1. Que les polynômes $Q(x)$ associés à une suite convergente d'éléments $\theta \in \mathfrak{S}$ n'ont pas nécessairement pour limite une fraction rationnelle.

2. L'ensemble $\mathfrak{S}$ n'est fermé, il suffit pour le voir de considérer la suite des éléments $\theta_n \in \mathfrak{S}$ associée à la suite de polynômes

$$Q_n(x) = p^r + ax + bx^2 \sum_{i=0}^{n-2} x^i$$

où $|b| < |a| = 1$.

3. On obtient alors une suite de fonctions holomorphes et uniformément bornées pour $|x| \leqslant 1$, dont la limite n'est pas bornée pour $|x| = 1$.

Si K est un corps de fonctions algébriques (extension finie d'un corps de fractions rationnelles sur un corps fini) on peut obtenir des resultats analogues dans les adéles de K.

Si K est un corps de nombres algébriques, ces résultats montrent qu'on ne peut espérer obtenir des ensembles fermés que si l'on considère les zeros de $P(x)$ à la fois dans $K_\mathfrak{p}$ et dans le corps C des nombres complexes, ce qui revient à les étudier dans l'anneau des adéles de K.

Lorsque K est le corps des rationnels on connait de tels ensembles fermés, citons par exemple:

Ensemble S_p^0 des nombres de Chabauty [2]. *Un nombre $\theta \in Q_p$ appartient à S_p^0, si il est p-integrable, si les autres racines du polynôme associé $P(x)$ sont, dans Ω_p de valeur absolue strictement inférieure à* 1. *Et si, de plus, dans C toutes les racines de $P(x)$ sont inférieures à* 1, *en valeur absolue.*

Travaux cités

[1] P. Bateman et A. Duquette, *The analogue of the Pisot-Vijayaraghavan numbers in fields of formal power series*, Illinois J. of Math. 6 (1962), p. 594-606.

[2] C. Chabauty, *Sur la répartition modulo 1 de certaines suites p-adiques*, C. R. Acad. Sc. Paris 231 (1950), p. 465-466.

[3] G. H. Hardy, *A problem of diophantine approximation*, J. Indian Math. Soc. 11 (1919), p. 162-166.

[4] C. Pisot, *La répartition modulo 1 et les nombres algébriques*, Ann. Sc. Norm. Sup. Pisa, Ser. 2, 7 (1938), p. 205-248.

[5] — *Sur quelques approximations rationnelles caracteristiques des nombres algébriques*, C. R. Acad. Sc. Paris 206 (1938), p. 1862-1864.

[6] R. Salem, *A remarkable class of algebraic integers. Proof of a conjecture of Vijayaraghavan*, Duke Math. J. 11 (1944), p. 103-108.

[7] T. Vijayaraghavan, *On the fractional parts of the powers of a number* (II), Proc. Camb. Phil. Soc. 37 (1941), p. 349-357.

Reçu par la Rédaction le 6. 6. 1967

ACTA ARITHMETICA
XIV (1968)

Le „Problème des Octaèdres” en dimension 5*

par

R. Bantegnie (Lille)

0. Introduction. L'étude des réseaux de l'espace euclidien permis pour un *„Octaèdre”* et en contenant les sommets a été considérée dès Minkowski [5] pour $n \leqslant 3$ puis pour $n = 4$ par divers auteurs, cf. [6] et [8]. Nous-même, cf. [1] et [2], avons examiné pour $n \leqslant 4$ le cas général où les réseaux peuvent avoir des points dans les faces de l'octaèdre distincts de ses sommets (deuxième cas) et non seulement le cas où cela est exclu (premier cas).

Rappelons comment la considération des réseaux précédents intervient dans la détermination de la constante critique d'une jauge. Si J est une jauge de l'espace euclidien $\boldsymbol{R}^n$, on sait qu'un réseau critique de J possède, sur la frontière de J, n points linéairement indépendants e_i; soit M le réseau ayant pour base les e_i, Ω *„l'octaèdre”* enveloppe convexe ouverte des points $\pm e_i$; il est utile de déterminer les *types* des réseaux appartenant à la famille $\mathfrak{M}$ des réseaux contenant le réseau M et permis pour Ω puisqu'un réseau critique de J appartient à $\mathfrak{M}$; on peut aussi considérer la famille $\overline{\mathfrak{M}}$ des réseaux contenant M et dont l'intersection avec l'adhérence $\overline{\Omega}$ de Ω est l'union de l'origine 0 et des sommets $\pm e_i$ car un réseau critique de J appartient à $\overline{\mathfrak{M}}$ si J est strictement convexe.

Determiner les *types* des réseaux de $\overline{\mathfrak{M}}$, resp. $\mathfrak{M}$ constitue le *„Problème des Octaèdres”*.

La considération de $\overline{\mathfrak{M}}$ correspond au premier cas, celle de $\mathfrak{M}$ au second.

On désigne par $\overline{\mathfrak{L}}$, resp. $\mathfrak{L}$ les parties de $\overline{\mathfrak{M}}$, resp. $\mathfrak{M}$ formées des réseaux Λ pour lesquels le groupe Λ/M est cyclique. Notons d'une part que pour $n \leqslant 3$, Λ/M est toujours cyclique pour Λ dans $\mathfrak{M}$, d'autre part que la considération du cas cyclique est un pas nécessaire, cf. [2].

On désigne par $\overline{m}_n$, resp. m_n l'ordre maximum pour Λ dans $\overline{\mathfrak{M}}$, resp. $\mathfrak{M}$ du groupe Λ/M; $\overline{p}_n$, resp. p_n sont eux les ordres maximum de Λ/M pour Λ dans $\overline{\mathfrak{L}}$, resp. $\mathfrak{L}$.

* Ce travail fait partie d'une thèse presentée en 1967 à la Faculté des Sciences de Lille.

On a evidemment $p_n \leqslant m_n$ et les théorèmes généraux de Minkowski montrent que $m_n \leqslant n!$. Nous avons montré ailleurs, cf. [5], que l'on a $m_n < n!$ pour $n \geqslant 3$.

Laub dans un gros travail [4] a abordé pour $n = 5$ le premier cas dans l'hypothèse où Λ/M est cyclique. Il n'est guère possible d'aller plus loin que lui sans utiliser les moyens modernes de calcul. On s'est donc proposé, dans l'hypothèse où Λ/M est cyclique, et en considérant à la fois le premier et le second cas de présenter une méthode qui permette de fixer un programme de calcul valable pour tout n. Pour déterminer $\overline{p}_n$ ou p_n, on n'est plus limité que par les possibilités des machines électroniques.

Les contingences pratiques sont cependant contraignantes et nous avons dû nous contenter de la considération du cas $n = 5$.

Notons une distinction entre le premier et le second cas. Si l'on suppose qu'un point $A = \frac{1}{p}\sum_{i=1}^{n} a_i e_i$, où $a_1, \ldots, a_n, p$ sont des entiers strictement positifs premiers entre eux, est *permis* pour l'octaèdre enveloppe convexe des points $\pm e_i$ on peut *a priori* dans le premier cas se limiter à la considération du cas où a_n vaut 1 pour $n \leqslant 5$; au contraire cette limitation n'est possible dans le second cas que pour $n \leqslant 4$.

