Astérisque

JOSEPH OESTERLÉ

Empilements de sphères

Astérisque, tome 189-190 (1990), Séminaire Bourbaki,
exp. n° 727, p. 375-397

<http://www.numdam.org/item?id=SB_1989-1990__32__375_0>

© Société mathématique de France, 1990, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI juin 1990
42ème année, 1989-90, n° 727

EMPILEMENTS DE SPHÈRES

par **Joseph OESTERLÉ**

Contrairement à l'usage en mathématiques, le mot "sphère" signifie ici "sphère pleine", *i.e.* est synonyme de "boule fermée".

Soit E un espace euclidien de dimension n. Un *empilement de sphères* dans E est une famille de sphères de même rayon d'intérieurs mutuellement disjoints. À tout réseau L de E, on associe un empilement de sphères : ces sphères ont pour centres les points de L et leur rayon commun est le plus grand pour lequel elles forment un empilement.

Soit (S_i) un empilement de sphères. Lorsque la limite

$$\lim_{R\to\infty}[\mathrm{vol}((\cup S_i)\cap B(0,R))/\mathrm{vol}(B(0,R))]$$

existe, on l'appelle la *densité de l'empilement.* Par exemple, l'empilement de sphères associé à un réseau L de E a pour densité

$$d(L) = \mathrm{vol}(B(0,r))/v = b_n\, r^n/v, \tag{1}$$

où r est le rayon commun des sphères, v le volume de E modulo L et $b_n = \pi^{n/2}/\Gamma\left(\frac{n+2}{2}\right)$ celui de la boule unité de E. Par abus de langage, on dit que $d(L)$ est la *densité du réseau* L.

Deux questions fondamentales concernant les empilements de sphères sont :

a) *Quelle est la densité maximale δ_n d'un empilement de sphères dans E ?*

b) *Quelle est la densité maximale d_n d'un réseau de E ?*

(Dans chacun des deux cas, on peut montrer que la densité maximale est effectivement atteinte ; par ailleurs, elle ne dépend que de n, puisque deux espaces euclidiens de même dimension sont isométriques. Enfin, il est clair que l'on a $d_n \leq \delta_n \leq 1$.)

Après quelques rappels sur l'état de ces questions, nous décrirons le procédé d'Elkies et Shioda qui , en utilisant l'arithmétique des courbes elliptiques sur les corps de fonctions, permet de retrouver (au moins en dimension ≤ 1000) la plupart des réseaux très denses connus et, pour certaines dimensions (par exemple 33, 54, 64, 80,...) d'en découvrir de nouveaux, plus denses.

La taille de cet exposé ne nous a pas permis d'aborder d'autres sujets pourtant fort intéressants : empilements de corps convexes, recouvrements par des sphères, nombre maximal de contacts entre sphères de même rayon (kissing number), applications à la géométrie des nombres, liens profonds entre la théorie du codage et celle des empilements de sphères, géométrie très riche des réseaux les plus denses connus, etc. Le lecteur intéressé pourra consulter le livre de Rogers ([Ro]), et celui de Conway et Sloane ([C,S]), qui contiennent d'excellentes bibliographies sur ces sujets.

1. EMPILEMENTS DE SPHÈRES

1.1. La dimension 2

La densité maximale d'un empilement de sphères en dimension 2 est $\delta_2 = \pi/2\sqrt{3} = 0,9068\ldots$. C'est la densité de l'empilement associé au réseau hexagonal :

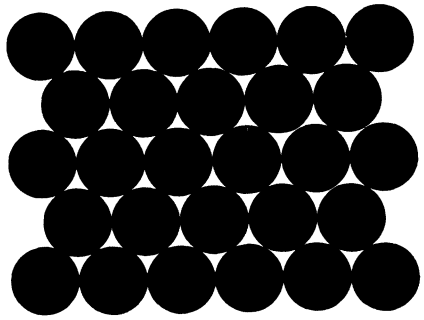

Figure 1.

Ce résultat, énoncé en 1882 par Thue ([Th]), n'a été démontré de façon complètement satisfaisante qu'en 1940 par Fejes ([Fe]). Une preuve élégante est due à Rogers ([Ro], ch. 7), qui démontre pour tout $n \geq 1$ l'inégalité

$$\delta_n \leq \sigma_n, \tag{2}$$

où σ_n est, dans un simplexe régulier à $n+1$ sommets de côté 2, la proportion du volume recouverte par les sphères de rayon 1 centrées aux sommets. (Pour $n = 2$, on a $\sigma_2 = \pi/2\sqrt{3}$ et (2) est une égalité car le plan peut être pavé par des triangles équilatéraux.)

1.2. La dimension 3

On ne connaît la densité maximale δ_n des empilements de sphères en dimension n pour aucun entier $n \geq 3$. Pour $n = 3$ par exemple, l'inégalité de Rogers $\delta_3 \leq \sigma_3 = \sqrt{2}(3 \operatorname{Arc\,cos} \frac{1}{3} - \pi) = 0,7796\ldots$ n'est pas une égalité. (On ne peut paver $\mathbf{R}^3$ par des tétraèdres réguliers car l'angle entre leurs faces, égal à $\operatorname{Arc\,cos} \frac{1}{3}$, ne divise pas 2π.) La majoration de Rogers a été légèrement améliorée par Lindsey: on a $\delta_3 < 0,7784\ldots$.

Considérons dans $\mathbf{R}^3$ le réseau

$$L = \{(n_1, n_2, n_3) \in \mathbf{Z} \mid n_1 + n_2 + n_3 \in 2\mathbf{Z}\}$$

(dit "cubique à faces centrées", car il s'obtient en répétant dans les trois directions le motif obtenu en plaçant des points aux sommets et aux centres des faces d'un cube) :

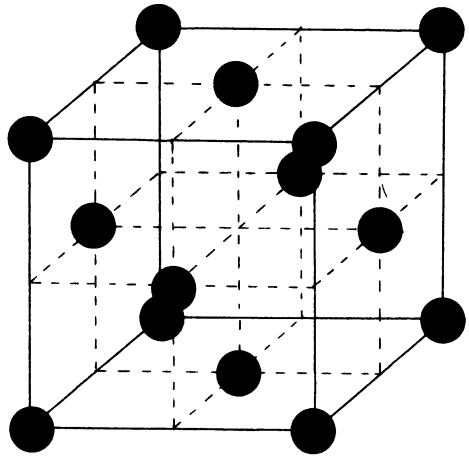

Figure 2.

L'empilement de sphères associé a pour densité $\pi/3\sqrt{2} = 0,7404\ldots$. Le réseau L est isométrique au réseau engendré par le système de racines A_3 : en effet, $(1,1,0)$, $(-1,0,1)$ et $(1,-1,0)$ forment une base de L par rapport à laquelle la matrice du produit scalaire de $\mathbf{R}^3$ est $\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}$. C'est pourquoi on note A_3 le réseau L et l'empilement de sphères associé. Gauss a démontré que A_3 est le réseau le plus dense en dimension 3, c'est-à-dire que l'on a $d_3 = \pi/3\sqrt{2}$.

