associée à χ par

$$\begin{aligned} D_H(\chi; s_1, \ldots, s_r) &= \sum_{H \text{ FNH}} \frac{\chi(H)}{H^{s_1,\ldots,s_r}} \\ &= \sum_{H \text{ FNH}} \frac{\chi(H)}{m_1(H)^{s_1} \ldots m_r(H)^{s_r}} \end{aligned}$$

où $m_k(H)$ est le $k$ième invariant de Smith de H. Cette définition a le désavantage de faire intervenir les valeurs de χ sur toutes les classes à droite alors que cette valeur ne dépend que de la double classe de la matrice considérée et il y a donc surdétermination. Par ailleurs, sauf sous "la condition de déterminant", i.e. $s_1 = rs_r$, $s_2 = (r-1)s_r, \ldots, s_{r-1} = 2s_r$, nous n'avons pas en général $D_H(\chi_1 \star \chi_2; s_1, \ldots, s_r) = D_H(\chi_1; s_1, \ldots, s_r) D_H(\chi_2; s_1, \ldots, s_r)$. Le fait que cette relation aie lieu sous la condition de déterminant est en fait une conséquence de ce que l'indice (défini dans la partie précédente) induise un homorphisme d'algèbre de $\mathcal{H}_r$ dans $\mathbb{C}$. Remarquons que si nous nous restreignons à cette condition, nous réduisons nos r variables à une seule, ce qui réduit notablement le champs d'intérêt.

Pour lever la surdétermination, nous considérons la série de Dirichlet formelle de doubles classes associée à χ, i.e.

$$D_S(\chi; s_1, \ldots, s_r) = \sum_{S \text{ FNS}} \frac{\chi(S)}{S^{s_1,\ldots,s_r}}.$$

Pour passer de D_S à D_H, nous avons besoin de la fonction indice : $D_H(\chi; s_1, \ldots, s_r) = D_S(\text{ind } \chi; s_1, \ldots, s_r)$. Rappelons que la p-composante de cet indice est un polynôme assez compliqué et que donc la transformation de FNH à FNS n'est certainement pas immédiate. Notons finalement que si χ est multiplicative, alors D_S (et D_H) s'expriment en produit eulérien.

Nous nous tournons à présent vers la série associée à un produit de convolution et nous restreignons à la condition de déterminant par simplicité. Nous avons

$$\sum_{S \text{ FNS}} \frac{(\chi_1 \star \chi_2)(S)}{|S|^s} = \sum_{S_1 \text{ FNS}} \frac{\chi_1(S_1)}{|S_1|^s} \sum_{S_2 \text{ FNS}} \frac{\chi_2(S_2)}{|S_2|^s} \sum_{S} \alpha(S_1, S_2; S)$$

où α est la quantité définie dans la partie précédente. Nous constatons que pour décrire $D_S(\chi_1 \star \chi_2)$ en termes de $D_S(\chi_1)$ et de $D_S(\chi_2)$, il nous faut évaluer $\sum_S \alpha(S_1, S_2; S)$. Jusqu'à présent, nous n'avons pas réussi à déterminer une expression suffisamment simple pour cette quantité (au moins pour ce qui est de la

p-composante, nous disposons d'expressions pour les polynômes de Hall et pouvons ajouter ces expressions... Le résultat est si compliqué qu'il est difficile de dire si nous avons augmenté l'information.).

Dans le cas $r = 2$, nous avons calculé de façon très explicite dans [BR1] les coefficients $\alpha(S_1, S_2; S)$. Soit $S_1 = \langle k, m\rangle_p$, $S_2 = \langle \ell, n\rangle_p$ et $S = \langle k + \ell + n - t, 2t + m - n\rangle_p$. Nous avons alors

$$\alpha(S_1, S_2; S) = \begin{cases} p^n(1 + 1/p) & \text{si } t = 0,\ m = n, \\ p^n & \text{si } t = 0, m \neq n, \\ p^{n-t}(1 - 1/p) & \text{si } 0 < t < n - m, \\ p^m & \text{si } t = n - m \neq 0, \end{cases}$$

Ceci nous a permis d'exprimer, dans le cas $r = 2$, la p-composante de la série $D_S(\chi_1 \star \chi_2; s_1, s_2)$ en fonction de séries associées à χ_1 et à χ_2. Les paramètres s_1 et s_2 peuvent ici être oubliés. Nous donnons une expression pour

$$\sum_{f_1, f_2 \geq 0} (\chi_1 \star \chi_2)\langle f_1, f_2\rangle_p X^{f_1} Y^{f_2}.$$

Nous reviendrons sur ceci lorsque nous aborderons les questions de rationalité. Notons que les expressions obtenues ne nous ont jusqu'à présent donné aucune indication quant à une formule générale valable pour r quelconque.

Si χ_1 et χ_2 sont multiplicatives, ceci nous permet bien entendu de retrouver la série de Dirichlet complète. Par exemple nous avons

$$D_S(\tau; 2s, s) = \zeta^2(s)\zeta^2(2s)\zeta(2s - 1) \prod_p \{1 + p^{-s} - 2p^{-3s}\}$$

où ζ est la fonction zéta de Riemann.