Il a fallu, pour éviter des temps de calcul trop longs, profiter d'une analyse en profondeur permettant d'éliminer „en bloc" certaines possibilités. Les moyens techniques mis à notre disposition (machine Bull M 40 du Laboratoire de Calcul de l'Université de Lille) ont permis de résoudre le cas $n = 5$. Les machines existant actuellement seraient incapables de donner une solution complète pour n plus grand.

Comme résultat, on obtient $\overline{p}_5 = 41$, $p_5 = 48$.

Le point $\frac{1}{41}(18e_1 + 16e_2 + 10e_3 + 4e_4 + e_5)$ est un point d'un réseau de $\overline{\mathfrak{L}}$, $\frac{1}{48}(23e_1 + 13e_2 + 7e_3 + 4e_4 + e_5)$ un point d'un réseau de $\mathfrak{L}$.

On complète en particulier les résultats de Laub.

Donnons pour terminer cette introduction la table des valeurs connues de $\overline{p}_n$, p_n, $\overline{m}_n$, m_n. Notre contribution a été de déterminer les nombres qui sont encerclés.

n	2	3	4	5
$\overline{p}_n$	1	2	5	41
p_n	2	4	16	48
$\overline{m}_n$	1	2	5	
m_n	2	4	18	

Les propriétés en jeu étant fort simples et bien connues pour $n = 1$ et 2 on suppose dans la suite $n \geqslant 3$.

1. Etude générale. On conserve les notations de l'introduction. On indexe si nécessaire les familles $\mathfrak{L}$, $\overline{\mathfrak{L}}$ etc. par l'indice n quand on les considère pour différentes valeurs de n. Les e_i $(1 \leqslant i \leqslant n)$ étant n points linéairement indépendants de $\boldsymbol{R}^n$, $\overline{\Omega}_n$ est donc l'enveloppe convexe des $2n$ points $\pm e_i$, Ω_n son intérieur. M est le réseau de base e_i.

On désigne par $\mathfrak{N}$ la famille des réseaux de $\boldsymbol{R}^n$ contenant M et par $\hat{\mathfrak{L}}$ la famille des réseaux Λ de $\mathfrak{N}$ tels que Λ/M soit un groupe cyclique; un réseau Λ de $\hat{\mathfrak{L}}$ est engendré par les points $e_1, \ldots, e_n$ et par un point $A = \frac{1}{p}\sum_{i=1}^{n} a_i e_i$ où les a_i sont entiers et p un entier positif; à un système $\{p; a_1, \ldots, a_n\}$ où p est entier positif et les a_i entiers on associe le point A comme ci-dessus et le réseau $\Lambda(A)$ engendré par $e_1, \ldots, e_n$ et A. On dit que A *engendre* $\Lambda(A)$. *L'ordre* de A est l'indice de M dans $\Lambda(A)$; cet indice vaut p/δ où δ est le p. g. c. d. des nombres $a_1, \ldots, a_n, p$. On dit que le point A est *réduit* si son ordre est p, autrement dit si les nombres $a_1, \ldots, a_n, p$ sont premiers entre eux dans leur ensemble.

Dans la suite on désigne par $(p_1, \ldots, p_r)$ le p. g. c. d. des r nombres $p_1, \ldots, p_r$. La notation $p \mid q$ pour un couple (p, q) d'entiers signifie que p divise q; $p \div q$ note la partie entière du quotient p/q.

On se propose *en gros* de déterminer $\mathfrak{L}$ et $\overline{\mathfrak{L}}$. Cependant on décrira un réseau de $\mathfrak{L}$ par un point l'engendrant; on introduit donc une relation d'équivalence entre les points:

Le point A et le point $A' = \frac{1}{p'}\sum_{i=1}^{n} a'_i e_i$ de même que les systèmes de nombres qui les représentent sont *(P)-équivalents* si $\Lambda(A)$ coïncide avec $\Lambda(A')$. Concernant cette relation d'équivalence, on a la

PROPOSITION 1. *Les points A et A' comme ci-dessus supposés réduits sont (P)-équivalents si et seulement si est vérifiée la condition*

(P') *On peut trouver s premier avec p tel que A' soit congru modulo M au point sA.*

De plus on a alors $p = p'$.

Preuve. Tout d'abord $\Lambda(A)$ et $\Lambda(A')$ coïncident si et seulement si l'on peut trouver des entiers s et s' tels que, pour chaque i, on ait le système de congruences

$$(*) \qquad \frac{a_i}{p} \equiv \frac{s' a'_i}{p'} \ (\mathrm{mod}\ 1), \qquad \frac{a'_i}{p'} \equiv \frac{s a_i}{p} \ (\mathrm{mod}\ 1)$$

puisque, quand i varie de 1 à n, ces congruences expriment respectivement que A appartient à $\Lambda(A')$ et que A' appartient à $\Lambda(A)$.

On a alors, pour chaque i, $\frac{a_i}{p}(ss'-1) \equiv 0 \pmod 1$ d'où $(ss'-1)\times \times(a_1, \ldots, a_n) \equiv 0 \pmod p$ et comme le point A est réduit, on a $ss' \equiv 1 \pmod p$ et s est premier avec p. De plus $p'|pa_i'$ donc $p'|p(a_1', \ldots, a_n')$ et, comme le point A' est réduit, $p'|p$. Intervertissant le rôle de p et de p' on voit que $p = p'$. De plus la condition (P') est bien vérifiée.

Inversement si (P') est vérifiée on a, pour chaque i, $\frac{a_i'}{p'} \equiv \frac{sa_i}{p} \pmod 1$ avec $(s, p) = 1$. Si s' est tel que $ss' \equiv 1 \pmod p$, on a, pour chaque i, $\frac{s'a_i'}{p'} \equiv \frac{a_i}{p} \pmod 1$; par suite $\Lambda(A)$ coïncide avec $\Lambda(A')$ et $p = p'$.

La proposition 1 montre qu'il y a correspondance bijective entre les classes de points réduits A par rapport à la relation d'équivalence (P') et les réseaux de $\hat{\mathfrak{L}}$.

Rappelons qu'un réseau est permis pour Ω_n s'il n'a en commun avec Ω_n que l'origine 0. $\mathfrak{L}$ est la famille des réseaux de $\hat{\mathfrak{L}}$ permis pour Ω_n et $\bar{\mathfrak{L}}$ la partie de $\mathfrak{L}$ formée des réseaux n'ayant en commun avec $\bar{\Omega}_n$ que 0 et les sommets $\{\pm e_i\}$.

σ étant une permutation de $[1, n]$ et (ε_i) une suite de n nombres valant ± 1, on associe à tout couple $\varphi = (\sigma, (\varepsilon_i))$ la permutation de $\boldsymbol{R}^n$ définie par

$$x = \sum_{i=1}^{n} x_i e_i \to \varphi(x) = \sum_{i=1}^{n} x_i \varphi(e_i)$$

avec $\varphi(e_i) = \varepsilon_i e_{\sigma(i)}$. On pose pour toute partie H de $\boldsymbol{R}^n$,

$$\varphi(H) = \bigcup_{x \in H} \varphi(x).$$

L'ensemble $\{\pm e_i\}$ et Ω_n sont invariants par toute permutation φ. Il en résulte qu'un réseau Λ appartient à $\mathfrak{R}, \hat{\mathfrak{L}}, \mathfrak{L}, \bar{\mathfrak{L}}$ respectivement si et seulement s'il en est de même pour $\varphi(\Lambda)$ quel que soit φ.