L'empilement A_3 est celui suivant lequel les épiciers empilent les oranges : il s'obtient en superposant des couches horizontales de sphères, les sphères de chaque couche étant réparties suivant un réseau carré et celles de la $n+1$-ième couche venant s'insérer dans les trous les plus profonds de la n-ième couche.

Lorsqu'on veut superposer de la même manière des couches horizontales dans lesquelles les sphères sont disposées suivant un réseau hexagonal (fig. 1), on peut poser la $n+1$-ième couche sur la n-ième de deux façons. Cela conduit à différents empilements possibles. L'un d'eux est encore

l'empilement A_3 (regarder la fig. 2 en prenant comme verticale une grande diagonale du cube), mais d'autres ne sont pas associés à des réseaux. Tous ces empilements ont la même densité $\pi/3\sqrt{2}$.

On ne connaît aucun empilement de sphères plus dense en dimension 3, d'où la célèbre phrase de Rogers : "Many mathematicians believe, and all physicists know, that the density cannot exceed $\pi/3\sqrt{2}$".

1.3. Les dimensions plus grandes

Pour certaines dimensions (par exemple $n = 10, 11, 13$), les empilements de sphères les plus denses connus actuellement ne sont pas associés à des réseaux. Il se pourrait que l'on ait $d_n < \delta_n$ pour ces dimensions.

Lorsque n est grand, la constante σ_n intervenant dans la majoration de Rogers est équivalente à $ne^{-1}\,2^{-n/2}$. Une meilleure majoration asymptotique de δ_n a été obtenue par Kabatiansky et Levenshtein [K,L] : pour n assez grand, on a $\delta_n \leq 2^{-0,599\,n}$.

Si l'on choisit un empilement de sphères *maximal* dans un espace euclidien E, on obtient un recouvrement de E en prenant les sphères de mêmes centres et de rayon double. De cette remarque élémentaire, on déduit aussitôt la minoration $\delta_n \geq 2^{-n}$. (On peut faire mieux : d'après Rogers ([Ro], th. 2.4), δ_n est supérieur à $\left(\frac{n}{2(n+1)}\right)^{n/2}\sigma_n$, qui est équivalent à $ne^{-3/2}\,2^{-n}$ lorsque n tend vers ∞.) Curieusement, personne n'a su jusqu'à présent exhiber "explicitement" pour une infinité de dimensions n, des empilements de sphères de densité $\geq 2^{-n}$; le mieux qui ait été fait dans cette direction est la construction explicite, par Rosenbloom et Tsfasman ([R,T]), d'empilements de sphères (associés à des réseaux) de densité $\geq 2^{-1,39\,n}$ pour une infinité de dimensions n.

1.4. Empilements aléatoires

Avant d'achever ce paragraphe, il convient de signaler le très joli chapitre 22 du livre de géométrie de Coxeter ([Co]) où sont décrits quelques faits expérimentaux concernant les empilements "aléatoires" en dimension 3. Coxeter mentionne en particulier les observations suivantes de G.D. Scott :

lorsqu'on remplit une grande boîte de petites billes identiques, en déversant les billes en vrac dans la boîte, on constate que la densité de l'empilement obtenu est d'environ $0,60$; si l'on agite la boîte pendant qu'on la remplit, l'empilement obtenu est plus dense et on constate que sa densité, remarquablement stable, est voisine de $0,6366$ (c'est-à-dire de $\frac{2}{\pi}$). Aucun modèle mathématique permettant d'expliquer ces observations n'existe à ce jour.

2. EMPILEMENTS DE SPHÈRES ASSOCIÉS À DES RÉSEAUX

2.1. Densité et constante d'Hermite

Soient E un espace euclidien de dimension n et L un réseau de E . Posons

$$m(L) = \inf_{\ell \in L, \ell \neq 0} \langle \ell, \ell \rangle. \tag{3}$$

Par abus de langage, les vecteurs $\ell \in L$ tels que $m(L) = \langle \ell, \ell \rangle$ sont appelés les *vecteurs minimaux* de L. Le nombre

$$\operatorname{disc}(L) = \det(\langle \ell_i, \ell_j \rangle), \tag{4}$$

où (ℓ_i) est une base de L, ne dépend pas de la base choisie et s'appelle le *discriminant* de L. Posons

$$\gamma(L) = m(L)/\operatorname{disc}(L)^{1/n}. \tag{5}$$

Le volume de E modulo L est $v = \sqrt{\operatorname{disc}(L)}$. L'empilement de sphères associé à L est formé de sphères de rayon $r = \frac{1}{2}\sqrt{m(L)}$ et sa densité est, d'après la formule (1)

$$d(L) = 2^{-n}\, b_n\, \gamma(L)^{n/2},$$

où $b_n = \pi^{n/2}/\Gamma\left(\frac{n+2}{2}\right)$ est le volume de la boule unité de E.

Le nombre $\gamma_n = \sup_L \gamma(L)$ est appelé la *constante d'Hermite* (en dimension n). Il est lié à la densité maximale d_n des réseaux de E par la relation

$$d_n = 2^{-n}\, b_n\, \gamma_n^{n/2}.$$

On a $\gamma_n \geq 1$: en effet si L est un réseau de E engendré par une base orthonormale de E, on a $m(L) = \mathrm{disc}(L) = \gamma(L) = 1$. Par ailleurs de l'inégalité $d_n \leq 1$ on déduit $\gamma_n = O(n)$.

Il est commode d'appeler *réseau euclidien* un $\mathbf{Z}$-module libre de rang fini L muni d'une application bilinéaire symétrique $B : L \times L \to \mathbf{R}$ "définie positive", *i.e.* possédant les propriétés équivalentes suivantes :

i) la forme bilinéaire sur $L \otimes_{\mathbf{Z}} \mathbf{R}$ qui prolonge B est définie positive ;

ii) la matrice de B dans une base de L est définie positive ;

iii) pour tout $c \geq 0$, il n'y a qu'un nombre fini d'éléments $\ell \in L$ tels que $B(\ell, \ell) \leq c$;

iv) il existe $c > 0$ tel que, pour tout $\ell \in L$, $\ell \neq 0$, on ait $B(\ell, \ell) > c$.

Sous ces hypothèses, $E = L \otimes_{\mathbf{Z}} \mathbf{R}$ est un espace euclidien et L un réseau de E ; cela permet de définir $m(L)$, $\mathrm{disc}(L)$, $\gamma(L)$, $d(L)$. Tout réseau dans un espace euclidien peut être considéré comme un réseau euclidien. Un réseau euclidien est dit *unimodulaire* si son discriminant est 1, *entier* si l'on a $B(L \times L) \subset \mathbf{Z}$, *pair* s'il est entier et que $B(\ell, \ell)$ est pair pour tout $\ell \in L$. Un réseau euclidien est dit *semblable* à (L, B) s'il est isomorphe à $(L, \lambda B)$ pour un nombre réel $\lambda > 0$.