Maintenant nous allons traiter le cas de la série de Dirichlet des fonctions de diviseurs σ_a plus explicitement. Bien qu'à l'heure actuelle l'expression explicite de $\sigma_a(F_r)$ donnée dans [B5] ne permette pas de calculer $D_S(\sigma_a)$, la connaissance du terme principal de $\sigma_a(F_r)$ (voir partie III) et le fait qu'il s'agisse d'un polynôme à coefficients positifs ou nuls induisent des propriétés intéressantes de cette série. Nous introduisons, comme dans [BW1] et [BW2], la fonction de niveau pour N dans $\mathbb{Z}^{(r,r)}$ comme étant

$$\ell_\tau^{(r)}(n) = \sum_{|N| = n} \tau(N),$$

ce qui nous permet d'écrire

$$Z^{(r)}(\tau, s) = \sum_{n=1}^{\infty} \frac{\ell_\tau^{(r)}(n)}{n^s} = \prod_p \sum_{\nu=0}^{\infty} \ell_\tau^{(r)}(p^\nu) p^{-\nu s}.$$

Le calcul du terme principal de $\sigma_a(F_r)$ nous donne

$$\tau\langle f_1, \ldots, f_r\rangle_p = \alpha(r) p^{\theta(r)} + R_p(f_1, \ldots, f_r)$$

où $\alpha(r)$ et $\theta(r)$ sont définis à la partie III (ici $a = 0$) et $R_p(f_1, \ldots, f_r)$ est un polynôme en p à coefficients ≥ 0 et de degré $\theta(r) - 1$. En rappelant que nous

connaissons $R_p(f_1,\dots,f_r)$ pour $p=1$, cela nous donne une borne inférieure et une borne supérieure précises pour τ, ce qui à son tour nous permet d'écrire $Z^{(r)}(\tau,s)$ sous la forme d'un produit de fonctions zéta de Riemann et d'une série de Dirichlet absolument convergente. Notons ici que le terme principal de $\tau(F_r)$ est sensible à la parité de r, et qu'il en est donc de même pour la fonction zéta associée. Dans [BW2], nous démontrons l'expression

$$Z^{(r)}(\tau,s)=\prod_{1\le j\le r}\zeta\big(js-[j^2/4]\big)^{1+\delta_j}C_r(s)$$

où $\delta_j=1$ si j est impair et 0 sinon, et où $C_r(s)$ est une série de Dirichlet absolument convergente pour $\Re s>[r^2/4]/r$. Dans ces expressions, $[x]$ désigne la partie entière de x. Ce résultat peut se développer en

$$\left.\begin{aligned}
&Z^{(2)}(\tau,s)=\zeta^2(s)\zeta(2s-1)G_2(s),\\
&Z^{(3)}(\tau,s)=\zeta^2(s)\zeta(2s-1)\zeta^2(3s-2)G_3(s),\\
&Z^{(2k)}(\tau,s)=\zeta^2(2ks-k^2)G_{2k}(s),\\
&Z^{(2k+1)}(\tau,s)=\zeta^2((2k+1)s-(k^2+k))G_{2k+1}(s)
\end{aligned}\right\}\ (k\ge 2)$$

où $G_r(s)=\sum_{n\ge1}g_r(n)n^{-s}$ est une série absolument convergente pour $\Re s>[r^2/4]/r$.

VII. Ordre moyens.

La suite des valeurs prises par une fonction arithmétique f est souvent erratique. Toutefois le comportement statistique de ces valeurs offre souvent une régularité surprenante. Le premier de ces renseignements statistiques est la valeur moyenne, soit $\frac{1}{x}\sum_{n\leq x} f(n)$.

En ce qui concerne les fonctions matricielles, les idées développées dans la partie précédente nous donnent accès à de tels renseignements. En 1993, nous avons introduit une série de Dirichlet associée aux formes normales de Smith [B4]. Si $a_r(n)$ est le nombre de matrices de $\mathbb{Z}^{(r,r)}$ en forme normale de Smith et de déterminant égal à n, nous avons $D(a_r,s)=\sum a_r(n)n^{-s}=\prod_{t=1}^{r}\zeta(ts)$. Il s'agit aussi de la fonction associée à l'espace de doubles classes $\mathcal{H}(\mathrm{GL}_r(\mathbb{Z}),\mathcal{I}nv_r)$ ou encore, via le théorème de structure des groupes abéliens finis, la fonction associée au nombre de groupes abéliens non-isomorphes de rang $\leq r$, i.e. $G\simeq\mathbb{Z}/b_1\mathbb{Z}\oplus\mathbb{Z}/b_2\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/b_r\mathbb{Z}$. Il est facile de montrer que

$$S_r(x)=\sum_{n\leq x}a_r(n)=L_{1,r}x+L_{2,r}x^{1/2}+L_{3,r}x^{1/3}+\mathcal{O}_\varepsilon(x^{\alpha+\varepsilon})$$

où les $L_{i,r}$ sont des constantes calculables non nulles (en fait $L_{i,r}=\prod_{1\leq j\leq r,j\neq i}\zeta(i/j)$) et où α est l'exposant du terme d'erreur pour la valeur moyenne de la fonction de diviseur en dimension 3 sur $\mathbb{Z}$. La meilleure borne connue est $\alpha\leq 0.2512$ [Liu].

Nous remarquons aussi que la série de Dirichlet associée à l'espace de classes unilatérales de $\mathcal{H}(\mathrm{GL}_r(\mathbb{Z}),\mathcal{I}nv_r)$ est donnée par $\prod_{t=0}^{r-1}\zeta(s-t)$ et compte le nombre de formes normales d'Hermite de déterminant fixé ou de sous-modules de $\mathbb{Z}^r$ d'indice donné. Cette dernière fonction est appelée la fonction zéta de Koecher [Te] ou la fonction zéta de Solomon. Nous montrons facilement que le nombre de matrices de $\mathbb{Z}^{(r,r)}$ en forme normale d'Hermite est équivalent à $\prod_{t=0}^{r-2}\zeta(r-t)\cdot x^r/r$. Remarquons ici que les fonctions de ce genre sont beaucoup étudiées, voir par exemple [Kn].