L'ensemble Φ des couples φ considérés ci-dessus est un groupe pour la loi de composition $(\varphi, \varphi') \to \varphi\varphi'$ avec $\varphi\varphi' = (\sigma\sigma', (\varepsilon_i\varepsilon_i'))$ et ce qui précède montre que l'on peut remplacer l'étude des réseaux de $\mathfrak{L}$, resp. $\bar{\mathfrak{L}}$ par l'étude des classes d'intransitivité de $\mathfrak{L}$, resp. $\bar{\mathfrak{L}}$ modulo Φ.

A tout *point* $A = \{p; a_1, \ldots, a_n\}$ on associe $\|A\| = \frac{1}{p}\sum_{i=1}^{n}|r_i|$, r_i étant le reste de valeur absolue minimum du nombre a_i modulo p. On a $\|A\| > 1$, resp. $\|A\| \geqslant 1$, si et seulement si A n'est congru, modulo M, à aucun point de Ω_n, resp. $\bar{\Omega}_n$.

On désigne par S_p le système de restes de valeur absolue minimum modulo p et par Σ_p l'ensemble des entiers s vérifiant les inégalités $0 < 2s \leqslant p$.

On dit qu'un point A est *admis* si, pour tout s de Σ_p, on a $\|sA\| > 1$, *semi-admis* si, pour tout s de Σ_p, on a $\|sA\| \geqslant 1$.

Un point A semi-admis est *semi-admis strictement* si l'on peut trouver s dans Σ_p tel que $\|sA\| = 1$. Un point A semi-admis strictement est un point *frontière* si l'on a $\|A\| = 1$.

Proposition 2. (i) *Tout point semi-admis est réduit.*

(ii) *Le point A est admis, resp. semi-admis si et seulement si $\Lambda(A)$ appartient à $\mathfrak{L}$, resp. $\bar{\mathfrak{L}}$.*

Preuve. (i) Si $\delta = (a_1, \ldots, a_n, p)$ est différent de 1, on a $A = \frac{1}{p}\sum_{i=1}^{n} a_i e_i = \frac{1}{q}\sum_{i=1}^{n} b_i e_i$, où l'on a posé $p = \delta q$, $a_i = \delta b_i$, et $\|qA\| = 0$ avec $2q \leqslant \delta q = p$; par conséquent le point A n'est pas semi-admis. D'ailleurs, en établissant une réciproque, on voit que $\delta \neq 1$ équivaut à l'existence de s dans Σ_p tel que $\|sA\| = 0$.

(ii) On a montré dans [1] que, pour les points A réduits, $\Lambda(A)$ appartient à $\mathfrak{L}$ (resp. $\bar{\mathfrak{L}}$) si et seulement si, pour tout s appartenant à S_p, on a $\|sA\| \geqslant 1$ (resp. $\|sA\| > 1$) d'où le résultat, compte tenu de (i) et en remarquant qu'il suffit d'étendre les conditions d'inégalité portant sur $\|sA\|$ aux s de Σ_p puisque $\|sA\| = \|-sA\|$.

Pour étudier les points $\{p; a_1, \ldots, a_n\}$ conduisant à des réseaux de $\mathfrak{L}$, resp. $\bar{\mathfrak{L}}$, il résulte des considérations précédentes que l'on peut considérer les points modulo les relations d'équivalence obtenues par les opérations suivantes:

(a) Réduire les points modulo M ce qui revient à prendre les a_i dans un système de restes modulo p par exemple S_p;

(b) Associer à chaque point son point réduit en divisant p et les a_i par $(a_1, \ldots, a_n, p)$;

(c) Considérer les points modulo la relation (P');

(d) Considérer les points modulo Φ.

Si l'on se contente d'étudier les points de rang n c'est à dire les points pour lesquels aucun des a_i n'est divisible par p (ce qui est justifié si l'on suppose le problème dejà résolu dans $\boldsymbol{R}^{n-1}$), étudier les points modulo la conjonction de (a) et de (d) revient à étudier les points $\{p; a_1, \ldots, a_n\}$ où les a_i et p sont des entiers vérifiant les inégalités

$$0 < 2a_n \leqslant 2a_{n-1} \leqslant \ldots \leqslant 2a_1 \leqslant p.$$

De plus, on sait que l'on a $p < n!$.

Dans la suite, on désigne par $\bar{\mathscr{A}}$ l'ensemble des points $\{p; a_1, \ldots, a_n\}$ où les a_i et p sont des entiers vérifiant les inégalités $0 < 2a_n \leqslant 2a_{n-1}$

$\leqslant \ldots \leqslant 2a_1 \leqslant p < n!$. $\bar{\mathscr{A}}$, resp. $\mathscr{A}$ est l'ensemble des points de $\hat{\mathscr{A}}$ qui sont admis, resp. semi-admis. D'après la proposition 2 les points de $\mathscr{A}$, resp. $\bar{\mathscr{A}}$ sont réduits et conduisent à des réseaux de $\mathfrak{L}$, resp. $\bar{\mathfrak{L}}$.

On dit que deux points réduits appartiennent au même *cycle* si et seulement s'ils sont équivalents modulo la conjonction de (P′) et de Φ autrement dit les points $A = \{p; a_1, \ldots, a_n\}$ et $A' = \{p'; a'_1, \ldots, a'_n\}$ appartiennent au même cycle si et seulement si l'on peut trouver s premier avec p et $\varphi = (\sigma, (\varepsilon_i))$ dans Φ tels que A' soit congru à $s\varphi(A)$ modulo M (ceci nécessite $p' = p$ on peut supposer que s est dans Σ_p).

On se propose alors de déterminer tous les éléments de $\bar{\mathscr{A}}$ resp. $\mathscr{A}$ ou, ce qui suffit, de déterminer tous les éléments d'une partie $\bar{\mathscr{B}}$ de $\bar{\mathscr{A}}$, resp. $\mathscr{B}$ de $\mathscr{A}$ contenant au moins un représentant de chaque cycle.

Dans la suite, comme on est amené à considérer les familles $\mathfrak{L}$, $\bar{\mathfrak{L}}$, $\mathscr{A}$, $\bar{\mathscr{A}}$, pour des valeurs différentes de l'entier n, on indexe ces familles par l'indice n. On indexe aussi, si nécessaire, les quantités $\|B\|$ associées à un point B de $\boldsymbol{R}^n$.

p_n, resp. $\bar{p}_n$ sont évidemment l'ordre maximum d'un élément de $\mathscr{A}_n$, resp. $\bar{\mathscr{A}}_n$.

Pour $n = 3, 4$ on peut énoncer la

PROPOSITION 3. (i) $p_3 = 4, \bar{p}_3 = 2$; *une liste de points semi-admis, de rang* 3, *contenant un et un seul représentant de chaque cycle des points de* $\mathscr{A}_3$ *est*: $\{2; 1, 1, 1\}$, $\{3; 1, 1, 1\}$, $\{4; 2, 1, 1\}$.