2.2. Existence d'un réseau de densité maximale

Les réseaux de l'espace euclidien $\mathbf{R}^n$ sont paramétrés par l'ensemble $\mathrm{GL}_n(\mathbf{R})/\mathrm{GL}_n(\mathbf{Z})$: à une classe $g\mathrm{GL}_n(\mathbf{Z})$ correspond le réseau $g(\mathbf{Z}^n)$. On munit l'ensemble des réseaux de $\mathbf{R}^n$ de la topologie quotient de celle de $\mathrm{GL}_n(\mathbf{R})$; la fonction $L \mapsto \gamma(L)$ est continue sur cet ensemble. Les réseaux de $\mathbf{R}^n$ de densité maximale sont ceux en lesquels la fonction γ atteint son maximum. On a $\gamma(\lambda L) = \gamma(L)$ pour tout $\lambda > 0$. Pour étudier les maxima de γ, on peut donc se restreindre à l'ensemble des réseaux unimodulaires de $\mathbf{R}^n$, qui s'identifie à $\mathrm{SL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{Z})$.

PROPOSITION 1.— *L'application* $\gamma : \mathrm{SL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{Z}) \to]0, +\infty[$ *est propre.*

C'est une conséquence de la théorie de la réduction de Minkowski : toute classe $\bar{g} \in \mathrm{SL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{Z})$ possède un représentant $g \in \mathrm{SL}_n(\mathbf{R})$ de la

forme kau, avec $k \in \mathrm{SO}_n(\mathbf{R})$, $a = \mathrm{diag}(t_1, \cdots, t_n)$ une matrice diagonale de déterminant 1 à coefficients positifs telle que $t_i \leq \frac{2}{\sqrt{3}} t_{i+1}$ pour $1 \leq i < n$, et u une matrice triangulaire supérieure unipotente dont les coefficients appartiennent à $[0,1]$. On a par définition $\gamma(\bar{g}) = \inf_{x \in \mathbf{Z}^n, x \neq 0} \langle gx, gx \rangle$, d'où $\gamma(\bar{g}) \leq \langle ge_1, ge_1 \rangle = t_1^2$. Il en résulte facilement que, pour tout $\varepsilon > 0$, l'image réciproque de $[\varepsilon, +\infty[$ par γ est une partie compacte de $\mathrm{SL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{Z})$, d'où la proposition.

La prop. 1 est parfois appelée "critère de Mahler". On en trouvera une autre démonstration dans [B], ch. 8, p. 187 et des généralisations dans [G], n° 2.2.

COROLLAIRE.— *Il existe des réseaux L de $\mathbf{R}^n$ de densité maximale (i.e. tels que $\gamma(L) = \gamma_n$).*

En effet, $\gamma : \mathrm{SL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{Z}) \to]0, +\infty[$ est une application continue, propre, majorée, donc atteint son maximum.

2.3. Réseaux extrêmes

DÉFINITION 1.— *Soit L un $\mathbf{Z}$-module libre de rang fini. Un sous-ensemble S de L est dit* parfait *si :*

i) *il existe une application bilinéaire symétrique $B : L \times L \to \mathbf{R}$ et une seule telle que $B(\ell, \ell) = 1$ pour $\ell \in S$;*

ii) *l'application B est définie positive et S est l'ensemble de ses vecteurs minimaux.*

Remarque.— Soit n le rang de L. L'espace vectoriel V des applications bilinéaires symétriques de $L \times L$ dans $\mathbf{R}$ est de dimension $n(n+1)/2$. Soit S un sous-ensemble parfait de L. De l'assertion d'unicité dans la condition i) de la définition, on déduit que l'espace vectoriel dual V^* est engendré par les formes linéaires $u \mapsto u(s,s)$, pour $s \in S$. En particulier, S contient au moins $\frac{n(n+1)}{2}$ paires de vecteurs opposés et l'on a $\mathrm{Card}(S) \geq n(n+1)$. Par ailleurs, si B est comme dans la définition, les coefficients matriciels de B dans une base de L s'obtiennent en résolvant un système d'équations linéaires à coefficients entiers. Ils sont donc rationnels.

Un réseau L d'un espace euclidien E de dimension n est dit *parfait* si l'ensemble S de ses vecteurs minimaux est parfait. (Dans ce cas, l'application B de la déf. 1 est l'application $(\ell, \ell') \mapsto \langle \ell, \ell' \rangle / m(L)$.) Le réseau L est dit *eutactique* si l'application identique de E peut s'écrire sous la forme $\sum_{s \in S} \lambda_s p_s$, où les λ_s sont des nombres réels > 0 et p_s désigne le projecteur orthogonal dans E d'image $\mathbf{R}s$.

Un réseau de E est dit *extrême* s'il correspond à un maximum local de la fonction γ. En étudiant, au voisinage d'un réseau L de E, le développement limité à l'ordre 2 de γ, on obtient la caractérisation suivante des réseaux extrêmes :

PROPOSITION 2 (Voronoï [Vo]).— *Un réseau de E est extrême si et seulement si il est parfait et eutactique.*

On en déduit, grâce à la remarque :

COROLLAIRE 1.—*Un réseau extrême de E a au moins $n(n+1)$ vecteurs minimaux.*

COROLLAIRE 2.—*Soit L un réseau extrême de E. La matrice du produit scalaire de E dans une base de L est proportionnelle à une matrice à coefficients rationnels. En particulier $\gamma(L)^n$ est rationnel.*

COROLLAIRE 3.—*La constante d'Hermite γ_n est la racine n-ième d'un nombre rationnel.*

Les classes modulo $GL_n(\mathbf{Z})$ de sous-ensembles parfaits de $\mathbf{Z}^n$ correspondent bijectivement aux classes de similitude de réseaux parfaits de rang n. Voronoï a démontré que ces classes sont en nombre fini et a donné un algorithme permettant (au moins en principe) d'en dresser la liste. D'après la prop. 2, l'algorithme de Voronoï fournit la liste (finie) des maxima locaux de γ et permet donc de calculer la constante d'Hermite γ_n.

En dimension 3, le seul réseau parfait (à similitude près) est A_3 (Gauss, 1831). Les réseaux parfaits en dimension 4 et 5 ont été déterminés par Korkine et Zolotareff ([K,Z],1877), en dimension 6 par Barnes (1957). En dimension 7, on connaît grâce à Stacey une liste de 33 réseaux parfaits

non semblables ; des calculs sur ordinateurs, effectués en ce moment par D.-O. Jaquet, en utilisant l'algorithme de Voronoï, devraient permettrent de prouver que cette liste est complète[1].