En ce qui concerne les diviseurs de groupes abéliens finis, Cohen en 1960 [Co] a introduit l'idée de compter les facteurs directs de ces groupes. Cette décomposition n'est que formelle et en conséquence ne tient pas compte de la structure de groupe. Par exemple, les seuls facteurs directs de $\mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p\mathbb{Z}$ sont $\mathbb{Z}/\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p\mathbb{Z}$.

Nous avons décidé d'étudier l'ordre moyen du nombre de classes de diviseurs au début des années 90. A l'heure actuelle, nous savons qu'en moyenne, une matrice de déterminant $\leq x$ et de rang $\leq r$ admet $A_r^* x^{([r^2/4]+1)/r-1}\operatorname{Log}^{\gamma_r}x$ diviseurs (où $A_r^*>0$ est un réel et où γ_r est un entier ≥ 0 que nous ne souhaitons pas détailler). De façon équivalente, il s'agit aussi du nombre moyen de sous-groupes d'un groupe abélien fini de cardinal $\leq x$ et de rang $\leq r$. Plus précisément [BW2], nous avons

$$\begin{aligned}\frac{1}{\sum\limits_{\substack{\det S\leq x\\ S\in\mathcal{I}nv_r}}1}\sum_{\substack{\det S\leq x\\ S\in\mathcal{I}nv_r}}\tau(S) &\sim A_r^* x^{\beta_r-1}\operatorname{Log}^{\gamma_r}x\\ &= \frac{1}{\sum\limits_{\substack{\mathrm{ordre}(G)\leq x\\ \mathrm{rang}(G)\leq r}}1}\sum_{\substack{\mathrm{ordre}(G)\leq x\\ \mathrm{rang}(G)\leq r}}\tau(G)\end{aligned}$$

où $\beta_r=([r^2/4]+1)/r$.

Ceci est un résultat assez étonnant car il montre que le nombre de diviseurs augmente énormément quand r devient grand. Historiquement, en 1991 et par des méthodes élementaires, nous avons prouvé que le nombre moyen de classes de diviseurs de matrices de déterminants $\leq x$ et de rang ≤ 2 était équivalent à $A_2^* \operatorname{Log}^2 x$ [B4]. Plus tard en introduisant

$$Z^{(2)}(\tau, s) = \zeta^2(s)\zeta(2s-1)\zeta^3(2s) \prod_p \{1 - 2p^{-3s} - p^{-4s} + 2p^{-5s}\}$$

et en utilisant une fonction de diviseurs de dimension 5 (nommément $d(1,1,2,2;n) = \sum_{n=n_1 n_2 n_3^2 n_4^2} 1$), nous avons montré [BM] que

$$T_2(x) = \sum_{n \leq x} \ell_\tau(n) = A_1 x \operatorname{Log}^2 x + A_2 x \operatorname{Log} x + A_3 x + \Delta(x),$$

où les A_i sont des constantes effectives, et où $\Delta(x) \ll x^{0.72098\cdots+\varepsilon}$, la borne triviale donnée par le principe de Dirichlet étant $x^{0.75+\varepsilon}$. Notons que, traduit en termes d'ordre moyen, ce résultat nous assure que le nombre moyen de diviseurs d'une matrice M dont le déterminant est compris entre x et $x + x^{0.72098\cdots+\varepsilon}$ et de rang ≤ 2 est égal à l'ordre moyen sur l'interval $[1, x]$. Rappelons ici le résultat pour la fonction de diviseurs classique [Hu] :

$$\tfrac{1}{x} \sum_{n \leq x} \tau(n) = \operatorname{Log} x + C + \mathcal{O}(x^{1/3-\alpha})$$

où C et $\alpha > 0$ sont des constantes effectives.

Menzer a ensuite amélioré cette borne pour $\Delta(x)$ en utilisant deux nouveaux résultats pour la fonction de diviseurs en trois dimensions et montré que $\Delta(x) \ll x^{0.64285\cdots+\varepsilon}$. Il a aussi conjecturé que $\Delta(x) = \Omega(x^{1/2} \operatorname{Log}^2 x)$ [Me].

Nous avons montré en 1996 que $\Delta(x) \ll x^{5/8+\varepsilon}$ $(5/8 = 0.625)$. Pour cette démonstration, l'un des ingrédients consiste en une estimation pour une fonction de diviseurs pondérée en dimension trois sur $\mathbb{Z}$, soit $\sum_{n_1 n_2 n_3^2 \leq x} n_3$, estimation obtenue par la technique des sommes d'exponentielles de types monomiales [BW1].

Grâce à un résultat oméga obtenu simultanément, nous savons que notre estimation de $\Delta(x)$ n'est pas trop loin du meilleur résultat possible. En fait, nous avons

$$\Delta(x) = \Omega_-(x^{1/2} \operatorname{Log}^2 x)$$

confirmant ainsi la conjecture de Menzer.