(ii) $p_4 = 16, \bar{p}_4 = 5$; *une liste de points semi-admis, de rang* 4, *contenant un et un seul représentant de chaque cycle des points de* $\mathscr{A}_4$ *est la liste des* 20 *points*:

$\{2; 1, 1, 1, 1\}$,	$\{3; 1, 1, 1, 1\}$,	$\{4; 1, 1, 1, 1\}$,	$\{4; 2, 1, 1, 1\}$,	$\{4; 2, 2, 1, 1\}$,
$\{5; 2, 1, 1, 1\}$,	$\{5; 2, 2, 1, 1\}$,	$\{6; 2, 2, 1, 1\}$,	$\{6; 3, 1, 1, 1\}$,	$\{6; 3, 2, 1, 1\}$,
$\{6; 3, 2, 2, 1\}$,	$\{7; 3, 2, 1, 1\}$,	$\{8; 3, 2, 2, 1\}$,	$\{8; 3, 3, 1, 1\}$,	$\{8; 4, 2, 1, 1\}$,
$\{8; 4, 3, 2, 1\}$,	$\{9; 4, 3, 2, 1\}$,	$\{10; 4, 3, 2, 1\}$,	$\{12; 5, 4. 2, 1\}$,	$\{16; 7, 5, 3, 1\}$.

Preuve. Elle est en substance dans [1]. En particulier, pour $n = 4$, on y a déterminé la liste $\mathscr{B}_4$ des points de $\mathscr{A}_4$ vérifiant les conditions $2 = 2a_4 \leqslant 2a_3 \leqslant 2a_2 \leqslant 2a_1 \leqslant p < 4!$ et montré que $\mathscr{B}_4$ contient un représentant au moins de chaque cycle. $\mathscr{B}_4$ contient les 20 points cités ci-dessus et les 3 points $\{5; 2, 2, 2, 1\}$, $\{7; 3, 2, 2, 1\}$, $\{7; 3, 3, 2, 1\}$; or, il est facile de voir que les points $\{5; 2, 1, 1, 1\}$ et $\{5; 2, 2, 2, 1\}$ de même que les trois points $\{7; 3, 2, 1, 1\}$, $\{7; 3, 2, 2, 1\}$, $\{7; 3, 3, 2, 1\}$ appartiennent à un même cycle tandis que les cycles des autres points de $\mathscr{B}_4$ sont distincts.

Pour déterminer une partie $\mathscr{B}_n$ de $\mathscr{A}_n$ contenant au moins un représentant de chaque cycle on utilise la

PROPOSITION 4. *Tout point* $A' = \{p'; a'_1, \ldots, a'_n\}$ *est* (P)*-équivalent à un point* $A = \{p; a_1, \ldots, a_n\}$ *tel que* $a_n = (a'_n, p)$.

COROLLAIRE. *Si le point* A' *appartient à* $\mathscr{A}_n$, *resp* $\bar{\mathscr{A}}_n$, *on peut trouver dans* $\mathscr{A}_n$, *resp.* $\bar{\mathscr{A}}_n$ *un point* A *du cycle de* A' *tel que* $a_n = \inf_i (a'_i, p)$.

Preuve. D'après la proposition 1, il suffit de montrer que l'on peut trouver s premier avec p tel que le point A soit congru à sA' modulo M et vérifie $a_n = (a'_n, p)$. Cela a lieu s'il est possible de trouver s premier avec p vérifiant la congruence $sa'_n \equiv (a_n, p) \pmod p$ et résulte du

LEMME 1. *Si* m *est un entier positif*, a *un entier quelconque, la congruence*

$$ax \equiv (a, m) \pmod m \tag{1}$$

admet au moins une solution x *telle que* $(x, m) = 1$.

Preuve du lemme. Si l'on pose $(a, m) = d$, $a = da'$, $m = dm'$, la congruence (1) est équivalente à la congruence

$$a'x \equiv 1 \pmod{m'}. \tag{1′}$$

Si x_0 est la solution unique de (1′) prise modulo m', les solutions de (1) prises modulo m sont au nombre de d et de la forme $x_0 + \lambda m'$ où λ parcourt un système complet de restes modulo d. Si $\alpha \neq 1$ divise (x_1, x_2, m) où $x_1 = x_0 + \lambda_1 m'$, $x_2 = x_0 + \lambda_2 m'$ sont deux solutions de (1), on a $\alpha | (\lambda_2 - \lambda_1) m'$; comme $1 = (x_0, m') = (x_1, m')$ entraîne $(\alpha, m') = 1$, on a $\alpha | (\lambda_2 - \lambda_1)$ et par conséquent, parmi les solutions de (1) prises modulo m, il y en a au plus d/α telles que $\alpha | (x, m)$. De plus, un tel α est nécessairement un diviseur de (a, m).

Soit $d = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_l^{\alpha_l}$ où les nombres p_i sont premiers et distincts; les solutions de (1) prises modulo m telles que pour un i on ait $p_i | (x, m)$ et que pour tout $j \neq i$ on ait $p_j \nmid (x, m)$ sont au plus (à vrai dire on peut montrer que le qualificatif au plus peut être supprimé) au nombre de

$$d\left(\sum_i \frac{1}{p_i} - \sum_{i \neq j} \frac{1}{p_i p_j} + \sum_{i \neq j \neq k} \frac{1}{p_i p_j p_k} \ldots\right) = d\left(1 - \prod_i \left(1 - \frac{1}{p_i}\right)\right) = d - \varphi(d)$$

où φ est la fonction d'Euler de l'entier d. Ce nombre étant inférieur à d pour $d \neq 1$, on a bien au moins une solution x pour laquelle $(x, m) = 1$.

Preuve du corollaire. Au point A' associons $A'' = \{p; a''_1, \ldots, a''_n\}$ où les a''_i sont une permutation des a'_i telle que $(a''_n, p) = \inf_i (a'_i, p)$. Au point A'' associons le point $B'' = \{p; b''_1, \ldots, b''_n\}$ (P)-équivalent à A'' et tel que $b''_n = (a''_n, p)$; on peut supposer, de plus, que les b''_i sont dans S_p et il est immédiat que pour tout i de $[1, n]$ on a $(b''_i, p) \geqslant b''_n$. Or le point B'' est Φ-équivalent au point $A = \{p; a_1, \ldots, a_n\}$ de $\mathscr{A}_n$ défini par $a_n = b''_n$ et où les a_j, pour $j = 1, \ldots, n-1$ sont une permutation convenable des $|b''_j|$ $(j = 1, \ldots, n-1)$.

La proposition 4 et son corollaire rendent utile la détermination d'une borne supérieure de $\inf_i (a_i, p)$ pour les points $A = \{p; a_1, \ldots, a_n\}$ de $\mathscr{A}_n$, resp. $\overline{\mathscr{A}}_n$.

Il est évident que $\inf_i (a_i, p) = 1$ si p est premier ou la puissance d'un nombre premier. La preuve de la proposition 3 (ii) passait d'autre part par la remarque que pour les points de $\mathscr{A}_4$, on avait aussi $\inf_i (a_i, p) = 1$.

Un premier résultat est la

PROPOSITION 5. *Pour les points A de $\mathscr{A}_n$, on a $\sup_i (a_i, p) \leqslant p_{n-1}$ et pour les points A de $\overline{\mathscr{A}}_n$, $\sup_i (a_i, p) \leqslant \overline{p}_{n-1}$.*

Preuve. En ce qui concerne les points de $\mathscr{A}_n$, la preuve est dans [1]. Elle est analogue pour les points de $\overline{\mathscr{A}}_n$.