Pour une généralisation de ces résultats aux réseaux G-stables dans un espace euclidien muni d'un groupe fini d'automorphismes G, et des applications à la géométrie des nombres, on pourra consulter [B,M].

2.4. Quelques valeurs de la constante d'Hermite

Pour $n \leq 8$, on connaît la valeur de γ_n et on sait qu'il n'existe à similitude près qu'un seul réseau euclidien L de rang n tel que $\gamma(L) = \gamma_n$. (Pour $n \leq 6$, c'est une conséquence des résultats décrits à la fin du n° 2.3 ; pour $n = 7$ et $n = 8$, cela a été démontré par Blichfeldt.) On a la table suivante (où un symbole tel que D_4, par exemple, désigne le réseau engendré par le système de racines D_4) :

n	L	m(L)	disc(L)	γ_n	d_n
1	A_1	2	2	1	1
2	A_2	2	3	1,1547...	0,9068...
3	D_3	2	4	1,2599...	0,7404...
4	D_4	2	4	1,4142...	0,6168...
5	D_5	2	4	1,5157...	0,4652...
6	E_6	2	3	1,6653...	0,3729...
7	E_7	2	2	1,8114...	0,2952...
8	E_8	2	1	2	0,2536...

On ne connaît la valeur de γ_n pour aucun entier $n \geq 9$. On trouvera, pour $n \leq 24$ et pour certaines valeurs de n comprises entre 24 et 2^{20}, les réseaux de rang n les plus denses connus (avant les travaux d'Elkies et Shioda) dans les tables de [C,S], p. 15 à 17.

Pour n petit, les "réseaux laminés" jouent un rôle important. Ils sont définis par récurrence sur n ; un réseau L de rang n est dit laminé si :

[1] Ces calculs ont été achevés en juillet 1990, après 100 jours CPU de calcul sur VAX. Effectivement, la liste de Stacey est complète.

i) il contient un réseau laminé L' de rang $n-1$ tel que $m(L') = m(L)$;

ii) il est de densité maximale parmi les réseaux ayant la propriété i).

Pour $n \leq 25$, on connaît tous les réseaux laminés ([C,S], ch. 6) ; ils sont plus denses que les autres réseaux de rang n connus, sauf pour $n = 11$, 12, 13.

Nous avons indiqué ci-dessous quelques valeurs de n pour lesquelles un réseau particulièrement dense L est connu. Son influence se fait sentir dans les dimensions voisines : on trouve par exemple des réseaux denses de rang $n-1$ parmi ses sections hyperplanes.

n	L	découvert par	m(L)	disc(L)	$\gamma(L)$
12	K_{12}	Coxeter et Todd	4	3^6	$4/\sqrt{3}$
24	Λ_{24}	Leech	4	1	4
32	Q_{32}	Quebbemann	6	2^{16}	$3\sqrt{2}$

2.5. Réseaux de grand rang

Supposons $n \geq 2$. Comme au n° 2.2, l'ensemble X des réseaux unimodulaires de $\mathbf{R}^n$ s'identifie à $SL_n(\mathbf{R})/SL_n(\mathbf{Z})$. Il existe sur X une unique mesure μ de masse 1, invariante par $SL_n(\mathbf{R})$. D'après un théorème de Siegel ([Si]), on a pour toute fonction continue à support compact f sur $\mathbf{R}^n$

$$\int_{\mathbf{R}^n} f(x)dx_1 \cdots dx_n = \zeta(n) \int_X \Big(\sum_{\ell \in L^{\mathrm{prim}}} f(\ell) \Big)\, d\mu(L), \tag{6}$$

où L^{prim} désigne l'ensemble des vecteurs primitifs de L (*i.e.* n'appartenant à mL pour aucun entier $m \geq 2$) et ζ la fonction zêta de Riemann.

Soit $r > 0$ un nombre réel tel que $\mathrm{vol}(B(0,r)) < 2\zeta(n)$. Il existe une fonction continue à support compact $f : \mathbf{R}^n \to [0,1]$, égale à 1 sur $B(0,r)$, d'intégrale $< 2\zeta(n)$. En appliquant (6) à cette fonction, on voit qu'il existe un réseau unimodulaire de $\mathbf{R}^n$ tel que $\sum_{\ell \in L^{\mathrm{prim}}} f(\ell) < 2$. Pour un tel réseau, on a $m(L) > r$, $\mathrm{disc}(L) = 1$, d'où $d(L) > 2^{-n}\,\mathrm{vol}(B(0,r))$. Nous avons ainsi démontré l'inégalité

$$d_n \geq 2^{1-n}\,\zeta(n). \tag{7}$$

(théorème de Minkowski). On ne sait pas construire explicitement des réseaux aussi denses pour n arbitrairement grand. Divers auteurs (Litsyn, Tsfasman, Quebbemann, Rosenbloom, etc.) ont cependant exhibé des suites de réseaux, dont le rang tend vers l'infini, et dont la densité satisfait une inégalité de la forme $d \geq c^n$ pour une constante c. (La meilleure constante c est pour l'instant $2^{-1,39}$; *cf.* [T,R]).

3. LES RÉSEAUX D'ELKIES ET SHIODA

Dans une conférence aux journées arithmétiques de Luminy au printemps 1989, Tsfasman signale l'intérêt pour les empilements de sphères de divers réseaux euclidiens intervenant en théorie des nombres et en géométrie algébrique. Cela donne l'idée à Elkies d'examiner la situation suivante : on choisit une courbe elliptique définie sur un corps global K, et on prend pour réseau euclidien le groupe $E(K)/E(K)_{\text{tors}}$, muni de la hauteur de Néron-Tate. Du point de vue des empilements de sphères, ces réseaux semblent peu intéressants lorsque K est un corps de nombres. (On ne sait même pas si, pour $K = \mathbf{Q}$, leur rang peut être arbitrairement grand.) Par contre, en prenant pour K un corps de fonctions d'une variable sur un corps fini et en choisissant E astucieusement, on découvre de nouveaux empilements de sphères plus denses que ceux connus auparavant.

Indépendamment et à la même époque, Shioda avait entrepris, dans une série d'articles ([Sh.1-6]), l'étude des liens entre la géométrie des surfaces elliptiques (sur un corps non nécessairement fini) et l'arithmétique des groupes de Mordell-Weil associés. La théorie des surfaces elliptiques est essentiellement équivalente à celle des courbes elliptiques sur les corps de fonctions d'une variable, quoique le dictionnaire pour passer de l'une à l'autre soit parfois délicat (*cf.* [Ta], §4). Au cours de son étude, Shioda obtient des résultats sur les empilements de sphères du même type que ceux d'Elkies ([Sh.6]).