Récemment, Ivič [Iv] a donné une autre preuve de cette conjecture en étudiant $\Delta(x)$ en moyenne quadratique et en montrant que

$$\int_1^x \Delta^2(x)dx = \Omega(x^2 \operatorname{Log} x).$$

Il obtient dans ce même article une borne supérieure en moyenne de $\Delta^2(x)$, soit

$$\int_1^x \Delta^2(x)dx \ll x^2 (\operatorname{Log} x)^{31/3} (\operatorname{Log} \operatorname{Log} x)^{28/3}.$$

Pour déterminer une bonne borne pour le terme d'erreur en dimension $r = 3$, nous avons besoin d'une estimation pour une fonction de diviseurs pondérée de dimension 5 sur $\mathbb{Z}$. En utilisant les résultats de sommes d'exponentielles de Wu [Wu], nous pouvons donner une bonne approximation pour $\sum_{n_1 n_2 n_3^2 n_4^2 n_5^2 \leq x} n_3 n_4 n_5^2$, et montrer [BW2] que

$$T_3(x) = xP_4(\operatorname{Log} x) + \mathcal{O}(x^{14/17} \operatorname{Log}^6 x)$$

où P_t désigne un polynôme de degré t.

Pour $r \geq 4$, les singularités de la fonction $Z^{(r)}(\tau, s)$ sont plus simples. Par contre, l'abscisse de convergence absolue est plus large, comme nous l'avions déjà montré dans [BR1]. A l'heure actuelle, nous savons que, pour $k \geq 2$,

$$T_{2k}(x) = A_{2k} x^{(k^2+1)/2k} + \mathcal{O}_{\varepsilon,k}(x^{k/2+\varepsilon})$$

et

$$T_{2k+1}(x) = A_{2k+1} x^{(k^2+k+1)/(2k+1)} P_1(\operatorname{Log} x) + \mathcal{O}_k(x^{(k^2+k+\alpha)/(2k+1)} \operatorname{Log}^\beta x)$$

où A_{2k}, α (< 1) et β sont des constantes strictement positives déterminables. Nous espérons améliorer ces deux derniers termes d'erreur.

Nous mentionnons ici un problème ouvert dont la résolution permettrait une compréhension bien meilleure du domaine : étant données deux fonctions arithmétiques χ_1 et χ_2 positives ou nulles, déterminer l'ordre moyen de $\chi_1 \star \chi_2$ à partir de ceux de χ_1 et de χ_2.

VIII. Ordres normaux.

Nous abordons ici la question de savoir si la valeur moyenne (essentiellement x^{β_r-1}) de τ est bien représentative, ou si une minorité de valeurs de τ perturbe cet ordre moyen. Comme dans le cas des entiers mais de façon bien plus spectaculaire, c'est la seconde interprétation qui est valable. Qui plus est, nous décrirons un ensemble assez dense où τ prend des valeurs exceptionnellement grandes.

Récemment nous avons donné une version de l'inégalité de Turàn-Kubilius adapté à ce problème [BR3]. Remarquons que le cadre dans lequel nous opérons pour établir cette inégalité est assez large pour fonctionner aussi sur les entiers généralisés de Beurling (retrouvant un résultat de 1968 de Horadam [Ho]) ou sur les ideaux entiers des corps de nombres (retrouvant un résultat de Hinz de 1993 [Hi]).

L'inégalité originelle de Turàn-Kubilius (voir [Ell] par exemple) porte sur les fonctions additives de $\mathbb{Z}$ et dit qu'il existe une fonction $\epsilon(x)$ qui tend vers 0 quand x tend vers l'infini et qui a la propriété suivante. Pour chaque fonction additive f, nous avons

$$\frac{1}{x}\sum_{n\leq x}|f(n)-M(x)|^2\leq(2+\epsilon(x))D(x)^2\qquad(x\geq 2)$$

où

$$M(x)=\sum_{p^\nu\leq x}f(p^\nu)p^{-\nu}(1-p^{-1})\quad\text{et}\quad D(x)^2=\sum_{p^\nu\leq x}|f(p^\nu)|^2p^{-\nu}.$$

Si nous avons $D(x)=o(M(x))$ quand x tends vers l'infini, alors $M(x)$ est un ordre normal pour f. Pour ce qui est de la fonction de diviseurs sur $\mathbb{Z}$, i.e. $\tau(n)$, nous pouvons ainsi avoir accès à l'ordre normal de $\operatorname{Log}\tau$. Cela nous donne $\tau(n)=(\operatorname{Log}n)^{\operatorname{Log}2+o(1)}$ presque partout. Nous constatons qu'il y a donc une disparité entre l'ordre moyen qui est $\operatorname{Log}n$ et l'ordre "normal" qui est $(\operatorname{Log}n)^{\operatorname{Log}2}$.

Nous avons adapté une telle approche à la situation matricielle. Une fonction arithmétique χ est dite additive si $\chi(AB)=\chi(A)+\chi(B)$ dès que $(|A|,|B|)=1$. Nous désignons par P une matrice générique dont le déterminant est une puissance du nombre premier p. Pour une telle fonction nous disposons de l'inégalité

$$\frac{1}{x}\sum_{\substack{S\text{ en FNS}\\ \det S\leq x}}|\chi(S)-M(\chi,x)|^2\ll D(\chi,x)^2\qquad(x\geq 2)$$

où la constante impliquée dans le symbole $\ll$ est indépendante de χ et où

$$M(\chi,x)=\sum_{\det P\leq x}\frac{\chi(P)}{|P|}\prod_{k=1}^{r}(1-p^{-k})$$

et

$$D(\chi,x)=\sum_{\det P\leq x}\frac{|\chi(P)|^2}{|P|}\prod_{k=1}^{r}(1-p^{-k}).$$