On a aussi la

PROPOSITION 6. (i) *Pour un point A de $\mathscr{A}_n$, on a pour tout $n \geqslant 3$, l'inégalité*

$$(*) \qquad \inf_i (a_i, p) \leqslant \sup\big(p_{n-3}, \inf(p_{n-2}, p_{n-1}-1), p_{n-1}-2\big)$$

et pour tout n, l'inégalité

$$(**) \qquad \inf_i (a_i, p) \leqslant \sup(p_{n-2}, p_{n-1}-n+1).$$

(ii) *Pour un point A de $\tilde{\mathscr{A}}_n$ on a dans des conditions analogues les inégalités ci-dessus dans lesquelles les p_k sont remplacés par $\overline{p}_k$.*

Preuve. (i) Prouvons d'abord $(*)$. A une permutation près, on peut supposer (1) $(a_{n-2}, p) \leqslant (a_{n-1}, p) \leqslant (a_n, p)$ avec $(a_n, p) = \sup_i (a_i, p) \leqslant p_{n-1}$.

Si dans (1) toutes les inégalités sont strictes on a

$$(a_{n-2}, p) \leqslant (a_n, p) - 2 \leqslant p_{n-1} - 2.$$

Si dans (1) il y a une seule égalité $(a_j, p) = (a_{j+1}, p) = r$ alors le point $\frac{p}{r} A$ est congru modulo M au point $\frac{1}{r} \sum_{\substack{i \neq j, j+1 \\ i=1}}^{n} a_i e_i$ qui est réduit d'ordre r et comme ce point doit appartenir au cycle d'un point de $\mathscr{A}_{n-2}$, on a $r \leqslant p_{n-2}$. Comme de façon évidente on a aussi $r \leqslant p_{n-1} - 1$, on a alors

$$(a_{n-2}, p) \leqslant \inf(p_{n-2}, p_{n-1} - 1).$$

Si dans (1) on a deux signes d'égalité alors pour $r = (a_{n-2}, p)$ le point $\frac{p}{r} A$ est congru modulo M au point réduit d'ordre r, $\frac{1}{r} \sum_{i=1}^{n-3} a_i e_i$ qui appartient au cycle d'un point de $\mathscr{A}_{n-3}$ et on a $r \leqslant p_{n-3}$.

Comme pour $n \geqslant 3$ on a $\inf_i (a_i, p) \leqslant (a_{n-2}, p)$ on a bien $(*)$.

Prouvons maintenant $(**)$. Supposons les (a_i, p) ordonnés dans l'ordre croissant. Si toutes les inégalités sont strictes on a bien $(a_1, p) \leqslant p_{n-1} - n + 1$ et si l'on a au moins une égalité $(a_i, p) = (a_{i+1}, p)$ alors $(a_i, p) \leqslant p_{n-2}$ d'où le résultat.

(ii) La preuve se fait de façon analogue.

Notons aussi la

PROPOSITION 7. *Pour tout n on a l'inégalité $\overline{p}_n \geqslant p_{n-1}$.*

Preuve. Soit $A = \{p; a_1, \ldots, a_{n-1}\}$ un point semi-admis de rang $n-1$ et $B = \{p; a_1, \ldots, a_{n-1}, 1\}$. Pour tout s de Σ_p, on a $p\|sB\| = s + p\|sA\|$ et comme on a $\|sA\| \geqslant 1$ on a aussi $\|sB\| \geqslant 1 + s/p > 1$; cela prouve que le point B est admis. Comme on peut prendre $p = p_{n-1}$ cela prouve qu'il existe des points admis de rang n d'ordre p_{n-1}.

2. Considérations pratiques. Le cas $n = 5$. Il est possible compte tenu des résultats du paragraphe 1 d'établir un programme en langage ALGOL permettant de déterminer $\mathscr{A}_n$ ou $\overline{\mathscr{A}}_n$. Pour cela, on fait parcourir à un point A tous les éléments de $\hat{\mathscr{A}}_n$ et pour chaque $A = \{p; a_1, \ldots, a_n\}$ on considère successivement pour $s = 1, \ldots, p \div 2$ la quantité $\|sA\|$. Si l'on a $\|sA\| \geqslant 1$ on considère $\|(s+1)A\|$ après avoir affecté une étiquette significative si $\|sA\| = 1$; si l'on a $\|sA\| < 1$ on élimine le point passant alors au point suivant relativement à l'ordre dont a été muni $\hat{\mathscr{A}}_n$. On détermine ainsi $\mathscr{A}_n$ en distinguant les points admis et les points semi-admis strictement. Pour la détermination directe de $\overline{\mathscr{A}}_n$, on procède de façon analogue en éliminant les cas où l'on a $\|sA\| \leqslant 1$.

Passons sur les détails techniques de rédaction du programme.

Evidemment on peut remplacer $\hat{\mathscr{A}}_n$ par une partie $\hat{\mathscr{B}}_n$ convenable en tenant compte des propositions 4, 5 et 6.

Des essais sur la machine I. B. M. 1620 du Laboratoire de Calcul de l'Université de Lille ont montré que cette méthode demande déjà pour $n = 4$, même si l'on tient compte que dans ce cas on peut prendre pour $\hat{\mathscr{B}}_4$ l'ensemble des $\{p; a_1, a_2, a_3, a_4\}$ vérifiant $2 = 2a_4 \leqslant 2a_3 \leqslant 2a_2 \leqslant 2a_1 \leqslant p \leqslant 23$, un temps de calcul trop long.

Il est donc nécessaire, si possible, de tenir compte de propriétés permettant d'éliminer en bloc des parties de $\mathscr{A}_n$.

On peut pour cela tenir compte de la

PROPOSITION 8. *Pour $t = 0, 1, \ldots, n-1$ le point $A = \frac{1}{p} \sum_{i=1}^{n} a_i e_i$ où les a_i sont entiers strictement positifs et p un entier au moins égal à 3, vérifie s'il est semi-admis les inégalités*

$$p \leqslant p\|A\| \leqslant (n-t-1)(p/2) + 2 \inf_I \Big(\sum_{i \in I} |a_i|\Big)$$

et s'il est admis les inégalités

$$p < p\|A\| < (n-t-1)(p/2) + 2\inf_{I}\Big(\sum_{i\in I}|a_i|\Big)$$

où I décrit les parties à t éléments de $[1, n]$ si $t \neq 0$, $I = \emptyset$ si $t = 0$.

Preuve. Dans le cas des points semi-admis elle est dans [1]. Elle est analogue pour les points admis.

Dans la suite, pour $p < n!$ on désigne par $\hat{\mathscr{A}}_n^p$ l'ensemble des points $\{p; a_1, \dots, a_n\}$ de $\hat{\mathscr{A}}_n$ pour les entiers a_i vérifiant $0 < 2a_n \leq \dots \leq 2a_1 \leq p$. Pour q entier supérieur ou égal à 1, on désigne par $\hat{\mathscr{A}}_{nq}$ resp. $\hat{\mathscr{A}}_{nq}^p$ l'ensemble des éléments de $\hat{\mathscr{A}}_n$ resp. $\hat{\mathscr{A}}_n^p$ pour lesquels $a_n = q$. En particulier, si le point A appartient à $\hat{\mathscr{A}}_{n1}$ le réseau $\Lambda(A)$ a pour base $e_1, \dots, e_{n-1}, A$.

$\mathscr{A}_{nq}$ resp. $\mathscr{A}_{nq}^p$ désigne l'ensemble des éléments de $\hat{\mathscr{A}}_{nq}$ resp. $\hat{\mathscr{A}}_{nq}^p$ qui sont semi-admis; $\mathscr{A}_{nq}$ resp. $\mathscr{A}_{nq}^p$ ensembles de points admis ont une signification analogue.