3.1. Courbes elliptiques sur un corps de fonctions

Soient k un corps fini de cardinal $q = p^r$, et K un corps de fonctions d'une variable sur k : autrement dit, K est le corps des fonctions rationnelles d'une courbe projective lisse absolument irréductible X définie sur k. On définit une application deg : $K \to \mathbf{N}$ en associant à une fonction rationnelle sur X son degré.

Considérons une courbe elliptique E définie sur K. Le groupe $E(K)$ est de type fini. Il existe une unique forme quadratique positive $h : E(K) \to \mathbf{R}$ possédant la propriété suivante : si $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ est un modèle de Weierstrass de E, l'application $P \mapsto h(P) - \frac{1}{2} \deg(x(P))$ de $E(K) - \{0\}$ dans $\mathbf{R}$ est bornée. (L'application h est, à un facteur multiplicatif $\log q$ près, la *hauteur de Néron-Tate* de E.) Le sous-groupe de torsion $E(K)_{\text{tors}}$ de $E(K)$ est formé des points P tels que $h(P) = 0$; il est fini. Posons $L = E(K)/E(K)_{\text{tors}}$. De l'application bilinéaire $(P, Q) \mapsto h(P+Q) - h(P) - h(Q)$ associée à h, on déduit par passage au quotient une application bilinéaire symétrique définie positive de $L \times L$ dans $\mathbf{R}$. Muni de cette application, L est un réseau euclidien que nous appellerons le *réseau de Mordell-Weil* de E. Pour étudier l'empilement de sphères associé à L, il convient de déterminer :

i) le rang n du $\mathbf{Z}$-module libre L ;

ii) le nombre $m(L) = \inf_{\ell \in L, \ell \neq 0} \langle \ell, \ell \rangle = 2 \inf_{P \in E(K) - E(K)_{\text{tors}}} h(P)$;

iii) le discriminant de L.

Le discriminant de L est l'un des ingrédients intervenant dans la conjecture de Birch et Swinnerton-Dyer (formulée pour les corps de fonctions par Tate dans [Ta]). Rappelons-en brièvement l'énoncé. Si v est une place de K (*i.e.* un point fermé de X), et si q_v est le cardinal du corps résiduel $k(v)$, le nombre de points à valeurs dans $k(v)$ d'un modèle de Weierstrass de E minimal en v est de la forme $1 + q_v - a_v$, avec $|a_v| \leq 2\sqrt{q_v}$. On pose $L_v(s) = (1 - a_v q_v^{-s} + q_v^{1-2s})^{-1}$ si E a bonne réduction en v et $L_v(s) = (1 - a_v q_v^{-s})^{-1}$ sinon. La série de Dirichlet $\prod_v L_v(s)$, appelée *fonction L de Hasse-Weil* de E sur K, est de la forme $L_{E/K}(q^{-s})$, où $L_{E/K}$ est une fonction rationnelle. La conjecture de Birch et Swinnerton-Dyer affirme que :

i) *la fonction rationnelle $L_{E/K}$ possède au point q^{-1} un zéro de multiplicité égale au rang n de $E(K)/E(K)_{\mathrm{tors}}$;*

ii) *le groupe de Tate-Šafarevič $Ш(E/K)$, qui classifie les espaces principaux homogènes sous E possédant un point rationnel sur chacun des complétés K_v de K, est fini ;*

iii) *la fonction rationnelle $L_{E/K}(T)/(1-qT)^n$ prend au point q^{-1} la valeur*

$$q^{1-g}\,\frac{\mathrm{Card}\,(Ш(E/K))\,\mathrm{disc}(L)}{\mathrm{Card}\,(E(K)_{\mathrm{tors}})^2}\prod_v c_v, \tag{8}$$

où g est le genre de X et où, pour chaque place v de K, c_v est le nombre des composantes connexes de la fibre géométrique en v du modèle de Néron de E, qui sont définies sur $k(v)$.

Fort heureusement, on dispose de nombreux résultats positifs dans cette direction :

a) *L'ordre n' de la fonction $L_{E/K}$ au point q^{-1} est toujours supérieur ou égal à n* (*cf.* [Ta], démonstration du th. 5.2).

b) *L'égalité $n' = n$ est équivalente à la finitude de $Ш(E/K)$ et implique la formule* (8). La "partie première à p" de cet énoncé a été démontrée par Tate ([Ta], th. 5.2), modulo une conjecture (*loc. cit.*, p. 13, conjecture (d)) qui a été prouvée par Gordon ([Go]). La "partie divisant p" de l'énoncé a été démontrée par Milne ([Mil.2]). Milne suppose $p \neq 2$ car il utilise un théorème de dualié plate pour les surfaces (Ann. Sci. ENS 9 (1976)), qui réfère (*loc. cit.*, p. 189) à un article de Bloch (IHES, vol. 47) ; en remplaçant cette dernière référence par un article d'Illusie (Ann. Sci. ENS 12 (1979)), on s'affranchit de l'hypothèse $p \neq 2$.

c) *La conjecture de Birch et Swinnerton-Dyer est démontrée lorsque la courbe elliptique E est constante* (*i.e.* provient par extension des scalaires d'une courbe elliptique définie sur k) ; un énoncé analogue vaut d'ailleurs pour les variétés abéliennes ([Mil.1], th. 3). Plus généralement :

d) *La conjecture de Birch et Swinnerton-Dyer est démontrée lorsque E est la tordue d'une courbe elliptique constante, i.e. lorsque $j(E)$ appartient à k.* En effet, il existe alors une extension galoisienne finie K' de K sur laquelle E devient une courbe elliptique constante. Le groupe

$Ш(E/K')$ est fini d'après c). Le noyau de l'homomorphisme canonique $Ш(E/K) \to Ш(E/K')$ est annulé par $[K';K]$ et tout sous-groupe de $Ш(E/K)$ d'exposant fini est fini. Par suite, $Ш(E/K)$ est fini et E satisfait à la conjecture de Birch et Swinnerton-Dyer, d'après b).

Ces résultats permettent, dans les exemples considérés par Elkies et Shioda, de déduire de la formule (8) des minorations du discriminant de L.

3.2. Cas où la courbe elliptique est constante

Nous allons expliciter les résultats du numéro précédent dans le cas particulier simple où la courbe elliptique considérée sur K est constante, c'est-à-dire provient par extension des scalaires de k à K d'une courbe elliptique E définie sur k.

Le groupe $E(K)$: il s'identifie au groupe $\mathrm{Mor}_k(X,E)$ des morphismes de X dans E (définis sur k). En effet, se donner un point de $E(K)$ équivaut à se donner une application rationnelle de X dans E, et une telle application se prolonge de façon unique en un morphisme de X dans E.

La forme quadratique $h : E(K) \to \mathbf{R}$: elle s'identifie à l'application $u \mapsto \deg u$ de $\mathrm{Mor}_k(X,E)$ dans $\mathbf{R}$.