Le problème ici est essentiellement d'exprimer $\chi(M)$ en fonction de $\chi(P)$. Si il existe $N\in\mathcal{I}nv_r$ telle que $\operatorname{FNS}(N)=\operatorname{FNS}(M)$, $S=N(N^{-1}S)$ et si les déterminants de N et $N^{-1}S$ sont premiers entre eux, nous utilisons la notation $N\to S$. Grâce à la

bijection entre groupes abéliens et matrices détaillée partie IV, nous avons montré que

$$\operatorname{Log}\tau(M) = \sum_{P \to M} \operatorname{Log}\tau(P).$$

Une évaluation du nombre de matrices M en FNS telles que $P \to M$ fournit alors l'inégalité précédente. Nous calculons ensuite la moyenne et la variance de $\operatorname{Log}\tau$ et obtenons

$$\frac{1}{x} \sum_{\substack{S \text{ en FNS} \\ \det S \leq x}} |\operatorname{Log}\tau(S) - \operatorname{Log} 2 \operatorname{Log}\operatorname{Log} x|^2 \ll \operatorname{Log}\operatorname{Log} x \qquad (x \geq 2)$$

ce qui généralise le célèbre théorème de Hardy-Ramanujan de 1917 [HR].

Il y a donc une discrépance notoire entre l'ordre moyen de τ (qui est une puissance de $\operatorname{Log}|S|$) et son ordre normal (qui est une puissance de $|S|$). Nous identifions dans la suite une collection de matrices où τ prend des valeurs très grandes. Notons que dans le cas $r = 2$ et en utilisant la technique de Selberg-Delange, nous avons déjà apporté dans [BW1] une réponse à cette question. Dans le cas $r \geq 3$, nous ne connaissons pas encore la fonction zéta associée suffisamment précisément pour qu'une telle approche fonctionne. Au lieu de cela, nous avons utilisé notre inégalité de Turàn-Kubilius générale dans un autre contexte. Nous nous sommes restreints aux matrices de "rang total r" (qui correspondent aux groupes abéliens finis de rang r et pas moins). Soit $\sum^*$ une somme portant sur de telles matrices. Alors nous avons montré que

$$x^{[r^2/4]+1)/r} \ll \sum_{|S| \leq x}{}^{*} \tau(S) \leq \sum_{|S| \leq x} \tau(S) \ll x^{[r^2/4]+1)/r} \operatorname{Log}^{\gamma_r} x$$

où les γ_r sont les constantes déjà apparues au cours de la partie VII, alors que l'ordre normal de τ sur l'ensemble des matrices de rang total r est aussi son ordre moyen.

IX. Rationalités des fonctions Zéta.

Jusqu'à présent, notre compréhension de la fonction de diviseurs a reposé énormément sur la formule de récurrence. Lorsque nous avons cherché une démonstration de cette formule via les groupes abéliens, nous avons bien retrouvé la formule initiale, mais aussi une seconde formule. La conjonction des deux va nous donner une formule fermée pour $\sigma_a(F_r)$.

Nous suivons les notations de la fin de la partie IV. Grâce à la dualité entre G et son groupe de caractères, nous pouvons écrire

$$\sigma_a(F_r) = \sum_{\substack{H\subset F_r\\ H\subset G_r}} |H|^a + \sum_{\substack{H\subset F_r\\ H\not\subset G_r}} |H|^a$$

au lieu d'utiliser le quotient F_r/H comme précédemment. Nous suivons alors l'argument comme auparavant. La première somme nous donne $\sigma_a(G_r)$ et, quant à la seconde, elle vaut

$$\sum_{K\subset F_{r-1}} |K|^a p^{a\ell} |F_{r-1}/K| = p^{a\ell}|F_{r-1}| \sum_{K\subset F_{r-1}} |K|^{a-1} = p^{a\ell}|F_{r-1}|\sigma_{a-1}(F_{r-1}).$$

En additionnant ces deux contributions, nous obtenons

$$\sigma_a(F_r) = \sigma_a(G_r) + p^{a\ell}|F_{r-1}|\sigma_{a-1}(F_{r-1}), \quad (\ell = f_1 + f_2 + \cdots + f_r).$$

Une comparaison avec la première formule de récurrence nous permet éliminer $\sigma_a(G_r)$ et d'aboutir à

$$(p^a-1)\sigma_a(F_r) = p^{a+t}\sigma_{a-1}(F_{r-1}) - \sigma_{a+1}(F_{r-1}) \quad \text{où} \quad t = \sum_{i=1}^{r} f_i(a+r-i).$$

Cette formule est algébrique en $q = p^a$ et maintenant, son application ne détruit plus la structure de forme normale de Smith tout en réduisant le rang !

En dévidant cette récursion, nous obtenons une formule qui est l'analogue de l'expression classique sur les entiers

$$\sigma_a(f_1) = \frac{p^{a(f_1+1)}-1}{p^a-1}$$

qui exprime σ_a comme une fraction rationnelle de $(p, p^a, p^{f_1}, \ldots, p^{f_r}, p^{af_1}, \ldots, p^{af_r})$, fraction rationnelle qui ne dépend donc que de r. D'un point de vue numérique, cette formule est beaucoup plus efficace que la précédente et les valeurs données en partie IV demandent quelques secondes, quand il fallait plusieurs minutes auparavant. La complexité est par ailleurs peu sensible à la taille des f_i et il nous est possible de calculer maintenant la fonction τ sur des exemples de dimension 10 en quelques minutes seulement.