D'après le corollaire de la proposition 4 tout point de $\mathscr{A}_n$ resp. $\bar{\mathscr{A}}_n$ d'ordre p appartient au même cycle qu'un point de $\mathscr{A}_{nq}$ resp. $\bar{\mathscr{A}}_{nq}$ où q est un diviseur de p. On pourra en conséquence, au lieu de déterminer $\mathscr{A}_n$, déterminer la partie $\bigcup_{q|p} \mathscr{A}_{nq}^p$ et de même déterminer la partie $\bigcup_{q|p} \bar{\mathscr{A}}_{nq}^p$ de $\bar{\mathscr{A}}_n$.

On désigne par p_{nq} resp. $\bar{p}_{nq}$ l'ordre maximum d'un élément de $\bigcup_{q|p} \mathscr{A}_{nq}$ resp. $\bigcup_{q|p} \bar{\mathscr{A}}_{nq}$. On pourra limiter q en tenant compte, par exemple, de la proposition 6.

De toute façon, une première étape consiste à déterminer $\mathscr{A}_{n1}$ et p_{n1}, $\bar{\mathscr{A}}_{n1}$ et $\bar{p}_{n1}$.

On désigne par $\mathscr{F}_n$ l'ensemble des points frontière; on pose $\mathscr{F}_n^p = \mathscr{F}_n \cap \mathscr{A}_n^p$; on désigne par f_n l'ordre maximum d'un point de $\mathscr{F}_n$. On a évidemment $f_n \leq p_n$.

On dit que le nombre p est un indice *possible* relativement à $\mathscr{A}_{nq}$ resp. $\bar{\mathscr{A}}_{nq}$ resp. $\mathscr{F}_n$ si $\mathscr{A}_{nq}^p$ resp. $\bar{\mathscr{A}}_{nq}^p$ resp. $\mathscr{F}_n^p$ est non vide. p_{n1} resp. $\bar{p}_{n1}$ est le maximum des indices possibles pour $\mathscr{A}_{n1}$ resp. $\bar{\mathscr{A}}_{n1}$; p_n, resp. $\bar{p}_n$ resp. f_n est le maximum des indices possibles pour $\bigcup_q \mathscr{A}_{nq}$ resp. $\bigcup_q \bar{\mathscr{A}}_{nq}$ resp. $\mathscr{F}_n$.

Dans la suite on suppose $n = 5$.

PROPOSITION 9. *Pour un point A de $\bar{\mathscr{A}}_5$, on a $\inf_i(a_i, p) = 1$; par conséquent on a $\bar{p}_5 = \bar{p}_{51}$.*

Preuve. Notons que la proposition 6 nous donne $\inf_i(a_i, p) \leq \sup(\bar{p}_3, \bar{p}_4 - 4) = 2$ puisque l'on a $\bar{p}_3 = 2$, $\bar{p}_4 = 5$. Supposons $(a_1, p) \leq (a_2, p) \leq (a_3, p) \leq (a_4, p) \leq (a_5, p)$ ce qui est possible à une permutation près.

On a $(a_5, p) \leq 5$. Si, dans les inégalités (*) $(a_3, p) \leq (a_4, p) \leq (a_5, p)$, il y a au moins un signe d'égalité alors on a $(a_3, p) \leq \bar{p}_3 = 2$ et, ou bien $(a_1, p) = 1$, ou bien $(a_1, p) = (a_2, p) = (a_3, p) = 2$, ce qui est exclu par $\bar{p}_2 = 1$. Si dans (*) les inégalités sont strictes on a $(a_3, p) \leq 3$; (a_2, p) ne peut être égal à 3 car cela ne serait possible qu'avec $(a_2, p) = (a_3, p)$ qui entraîne $(a_2, p) \leq \bar{p}_3$; on a donc $(a_2, p) \leq 2$; si (a_1, p) est différent de 1, on voit que 2 divise au moins trois des (a_i, p) ce qui est exclu par l'égalité $\bar{p}_2 = 1$.

Dans tous les cas on a bien $(a_1, p) = 1$.

On se propose alors

(a) *La détermination d'une liste des p possibles pour $\mathscr{A}_{51}$*, avec pour chaque p possible l'exemple d'un point de $\mathscr{A}_{51}^p$: Cela nous donnera en particulier la valeur de p_{51}.

(b) *La détermination de $\bar{\mathscr{A}}_{51}$.* La proposition 9 montrant que tout point de $\bar{\mathscr{A}}_5$ appartient au même cycle qu'un point de $\mathscr{A}_{51}$, on résoud ainsi complétement le problème des octaèdres pour $n = 5$ dans le cas fermé. On utilise (a) notamment pour borner les p possibles pour $\bar{\mathscr{A}}_{51}$ puisque l'on a $\bar{p}_{51} \leq p_{51}$. Laub [4] ayant déterminé $\bar{\mathscr{A}}_{51}^p$ pour $p \leq 37$, on vérifie ainsi et complète ses résultats.

(c) *La détermination d'une liste des p possibles pour $\mathscr{F}_5$.*

(d) *La détermination de p_5.*

On est amené aussi à utiliser le corollaire de la

PROPOSITION 10. *Pour tout point $A = \{p; a_1, \dots, a_n\}$ de $\mathscr{A}_n$ on a nécessairement, pour $n \geq 4$, l'inégalité $p \leq 16 \sum_{i=4}^{n} a_i$.*

COROLLAIRE. *Pour tout point $A = \{p; a_1, a_2, a_3, a_4, q\}$ de $\mathscr{A}_{5q}^p$, on a nécessairement $a_4 + q - 1 \geq (p-1) \div 16$ et, en particulier $a_4 \geq (p-1) \div 16$ pour tout point A de $\mathscr{A}_{51}^p$.*

Preuve du corollaire. Elle résulte de la remarque que $p \leq 16 \sum_{i=4}^{n} a_i$ équivaut à $p - 1 < 16 \sum_{i=4}^{n} a_i$ donc à $1 + (p-1) \div 16 \leq \sum_{i=4}^{n} a_i$ du fait que les a_i et p sont entiers.

Remarque. Il résulte immédiatement de la proposition 10 que pour un point A de $\mathscr{A}_{41}$ on a $p \leq 16$ et la proposition 10 n'est autre qu'une généralisation du lemme 5 de [1].

Preuve de la proposition 10. Considérons plusieurs cas

(i) Si l'on a $\frac{1}{3}p \geq a_1$ alors $p - 3a_i \geq 0$ pour $i = 1, 2, 3$ et considérant le point $3A$ on a

$$p\|3A\| \leq (p - 3a_1) + (p - 3a_2) + (p - 3a_3) + 3\sum_{i=4}^{n} a_i = 3p - 3p\|A\| + 6\sum_{i=4}^{n} a_i.$$

L'inégalité $p\,\|A\| \geqslant p$ entraîne donc $p\,\|3A\| \leqslant 6\sum_{i=4}^{n} a_i$ et l'inégalité $p\,\|3A\| \geqslant p$ ne peut avoit lieu que pour $p \leqslant 6\sum_{i=4}^{n} a_i$.

(ii) Si l'on a $\frac{1}{3}p \leqslant a_3$ alors $3a_i - p \geqslant 0$ pour $i = 1, 2, 3$ et considérant le point $3A$ on a

$$p\,\|3A\| \leqslant (3a_1 - p) + (3a_2 - p) + (3a_3 - p) + 3\sum_{i=4}^{n} a_i = 3(p\,\|A\| - p).$$

Or la proposition 8 appliquée pour $t = n-3$ nous donne

$$p\,\|A\| \leqslant 2(p/2) + 2\sum_{i=4}^{n} a_i$$

d'où

$$p\,\|A\| - p \leqslant 2\sum_{i=4}^{n} a_i \quad \text{et} \quad p\|3A\| \leqslant 6\sum_{i=4}^{n} a_i.$$

L'inégalité $p\,\|3A\| \geqslant p$ ne peut donc avoir lieu que pour $p \leqslant 6\sum_{i=4}^{n} a_i$.