Le sous-groupe de torsion $E(K)_{\mathrm{tors}}$: il est égal à $E(k)$ et s'identifie au sous-groupe de $\mathrm{Mor}_k(X,E)$ formé des morphismes constants de X dans E.

Le Z-module $L = E(K)/E(K)_{\mathrm{tors}}$: il est canoniquement isomorphe au groupe $\mathrm{Hom}_k(J(X),E)$ des morphismes de variétés abéliennes de $J(X)$ (la jacobienne de X) dans E,définis sur k. En effet, l'homomorphisme $u \mapsto u_*$ de $\mathrm{Mor}_k(X,E)$ dans $\mathrm{Hom}_k(J(X),E)$ (où u_* est déduit de u par fonctorialité d'Albanese) est surjectif, et son noyau est formé des morphismes constants de X dans E.

Le rang n **de** L. La variété abélienne $J(X)$ est k-isogène à un produit $A_1 \times \cdots \times A_m$ de variétés abéliennes simples sur k. Si s est le nombre de celles qui sont k-isogènes à E et si t est le rang du $\mathbf{Z}$-module $\mathrm{End}_k(E)$, on a $n = st$: en effet $\mathrm{Hom}_k(A_i,E)$ est de rang t si A_i est isogène à E et est nul sinon.

Nous allons décrire une autre façon de calculer n. Pour cela, considérons la fonction $Z(X,T)$ de la courbe X, définie par

$$Z(X,T) = \prod_v \left(1 - T^{[k(v):k]}\right)^{-1} \tag{9}$$

(où v parcourt l'ensemble des points fermés de X). C'est une fonction rationnelle en T, de la forme

$$Z(X,T) = \frac{\prod_{i=1}^{2g}(1-\alpha_i T)}{(1-T)(1-qT)} \tag{10}$$

où g est le genre de X et $\alpha_1, \cdots, \alpha_{2g}$ des nombres complexes de valeur absolue $q^{1/2}$. Écrivons de même

$$Z(E,T) = \frac{(1-\beta_1 T)(1-\beta_2 T)}{(1-T)(1-qT)}. \tag{11}$$

PROPOSITION 3.— *Le rang du* $\mathbf{Z}$*-module* $L = E(K)/E(K)_{\text{tors}}$ *est le nombre de couples* (i,j)*, avec* $1 \leq i \leq 2g$, $1 \leq j \leq 2$ *tels que* $\alpha_i = \beta_j$.

Soit ℓ un nombre premier distinct de p. Les points de ℓ^∞-torsion de $J(X)$ et E permettent de définir des représentations ℓ-adiques de $\mathrm{Gal}(\bar{k}/k)$ dans des $\mathbf{Q}_\ell$-espaces vectoriels $V_\ell(J(X))$ et $V_\ell(E)$ de dimensions respectives $2g$ et 2. D'après un théorème de Tate, les $\mathbf{Q}_\ell$-espaces vectoriels $L \otimes_{\mathbf{Z}} \mathbf{Q}_\ell = \mathrm{Hom}_k(J(X),E) \otimes_{\mathbf{Z}} \mathbf{Q}_\ell$ et $\mathrm{Hom}_{\mathrm{Gal}(\bar{k}/k)}(V_\ell(J(X)), V_\ell(E))$ sont isomorphes. Leur dimension est le nombre de couples (i,j) tels que $\alpha_i = \beta_j$, car l'automorphisme de Frobenius $x \mapsto x^q$ de $\bar{k}$, qui engendre $\mathrm{Gal}(\bar{k}/k)$ topologiquement, opère sur $V_\ell(J(X))$ et $V_\ell(E)$ suivant des endomorphismes semi-simples, de polynômes caractéristiques respectifs $\prod_{i=1}^{2g}(T-\alpha_i)$ et $\prod_{j=1}^{2}(T-\beta_j)$.

Le nombre $m(L)$. Par définition, on a

$$m(L) = \inf_{\ell \in L, \ell \neq 0} \langle \ell, \ell \rangle = 2 \inf_u \deg u, \tag{12}$$

où la seconde borne inférieure est prise sur l'ensemble des morphismes non constants $u : X \to E$, définis sur k. Par ailleurs, il est clair que, pour toute extension finie k' de k, on a

$$\inf_u \deg u \geq \mathrm{Card}(X(k'))/\mathrm{Card}(E(k')). \tag{13}$$

Cela permet de minorer $m(L)$.

La fonction de Hasse-Weil de E sur K. Conservons les notations des formules (9), (10), (11). Soit v un point fermé de X. Notons $k(v)$ son corps résiduel et posons $q_v = \mathrm{Card}(k(v))$, $\deg v = [k(v) : k]$. Le cardinal de $E(k(v))$ est $1 - a_v + q_v$, avec $a_v = \beta_1^{\deg v} + \beta_2^{\deg v}$. On a $\beta_1\beta_2 = q$. La fonction de Hasse-Weil de E sur K, égale à $\prod_v (1 - a_v q_v^{-s} + q_v^{1-2s})^{-1}$, s'écrit donc $L_{E/K}(q^{-s})$, avec

$$
\begin{aligned}
L_{E/K}(T) &= \prod_v ((1 - (\beta_1 T)^{\deg v})(1 - (\beta_2 T)^{\deg v}))^{-1} \\
&= Z(X, \beta_1 T) Z(X, \beta_2 T) = Z\Big(X, \frac{qT}{\beta_1}\Big) Z\Big(X, \frac{qT}{\beta_2}\Big).
\end{aligned} \tag{14}
$$

On constate que, conformément à la conjecture de Birch et Swinnerton-Dyer (qui comme nous l'avons dit est ici un théorème de Milne), la fonction $L_{E/K}$ possède en q^{-1} un zéro de multiplicité égale au nombre de couples (i, j) tels que $\alpha_i = \beta_j$, c'est-à-dire (prop. 3) au rang n de $E(K)/E(K)_{\mathrm{tors}}$.

Le discriminant de L. Le théorème de Milne nous dit que la valeur en q^{-1} de $L_{E/K}(T)/(1 - qT)^n$ est

$$
\frac{q^{1-g}\,\mathrm{Card}\,(Ш(E/K))\,\mathrm{disc}\,(L)}{\mathrm{Card}\,(E(K)_{\mathrm{tors}})^2}.
$$

Compte tenu des relations (10), (14) et du fait que le groupe $E(K)_{\mathrm{tors}}$, égal à $E(k)$, a pour cardinal $(1 - \beta_1)(1 - \beta_2)$, on a

$$
\mathrm{Card}\,(Ш(E/K))\,\mathrm{disc}\,(L) = q^g \prod_{\alpha_i \neq \beta_j} \Big(1 - \frac{\alpha_i}{\beta_j}\Big). \tag{15}
$$

3.3. Un exemple

Soit q une puissance d'un nombre premier p. Considérons sur le corps $k = \mathbf{F}_{q^2}$ la courbe de Fermat X d'équation

$$
x^{q+1} + y^{q+1} + z^{q+1} = 0
$$

Lemme.— a) *Le genre de* X *est* $g = q(q-1)/2$.

b) *Le cardinal de* $X(k)$ *est* $q^3 + 1$.

c) *On a* $Z(X,T) = (1+qT)^{2g}/((1-T)(1-q^2T))$.

d) *Soit* π *l'endomorphisme de Frobenius (relatif à* k*) de la jacobienne de* X.