En utilisant la formule explicite de [BR1], nous avons montré dans le cas $r = 2$ que, si la p-composante de la fonction zéta associée à χ était rationnelle, il en était de même de celle de $\mathbb{1} \star \chi$. Il en est probablement de même si l'on prend le produit de convolution de deux fonctions dont les facteurs locaux sont rationnels, mais nous n'avons pas encore complété cette preuve. Le cas r général semble hors

de notre portée à l'heure actuelle, mais la formule précédente permet de démontrer la rationalité des facteurs locaux de $Z^{(r)}(\sigma_a, s)$, et même de donner une formule fermée pour ces facteurs. Dénotons par $Q_{r,a}(X_1, \dots, X_r)$ un tel facteur, i.e.

$$Q_{r,a}(X_1, \dots, X_r) = \sum_{f_1,\dots,f_r \geq 0} \sigma_a(F_r)\, X_1^{f_1} X_2^{f_2} \dots X_r^{f_r}$$

le paramètre p restant sous-entendu. La relation de récurrence ci-dessus diminue directement le nombre de variables d'une unité, ce qui nous donne

$$\begin{aligned}(p^a-1)Q_{r,a}(X_1,\dots,X_r) = \\ p^a Q_{r-1,a-1}(p^{a+r-1}X_1, p^{a+r-2}X_2, \dots, p^{a+1}X_{r-1}) \sum_{f_r\geq 0} (p^a X_r)^{f_r} \\ - Q_{r-1,a+1}(X_1,\dots,X_{r-1}) \sum_{f_r\geq 0} X_r^{f_r}\end{aligned}$$

que nous réécrivons en

$$\begin{aligned}Q_{r,a}(X_1,\dots,X_r) = \\ \frac{p^a}{(p^a-1)(1-p^aX_r)} Q_{r-1,a-1}(p^{a+r-1}X_1, p^{a+r-2}X_2, \dots, p^{a+1}X_{r-1}) \\ - \frac{1}{(p^a-1)(1-X_r)} Q_{r-1,a+1}(X_1,\dots,X_{r-1}).\end{aligned}$$

Nous pouvons bien entendu poursuivre ce procédé et obtenir en un nombre fini d'étapes une fraction rationnelle.

Chaque fois que nous utilisons la formule ci-dessus, nous changeons la variable r de $Q_{r,a}$ par $r-1$, a par $a+\epsilon$, où $\epsilon = \pm 1$, et les X_i par $p^{\epsilon^*(a+r-i)}X_i$, où $\epsilon^* = (1-\epsilon)/2$. De plus nous devons ajouter un facteur

$$-\epsilon \frac{p^{\epsilon^* a}}{p^a-1} \cdot \frac{1}{1-p^{\epsilon^* a}X_r}$$

que nous appelons $w_\epsilon(p^a, X_r)$. Avec ces notations, notre relation s'écrit

$$Q_{r,a}(X_1,\dots,X_r) = \sum_\epsilon w_\epsilon(p^a, X_r) Q_{r-1,a+\epsilon}(p^{\epsilon^*(a+r-i)}X_i, 1 \leq i \leq r-1).$$

En poursuivant ce chemin, nous aboutissons à

$$\sum_{(\epsilon_k)} \prod_{k=1}^{r} w_{\epsilon_k}\left(p^{a+\sum_{\ell=1}^{k-1}\epsilon_\ell}, p^{\sum_{\ell=1}^{k-1}\epsilon_\ell^*(a+k-1+\sum_{m=1}^{\ell-1}(\epsilon_m-1))}X_{r-k+1}\right),$$

ce qui en définitive nous donne

$$\begin{aligned}Q_{r,a}(X_1,\dots,X_r) = \\ \sum_{(\epsilon_k)} \prod_{k=1}^{r} (-\epsilon_k) \frac{p^{\epsilon_k(a+\sum_{\ell=1}^{k-1}\epsilon_\ell)}}{(p^{a+\sum_{\ell=1}^{k-1}\epsilon_\ell}-1)} \cdot \frac{1}{(1-p^{\sum_{\ell=1}^{k-1}\epsilon_\ell^*(a+k-1+\sum_{m=1}^{\ell-1}(\epsilon_m-1))}X_{r-k+1})}.\end{aligned}$$

A titre d'exemple simple, nous avons

$$Q_{2,0} = \frac{1 + X_2 - 2X_1X_2}{(1-X_1)^2(1-X_2)^2(1-pX_2)}.$$

En prenant $X_1 = p^{-s}$ et $X_2 = p^{-2s}$, nous retrouvons $Z^{(2)}(\tau, s)$. Par contre

$$Q_{4,1} = \frac{N(X_1, X_2, X_3, X_4)}{(1-X_1)^2(1-p^3X_1)^2(1-p^4X_1)(1-X_2)^2(1-p^2X_2)(1-X_3)^2(1-pX_3)(1-X_4)}$$

où $N(X_1, X_2, X_3, X_4)$ est un polynôme très compliqué.

Les dénominateurs des expressions obtenues sont assez naturels mais nous n'avons pas encore compris la signification du numérateur.

Signalons que, via la correspondance avec l'algèbre de Hall, notre résultat nous dit aussi que la fonction

$$Q(p, X_1, \ldots, X_r) = \sum_{\mu,\nu} \sum_{\lambda} g^{\lambda}_{\mu,\nu}(p) \prod_{j=1}^{r} X_j^{\lambda_j - \lambda_{j+1}}$$

est rationnelle.