(iii) Si l'on a $a_3 < \frac{1}{3}p \leqslant a_2$, pour le point $3A$ on a

$$p\,\|3A\| \leqslant (3a_1 - p) + (3a_2 - p) + (p - 3a_3) + 3\sum_{i=4}^{n} a_i = 3p\,\|A\| - 6a_3 - p.$$

Or la proposition 8 appliquée pour $t = n-2$ nous donne

$$p\,\|A\| \leqslant p/2 + 2a_3 + 2\sum_{i=4}^{n} a_i \quad \text{d'où} \quad p\,\|3A\| \leqslant 3(p/2) - p + 6\sum_{i=4}^{n} a_i$$

et l'inégalité $p\,\|3A\| \geqslant p$ ne peut avoir lieu que pour $p \leqslant 12\sum_{i=4}^{n} a_i$.

(iv) Si l'on a $a_2 < \frac{1}{3}p \leqslant a_1$, pour le point $3A$ on a

$$p\,\|3A\| \leqslant (3a_1 - p) + (p - 3a_2) + (p - 3a_3) + 3\sum_{i=4}^{n} a_i$$

$$= 6a_1 + 6\sum_{i=4}^{n} a_i + p - 3p\,\|A\|$$

et l'inégalité $p\,\|A\| \geqslant p$ entraîne

$$p\,\|3A\| \leqslant 6a_1 + 6\sum_{i=4}^{n} a_i - 2p.$$

L'inégalité $p\,\|3A\| \geqslant p$ nécessite alors

$$(*) \qquad a_1 + \sum_{i=4}^{n} a_i \geqslant p/2;$$

appliquons alors la proposition 8 au point $2A - e_1$ pour $t = n-2$ en prenant pour partie à $n-2$ éléments de $[1, n]$ les entiers différents de 2 et 3. On doit avoir

$$p \leqslant p\,\|2A\| \leqslant p/2 + 2\Big((p - 2a_1) + 2\sum_{i=4}^{n} a_i\Big).$$

Or $(*)$ entraîne $p - 2a_1 \leqslant 2\sum_{i=4}^{n} a_i$ et on doit donc avoir $p \leqslant p/2 + 8\sum_{i=4}^{n} a_i$ ce qui ne peut se produire que pour $p \leqslant 16\sum_{i=4}^{n} a_i$.

Pour un point de $\mathscr{A}_n$ on se trouve nécessairement dans l'un des quatre cas considérés ci-dessus ce qui achéve la démonstration.

Le corollaire de la proposition 3 donne une borne inférieure de a_4 pour un point de $\mathscr{A}_{5q}$. Une borne supérieure est donnée par le

Lemme 2. *Pour un point de $\mathscr{A}_{5q}^p$ on a $a_4 < p/3$ pourvu que l'on ait $p > 12q$.*

Preuve. Supposons que pour un point A de $\mathscr{A}_{5q}^p$, on ait $a_4 \geqslant p/3$. On a alors $3a_i - p \geqslant 0$ pour $i = 1, 2, 3, 4$ d'où

$$p\,\|3A\| \leqslant (3a_1 - p) + (3a_2 - p) + (3a_3 - p) + (3a_4 - p) + 3a_5 = 3p\,\|A\| - 4p.$$

Or la proposition 8 appliquée pour $t = 1$ nous donne

$$p\,\|A\| \leqslant 3(p/2) + 2a_5 \quad \text{soit} \quad p\,\|3A\| \leqslant p/2 + 6a_5.$$

L'inégalité $p\,\|3A\| \geqslant p$ n'est alors possible que pour $p/2 \leqslant 6a_5$ soit $p \leqslant 12a_5 = 12q$.

Les divers programmes de calcul que nous avons établis ont utilisé les propositions 8, 9 et 10 et le lemme 2.

Donnons maintenant les résultats.

La détermination des p possibles pour $\mathscr{A}_{51}$ est donnée par le

Théorème 1. *Aucun $p > 48$ n'est possible pour $\mathscr{A}_{51}$. Pour $p \leqslant 48$ toutes les valeurs de $p \geqslant 2$ sont possibles sauf les valeurs 42, 43, 44, 45, 46, et 47. La liste suivante donne pour chaque valeur possible de p un point semi-admis de $\mathscr{A}_{51}^p$. Un tel point est choisi semi-admis strictement quand cela est possible c'est à dire pour les valeurs de p possibles distinctes de 2, 3 et 41; il est choisi point frontière quand cela est possible c'est-à-dire pour les valeurs de p possibles distinctes de 2, 3, 4, 33, 35, 38, 39, 41.*

{2; 1, 1, 1, 1, 1}*, {3; 1, 1, 1, 1, 1}*, {4; 2, 2, 2, 1, 1}*, {5; 1, 1, 1, 1, 1},
{6; 2, 1, 1, 1, 1}, {7; 3, 1, 1, 1, 1}, {8; 4, 1, 1, 1, 1}, {9; 4, 2, 1, 1, 1},
{10; 5, 2, 1, 1, 1}, {11; 5, 3, 1, 1, 1}, {12; 6, 3, 1, 1, 1}, {13; 6, 3, 2, 1, 1},
{14; 7, 3, 2, 1, 1}, {15; 7, 4, 2, 1, 1}, {16; 8, 4, 2, 1, 1}, {17; 7, 5, 3, 1, 1},
{18; 8, 5, 3, 1, 1}, {19; 8, 6, 3, 1, 1}, {20; 9, 6, 3, 1, 1}, {21; 9, 6, 4, 1, 1},
{22; 9, 7, 4, 1, 1}, {23; 10, 7, 4, 1, 1}, {24; 11, 7, 4, 1, 1}, {25; 10, 8, 3, 3, 1}
{26; 11, 8, 5, 1, 1}, {27; 11, 7, 5, 3, 1}, {28; 12, 9, 5, 1, 1}, {29; 13, 7, 5, 3, 1},

{30; 13, 9, 5, 2, 1}, {31; 14, 9, 5, 2, 1}, {32; 14, 10, 6, 1, 1}, {33; 15, 12, 8, 2, 1}*, {34; 15, 10, 6, 2, 1}, {35; 17, 14, 5, 3, 1}*, {36; 16, 11, 6, 2, 1}, {37; 17, 9, 6, 4, 1}, {38; 18, 12, 7, 3, 1}*, {39; 17, 15, 10, 4, 1}*, {40; 18, 12, 7, 2, 1}, {41; 18, 16, 10, 4, 1}*, {48; 23, 13, 7, 4, 1}.

Dans la liste ci-dessus les points marqués de * sont les seuls points qui ne sont pas points frontière. Parmi eux les points {2; 1, 1, 1, 1, 1}, {3; 1, 1, 1, 1, 1} et {41; 18, 16, 10, 4, 1} sont admis, les autres étant semi-admis strictement.