On a $\pi + q = 0$.

L'assertion a) résulte de ce que X est une courbe projective plane lisse de degré $q+1$.

Lorsque x décrit $k = \mathbf{F}_{q^2}$, x^{q+1} prend une fois la valeur 0 et $q+1$ fois chaque valeur dans $\mathbf{F}_q^\times$. On a des résultats analogues pour y et z. Un comptage élémentaire fournit alors l'assertion b).

La fonction rationnelle $Z(X,T)$ admet une expression de la forme $\prod_{i=1}^{2g}(1-\alpha_i T)/((1-T)(1-q^2T))$ et l'on a

$$\mathrm{Card}\,(X(k)) = 1 + q^2 - \sum_{i=1}^{2g} \alpha_i.$$

Par suite, d'après b), la somme des α_i est égale à $q^2 - q^3$, c'est-à-dire à $-2gq$. Comme les α_i sont de valeur absolue q, il sont égaux à $-q$.

Soit ℓ un nombre premier distinct de p. On sait que π opère sur $V_\ell(J(X))$ suivant un endomorphisme semi-simple, dont le polynôme caractéristique est $\prod_{i=1}^{2g}(T-\alpha_i) = (T+q)^{2g}$. Il en résulte que $\pi + q$ annule $V_\ell(J(X))$, donc que le noyau de $\pi + q$ contient tous les points de $J(X)$ d'ordre une puissance de ℓ. Cela entraîne l'égalité $\pi + q = 0$.

Choisissons une courbe elliptique E, définie sur k, telle que $E(k)$ ait $q^2 + 2q + 1$ éléments. (Il en existe ; par exemple, si q est un nombre premier ≥ 5, n'importe quelle courbe elliptique supersingulière définie sur $\mathbf{F}_q$ convient.) On a $Z(E,T) = (1+qT)^2/((1-T)(1-q^2T))$. Soit K le corps des fonctions de la courbe de X. Nous allons appliquer les résultats du numéro précédent au réseau de Mordell-Weil $L = E(K)/E(K)_{\mathrm{tors}}$.

PROPOSITION 4.— a) *Le rang* n *de* L *est* $4g = 2q(q-1)$.

b) *On a* $m(L) \geq 2(q-1)$.

c) *On a* $\mathrm{Card}\,(Ш(E/K))\,\mathrm{disc}\,(L) = q^{2g} = q^{q(q-1)}$.

d) *On a* $\gamma(L) \geq 2(q-1)/\sqrt{q}$.

L'assertion a) résulte de la prop. 3 (tous les α_i et β_j sont égaux à $-q$). On a

$$\mathrm{Card}(X(k))/\mathrm{Card}(E(k)) = (q^3+1)/(q+1)^2 > q-2,$$

donc b) résulte des formules (12) et (13). L'assertion c) est un cas particulier de la formule (15) ; elle implique l'inégalité $\mathrm{disc}(L) \leq q^{2g}$. Enfin, d) se déduit de ce qui précède, puisque l'on a $\gamma(L) = m(L)/\mathrm{disc}(L)^{1/n}$.

Pour obtenir de meilleures majorations du discriminant de L, il convient d'étudier le groupe Ш(E/K). C'est ce qu'a fait Gross ([Gr], prop. 14.10) : il démontre que Ш(E/K) est nul si q est égal à p ou à p^2, et non nul si p^3 divise q ; par exemple, pour $q = p^3$, on a $\mathrm{Card}(Ш(E/K)) \geq p^{p^3(p-1)^3/2}$.

Gross ([Gr]) construit et caractérise de façon purement algébrique les réseaux L ci-dessus. Il en tire des informations sur leur géométrie : lorsque $q = p^2$, par exemple, on a $\langle \ell, \ell' \rangle \in p\mathbf{Z}$ pour ℓ, ℓ' dans L, et $\left(L, \frac{1}{p}\langle\ ,\ \rangle\right)$ est un réseau entier unimodulaire pair.

Le réseau L construit dans ce numéro est isomorphe à D_4 pour $q = 2$, au réseau de Coxeter-Todd K_{12} pour $q = 3$, et semblable au réseau de Leech pour $q = 4$.

Remarque.— Les réseaux de Mordell-Weil que nous avons considérés ont un rang élevé parce que la courbe de Fermat X d'équation (16) satisfait aux conditions équivalentes c) et d) du lemme. D'autres courbes remplissent ces conditions (entre autres, les quotients de X) et fournissent également de bons empilements de sphères. Notons que l'équation (16) s'écrit $x\overline{x} + y\overline{y} + z\overline{z} = 0$ (avec $\overline{x} = x^q$), et se transforme, après un changement linéaire convenable de coordonnées, en $x\overline{y} + y\overline{x} - z\overline{z} = 0$. Donc $x + x^q = z^{q+1}$ est un modèle affine de X. Pour tout entier f qui divise $q+1$, $x + x^q = z^f$ est un modèle affine d'un quotient de X ; si de plus q est une puissance de 2, $u^2 + u = v^f$ est un modèle affine d'un quotient de X, comme on le voit en posant $u = x + x^2 + x^4 + \cdots + x^{q/2}$ et $v = z$.

Exemple.— Si l'on prend pour X la courbe d'équation $y^2 + y = x^{q+1}$ sur le

corps $k = \mathbf{F}_{q^2}$, avec $q = 2^r$, et pour E la même courbe elliptique qu'avant, le réseau de Mordell-Weil associé L est entier, pair, de rang $2q$. Elkies décrit explicitement un sous-réseau d'indice fini de L semblable au réseau de Barnes-Wall BW_{2q}. Pour $q = 16$, L est un réseau de rang 32 qui a la même densité que le réseau de Quebbemann Q_{32} ; il est probablement isomorphe à Q_{32}, mais cela n'a pas été prouvé pour l'instant ; l'étude de certains trous profonds de L a permis à Elkies de construire un réseau euclidien de rang 33 plus dense que ceux connus auparavant. Pour $q = 32, 64, \cdots, 512$, les réseaux L ou certains de leurs sous-réseaux améliorent les records de densité en dimension $64, 128, \cdots, 1024$.