Remarquons aussi que ce résultat de rationalité de la fonction zéta de sous-groupes de groupes abéliens (pour $a = 0$) trouve un parallèle parmis les travaux de rationalité de fonctions zéta associées aux sous-groupes de divers groupes, comme la famille des groupes nilpotents, mais qui sont tous sans torsion (voir par exemple les travaux de Grünewald, Segal et Smith [GSS] ou de Lubotzky [L]).

Références

[Bo] *"Über die Fourier-Jacobi Entwicklung Siegelscher Eisensteinreihen" de* S. Böcherer *dans* Math. Z. 183 (**1983) ,** *pages 21–46 .*

[B1] *"On arithmetical functions of integer matrices" de* G. Bhowmik , Thèse de doctorat Panjab University, Chandigarh, India (**1989) .**

[B2] *"Completely Multiplicative Arithmetical Functions of Matrices and Certain Partition Identities" de* G. Bhowmik *dans* J. Ind. Math. Soc. 56 (**1991) ,** *pages 73–83 .*

[B3] *"Divisor functions of integer matrices : evaluations, average orders and applications" de* G. Bhowmik *dans* Astérisque 209 (**1992) ,** *pages 169–177 .*

[B4] *"Average orders of certain functions connected with arithmetic of matrices" de* G. Bhowmik *dans* J. Ind. Math. Soc. 59 (**1993) ,** *pages 97–106 .*

[B5] *"Evaluation of the divisor function of matrices" de* G. Bhowmik *dans* Acta Arith. 74 (**1996) ,** *pages 155–159 .*

[BM] *"On the number of subgroups of finite abelian groups" de* G. Bhowmik & H. Menzer *dans* Abh. Sem. Hamburg 67 (**1997) .**

[BN] *"Arithmetic of matrices" de* G. Bhowmik & V.C. Nanda , Manuscript .

[BR1] *"Average orders of multiplicative arithmetical functions of integer matrices" de* G. Bhowmik & O. Ramaré *dans* Acta Arith. 66.1 (**1994) ,** *pages 45–62 .*

[BR2] *"Algebra of Matrix Arithmetic" de* G. Bhowmik & O. Ramaré *dans* Publications IRMA 43, No.IV (**1997) .**

[BR3] *"A Turàn-Kubilius Inequality for Integer Matrices" de* G. Bhowmik & O. Ramaré *soumis à* J. Number Theory (**1997) .**

[BW1] *"On the asymptotical behaviour of the number of subgroups of a finite abelian group" de* G. Bhowmik & J. Wu *dans* Archiv der Math. 69 (**1997) ,** *pages 95–104 .*

[BW2] *"Zeta functions of subgroups of abelian groups" de* G. Bhowmik & J. Wu , Préprint (**1997) .**

[B] *"Subgroups of abelian groups" de* G. Birkhoff *dans* Proc. London Math. Soc. 38 (2) (**1933) ,** *pages 385–401 .*

[Bu] *"A unimodality result in the enumeration of subgroups of a finite abelian group" de* L.M. Butler *dans* Proc. Amer. Math. Soc. 101 (**1987) ,** *pages 771–775 .*

[CE] *"The ring of number-theoretic functions" de* E.D. Cashwell & C.J. Everett *dans* Pacific J. of Math. 9 (**1959) ,** *pages 975–985 .*

[Ch] *"Über teilerfremde symmetrische Matrizenpäre" de* U. Christian *dans* J. Reine Angew. Math. 229 (**1968) ,** *pages 43–49 .*

[Co] *"On the average number of direct factors of a finite abelian group" de* E. Cohen *dans* Acta Arith. 6 (**1960) ,** *pages 159–173 .*

[Da] *"On Poincaré series on Sp_m" de* A. Dabrowski *dans* Math. Z. 221 (**1996) ,** *pages 573–589 .*

[Ell] *"Probalistic Number Theory : means value theorems" de* P.D.T.A. Elliot *publié par* Gründlehren der Math. Wiss. ,Springer-Verlag, New York-Berlin-Heidelberg 239 (**1979) .**

[Fr] *"Singular Modular Forms and Theta Relations" de* E. Freitag *publié par* Lecture Notes, Springer-Verlag 1487 (**1991) .**

[Ge] *"A Local Approach to Matrix Equivalence" de* L.J. Gerstein *dans* Lin. Alg. Appl. 16 (**1977) ,** *pages 221–232 .*

[G] *"Symmetric functions and p-modules" de* J.A. Green *publié par* Lecture Notes, Manchester (**1961) .**

[GSS] *"Subgroups of finite index in nilpotent groups" de* F.J. Grünewald, D. Segal & G.C. Smith *dans* Invent. Math. 93 (**1988) ,** *pages 185–223 .*

[HR] *"The normal order of prime factors of the number n" de* G.H. Hardy & S. Ramanujan *dans* Quart. J. Math. 48 (**1917) ,** *pages 76–92 .*

[Hi] *"On the prime ideal theorem" de* J.G. Hinz *dans* J. Ind. Math. Soc. 59 (**1993) ,** *pages 243–260 .*

[Ho] *"Normal order for divisor functions of generalised integers" de* E.M. Horadam *dans* Portugaliae Math. 27 (**1968) ,** *pages 201–207 .*

[H] *"Introduction to Number Theory" de* L.K. Hua *publié par* Springer-Verlag (**1982) .**