3.4. Conclusion

Dans cet exposé, nous n'avons étudié que le cas des courbes elliptiques constantes. D'autres courbes elliptiques ont été utilisées par Elkies et Shioda pour construire de bons empilements de sphères. Celles qui s'avèrent intéressantes sont des courbes elliptiques dont l'invariant modulaire $j(E)$ appartient à k (*i.e.* qui sont tordues de courbes constantes), et plus particulièrement celles considérées dans [T,S] pour obtenir des groupes de Mordell-Weil de grand rang. Il est parfois utile d'étudier des sous-réseaux du réseau de Mordell-Weil : par exemple, celui provenant des points de $E(K)$ dont la réduction en chaque place appartient à la composante neutre du modèle de Néron.

Il serait intéressant de savoir ce que l'on obtient en remplaçant E par une variété abélienne A (en particulier lorsque A est la jacobienne d'une courbe définie sur $\mathbf{F}_{q^2}$, pour laquelle les conditions c), d) du lemme de 3.3 sont satisfaites).

Il ne semble pas pour l'instant que les constructions d'Elkies et Shioda soient susceptibles de fournir des suites de réseaux dont le rang n tend vers l'infini, et dont la densité d est supérieure à c^n, pour une constante c convenable. Elles ont seulement permis d'exhiber des suites pour lesquelles $\log d$ est équivalent à $-\frac{n \log n}{12}$.(*)

(*) Elkies m'a signalé après l'exposé qu'il sait remplacer la condition $\log d \sim -\frac{n \log n}{12}$ par $-\log d = \mathcal{O}(n \log n^{0.5+\varepsilon})$, pour tout $\varepsilon > 0$.

Voici la liste de quelques dimensions n pour lesquelles un réseau L plus dense que ceux connus auparavant a été construit par les méthodes d'Elkies et Shioda. Pour chacune de ces dimensions, nous avons indiqué une minoration de $\log_2 \delta$, où $\delta = d(L)/b_n$ est la densité centrée de L ; afin de permettre la comparaison, nous avons rappelé entre parenthèses l'ancien record, lorsque celui-ci figure dans les tables de [C,S], p. 16-17.

n	54	64	80	104	128
$\log_2 \delta \geq$	15,88	24,71	40,14	67,01	97,40
		(22)	(36)	(60)	(88)
référence	[E]	[E]	[Sh.6]	[Sh.6]	[E]

n	256	508	512	520	1024
$\log_2 \delta \geq$	294,80	745,62	797,12	770,37	2018,24
	(270,89)	(742,66)	(698)	(767,46)	
référence	[E]	[Sh.6]	[E]	[Sh.6]	[E](**)

(**) La minoration de $\log_2 \delta$ figurant dans [E] est 2012,24 ; elle peut être remplacée par 2018,24, si l'on tient compte que dans l'exemple considéré le groupe $Ш(E/K)$ est d'ordre $\geq 2^{12}$.

BIBLIOGRAPHIE

[B,M] A.M. BERGÉ et J. MARTINET - *Réseaux extrêmes pour un groupe d'automorphismes*, à paraître dans les actes des Journées Arithmétiques de Luminy, 1989, éditions Astérisque.

[B] N. BOURBAKI - *Éléments de mathématique, Intégration*, Act. Sci. et Ind., ed. Hermann, 1963.

[C,S] J.H. CONWAY and N.J.A. SLOANE - *Sphere packings, lattices and groups*, Grundlehren der mathematischen Wissenschaften 290, Springer Verlag, 1988.

[Co] H.S.M. COXETER - *Introduction to Geometry*, John Wiley & sons, 1961.

[E] N. ELKIES - Lettres électroniques à N.J. SLOANE, du 15 août et du 15 septembre 1989.

[Fe] J. FEJES - *Über einen geometrischen Satz*, Math. Z. 46 (1940), 79-83.

[G] R. GODEMENT - *Domaines fondamentaux des groupes arithmétiques*, Séminaire Bourbaki, mai 1963, exposé n° 257, Benjamin, volume 1962-63, New York, 1966.

[Go] W.J. GORDON - *Linking the conjectures of Artin-Tate and Birch-Swinnerton-Dyer*, Compositio math. 38 (1979), 163-199.

[Gr] B.H. GROSS - *Group representations and lattices*, preprint.

[K,L] G.A. KABATIANSKY and V.I. LEVENSHTEIN - *Bounds for packings on a sphere and in space*, Problems of Information Transmission 14, n° 1, 1978, 1-17.

[K,Z] A. KORKINE et G. ZOLOTAREFF - *Sur les formes quadratiques positives*, Math. Ann. 11 (1977), 242-292.

[Mil.1] J.S. MILNE - *The Tate-Šafarevič group of a constant Abelian variety*, Invent. math. 6 (1968), 91-105.

[Mil.2] J.S. MILNE - *On a conjecture of Artin and Tate*, Annals of math. 102 (1975), 517-533.

[Ro] C.A. ROGERS - *Packing and covering*, Cambridge tracts in mathematics and mathematical physics, vol. 54, Cambridge University Press, 1964.

[R,T] M.Y. ROSENBLOOM and M.A. TSFASMAN - *Multiplicative lattices in global fields*, à paraître dans Invent. math., 1990.

[Sh.1] T. SHIODA - *The Galois representation of type E_8 arising from certain Mordell-Weil groups*, Proc. Jap. Acad. 65, Ser. A (1989), 195-197.

[Sh.2] T. SHIODA - *Mordell-Weil lattices and Galois representation*, I, II, III, Proc. Jap. Acad. 65, Ser. A (1989), 268-271, 296-299, 300-303.

[Sh.3] T. SHIODA - *Construction of elliptic curves over $\mathbf{Q}(t)$ with high rank : a preview*, Proc. Jap. Acad. 66, Ser. A (1989), 57-90.

[Sh.4] T. SHIODA - *Construction of elliptic curves with high rank via the invariants of the Weyl groups*, preprint.

[Sh.5] T. SHIODA - *Mordell-Weil lattices of type E_8 and deformation of singularities*, preprint.

[Sh.6] T. SHIODA - *Mordell-Weil lattices and sphere packings*, preprint.

[Si] C.L. SIEGEL - *A mean value theorem in the geometry of numbers*, Ann. of math. 46 (1945), 340-347.

[Ta] J. TATE - *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki 1965/66, exposé n° 306.

[T,S] J. TATE and I.R. ŠAFAREVIČ - *The rank of elliptic curves*, Dokl. Akad. Nauk SSSR 175 (= Soviet Math. 8) (1967), 917-925.

[Th] A. THUE - *Om nogle geometrisk-taltheoretiske Theoremer*, Forhandlige ved de Skandinaviske Naturforskeres, 14 Møde, Kjøbenhavn, 1882, 352-353.

[Vo] G. VORONOÏ - *Sur quelques propriétés des formes quadratiques positives parfaites*, J. reine angew. Math. 133 (1908), 97-178.

Joseph OESTERLÉ

Université de Paris 6
Département de Mathématiques
Tour 45-46 - 5ème étage
4 place Jussieu
F-75230 Paris Cedex 05