[Hu] *"Exponential Sums and Lattice Points, II" de* M.N. Huxley *dans* Proc. London Math. Soc. 26 (**1994) ,** *pages 279–301 .*

[Iv] *"On the number of subgroups of finite abelain groups"* *de* A. Ivić , Préprint (**1997) .**
[Ka] *"Elementary divisors and modules"* *de* I. Kaplansky *dans* Trans. Amer. Math. Soc. 66 (**1949) ,** *pages 464–491 .*
[K] *"The Hall polynomial"* *de* T. Klein *dans* J. Alg. 12 (**1969) ,** *pages 61–78 .*
[Kn] *"Enumerating non-equivalent matrices over principal ideal domains"* *de* J. Knopfmacher *dans* Math. Slovaca 44 (**1994) ,** *pages 287–296 .*
[Ko] *"On Poincaré Series of Exponential Type on Sp_2"* *de* W. Kohnen *dans* Abh. Math. Sem. Univ. Hamburg 63 (**1993) ,** *pages 283–297 .*
[Koe] *"Matrices over $\mathbb{Z}$"* *de* M. Koecher , Manuscript, Münster (**1985) .**
[Kr] *"Hecke Algebras"* *de* A. Krieg *dans* Memoirs of the AMS 87 (**1990) .**
[La] *"Products of idempotent matrices"* *de* T.J. Laffey *dans* Lin. and Multilinear Algebra 14 (**1983) ,** *pages 309–314 .*
[LR] *"Matrices and pairs of modules"* *de* L. Levy & J. Robson *dans* J. Algebra 29 (**1974) ,** *pages 427–454 .*
[Liu] *"On the number of abelian groups of a given order (supplement)"* *de* H.Q. Liu *dans* Acta Arith. 64 (**1993) ,** *pages 285–296 .*
[Lu] *"Subgroup Growth"* *de* A. Lubotzky , Preliminary version no 1, University College, Galway, Ireland (**1993) .**
[Ma] *"Lectures on Siegel's Modular Functions"* *de* H. Maass *publié par* TIFR, Bombay (**1954-55) .**
[Md] *"Symmetric functions and Hall polynomials"* *de* I.G. Macdonald *publié par* Oxford Univ. Press (**1979) .**
[Me] *"On the number of subgroups of finite abelian groups"* *de* H. Menzer *dans* Proc. Conf. Analytic and Elementary Number Theory, Universität Wien (**1996) ,** *pages 181–188 .*
[N1] *"On GCD and LCM of Matrices"* *de* V.C. Nanda *dans* J. Ind. Math. Soc. .
[N2] *"Arithmetic Functions of Matrices and Polynomial Identities"* *de* V.C. Nanda *dans* Colloq. Math. Soc. Jànos Bolyai 34 (**1982) ,** *pages 1107–1126 .*
[N3] *"Generalizations of Ramanujan's sum to matrices"* *de* V.C. Nanda *dans* J. Ind. Math. Soc. 48 (**1984) ,** *pages 177–187 .*
[N4] *"On arithmetical functions of integral matrices"* *de* V.C. Nanda *dans* J. Ind. Math. Soc. 55 (**1990) ,** *pages 175–188 .*
[Na] *"Generalized Inverses and Applications"* *de* Ed. M. Zuhair Nashed *publié par* Academic Press, New York-San Francisco-London (**1976) .**
[Ne] *"Integral Matrices"* *de* M. Newman *publié par* Academic Press, New York-London (**1972) .**
[Pr] *"To the problem of multiplicativity of canonical diagonal forms of matrices over the domain of principal ideals"* *de* V.M. Prokip *dans* Ukrainian Math. J. 47 (**1995) ,** *pages 1806–1810 .*
[RS] *"Some generalizations of Ramanujan's sum"* *de* K.G. Ramanathan & M.V. Subbarao *dans* Canad. J. Math. 32 (**1980) ,** *pages 1250–1260 .*
[S1] *"Über die analytische Theorie der quadratischen Formen I, II, III"* *de* C.L. Siegel *dans* Gesammelte Abhandlungen, Band I, Springer-Verlag (**1966) ,** *pages 326–405, 410–443, 469–548 .*
[S2] *"Einführung in die Theorie der Modulfunktionen n-ten Grades"* *de* C.L. Siegel *dans* Gesammelte Abhandlungen, Band II, Springer-Verlag (**1966) ,** *pages 97–137 .*
[Ter] *"Harmonic Analysis on Symmetric Spaces and Applications, II"* *de* A. Terras *publié par* Springer-Verlag, New York-Berlin-Heidelberg (**1988) .**
[T1] *"An inequality for invariant factors"* *de* R.C. Thompson *dans* Proc. Amer. Math. Soc. 86 (**1982) ,** *pages 9–11 .*
[T2] *"Smith invariants of a product of integral matrices"* *de* R.C. Thompson *dans* Collection Linear algebra and its role in system theory (Brunswick, Maine, 1984) Contemp. Math. 47 (**1985) ,** *pages 401–435 .*
[T3] *"Left Multiples and Right Divisors of Integral Matrices"* *de* R.C. Thompson *dans* Linear and Multilinear Alg. 19 (**1986) ,** *pages 287–295 .*
[Wu] *"On the distribution of square-full and cube-full integers"* *de* J. Wu *dans* Mh. Math. à paraître .
[Z] *"Inequalities for the Weyr characteristic of modules"* *de* I. Zaballo *dans* Algebra Lineal y Applicaciones Universidad del Pais Vasco (**1984) ,** *pages 432–442 .*