Preuve. On commence par établir à la machine la liste des p possibles pour $2 \leqslant p \leqslant 83$. On obtient les p indiqués ci-dessus. Pour $84 \leqslant p \leqslant 119$, les p pairs différents de 96 ne sont pas possibles car si pour un tel p il existait un point semi-admis $A = \{p; a_1, a_2, a_3, a_4, 1\}$ le point $2A$ serait aussi un point semi-admis d'ordre $p/2$ avec $42 \leqslant p/2 \leqslant 59$ et $p/2 \neq 48$ ce qui est exclu par les résultats déjà obtenus.

Reste alors à vérifier que $p = 96$ et p impair avec $85 \leqslant p \leqslant 119$ ne sont pas des p possibles.

Ce qu'a fait la machine.

La détermination de $\bar{p}_5$ est donnée par le

THÉORÈME 2. *On a $\bar{p}_5 = 41$. Aucun $p \geqslant 42$ n'est possible pour un point de $\bar{\mathscr{A}}_{51}$. Pour $p \leqslant 41$ toutes les valeurs de p sont possibles pour $\bar{\mathscr{A}}_{51}$ sauf 27, 28 et $30 \leqslant p \leqslant 40$. Une liste complète des cycles des points de $\bar{\mathscr{A}}_5$ est la liste des cycles des points*

{2; 1, 1, 1, 1, 1},	{3; 1, 1, 1, 1, 1},	{4; 1, 1, 1, 1, 1},	{4; 2, 1, 1, 1, 1},
{4; 2, 2, 1, 1, 1},	{5; 2, 1, 1, 1, 1},	{5; 2, 2, 1, 1, 1},	{6; 3, 1, 1, 1, 1},
{6; 2, 2, 1, 1, 1},	{6; 3, 2, 1, 1, 1},	{6; 3, 2, 2, 1, 1},	{7; 3, 2, 1, 1, 1},
{7; 3, 3, 1, 1, 1},	{7; 3, 2, 2, 1, 1},	{8; 4, 2, 1, 1, 1},	{8; 3, 3, 1, 1, 1},
{8; 3, 2, 2, 1, 1},	{8; 3, 3, 2, 1, 1},	{8; 4, 3, 2, 1, 1},	{9; 4, 3, 1, 1, 1},
{9; 4, 2, 2, 1, 1},	{9; 4, 3, 2, 1, 1},	{10; 5, 2, 2, 1, 1},	{10; 4, 3, 2, 1, 1},
{10; 5, 3, 2, 1, 1},	{10; 5, 3, 3, 1, 1},	{10; 4, 4, 3, 1, 1},	{10; 5, 4, 3, 2, 1},
{11; 5, 3, 2, 1, 1},	{11; 4, 4, 2, 1, 1},	{11; 5, 4, 2, 1, 1},	{11; 5, 4, 3, 1, 1},
{11; 5, 4, 3, 2, 1},	{12; 5, 4, 2, 1, 1},	{12; 5, 5, 3, 1, 1},	{12; 5, 3, 2, 2, 1},
{12; 5, 4, 3, 2, 1},	{13; 6, 4, 2, 1, 1},	{13; 5, 5, 2, 1, 1},	{13; 6, 4, 3, 1, 1},
{13; 6, 5, 3, 1, 1},	{13; 5, 4, 3, 2, 1},	{14; 6, 4, 3, 1, 1},	{14; 6, 5, 3, 1, 1},
{14; 5, 4, 3, 2, 1},	{15; 7, 5, 3, 1, 1},	{15; 7, 4, 3, 2, 1},	{15; 7, 5, 4, 2, 1},
{16; 7, 5, 3, 1, 1},	{16; 7, 6, 4, 1, 1},	{16; 7, 4, 3, 2, 1},	{16; 6, 5, 3, 2, 1},
{16; 7, 5, 3, 2, 1},	{17; 8, 5, 3, 1, 1},	{17; 8, 6, 4, 1, 1},	{17; 8, 4, 3, 2, 1},
{17; 8, 5, 3, 2, 1},	{17; 7, 6, 3, 2, 1},	{18; 7, 5, 4, 2, 1},	{19; 9, 5, 3, 2, 1},
{19; 8, 7, 3, 2, 1},	{19; 8, 5, 4, 2, 1},	{20; 8, 7, 3, 2, 1},	{20; 9, 8, 5, 2, 1},
{20; 9, 7, 5, 3, 1},	{21; 9, 8, 5, 2, 1},	{22; 9, 6, 5, 2, 1},	{22; 9, 8, 5, 2, 1},
{22; 9, 7, 5, 3, 1},	{23; 10, 7, 4, 2, 1},	{23; 11, 7, 4, 2, 1},	{23; 10, 9, 6, 2, 1},
{24; 11, 7, 5, 3, 1},	{25; 12, 7, 4, 2, 1},	{25; 11, 9, 6, 2, 1},	{26; 12, 8, 5, 3, 1},
{29; 13, 9, 6, 2, 1},	{41; 18, 16, 10, 4, 1}.		

Preuve. La liste ci-dessus, sauf le point d'ordre 41, est due à Laub (cf. [4], p. 50). D'après le théorème 1 et la proposition 9, il suffit de

déterminer $\bar{\mathscr{A}}_{51}^p$ pour $p \leqslant 48$. On range ensuite les points obtenus par cycles.

Notons aussi que les p possibles pour $\mathscr{F}_5$ sont tous les $p \leqslant 48$ distincts de 2, 3, 4, 33, 35, 38 et des p vérifiant $41 \leqslant p \leqslant 47$. On obtient pour chaque valeur de p possible pour $\mathscr{F}_5$ un point frontière d'ordre p en consultant la liste des points frontière incluse dans la liste donnée dans le théorème 1 et en y ajoutant le point frontière {39; 19, 8, 7, 3, 2}.

On aborde maintenant la détermination de p_5.

Comme évidemment on a l'inégalité $p_5 \geqslant p_{51}$ et que l'on a prouvé

$$\bigcup_{48<p<120} \mathscr{A}_{51}^p = \emptyset,$$

il nous suffit de considérer

$$\bigcup_{\substack{48<p<120\\ q>1,\, q\mid p}} \mathscr{A}_{5q}^p.$$

Pour p fixé, $48 < p < 120$, un point $A = \{p; a_1, a_2, a_3, a_4, a_5\}$ de $\mathscr{A}_5^p$ appartient nécessairement au même cycle qu'un point de $\mathscr{A}_{5q}^p$ avec $q = \inf\limits_i(a_i, p)$. En particulier, si pour p fixé on est assuré que l'on a $\inf\limits_i(a_i, p) = 1$ pour un point A de $\mathscr{A}_5^p$, les résultats précédents montrent que $\mathscr{A}_5^p = \emptyset$. Nous dirons d'un tel p que ce n'est pas un p possible.

On a alors le

LEMME 3. *Pour $48 < p < 120$,*

(i) *si p est premier, puissance d'un nombre premier ou produit de deux nombres premiers distincts, p n'est pas possible;*

(ii) *si p est produit de trois nombres premiers r, s, t avec $r \leqslant s \leqslant t$, $t \geqslant 11$, et $rs \neq 6$, 10, p n'est pas possible;*

(iii) 63, 75, 88, 98, 104 *et* 105 *ne sont pas des p possibles.*

Notons que le (i) du lemme montre que les 40 valeurs suivantes de p ne sont pas possibles:

$49 = (7)^2$, $51 = 3 \cdot 17$, 53, $55 = 5 \cdot 11$, $57 = 3 \cdot 19$, $58 = 2 \cdot 29$, 59, 61, $62 = 2 \cdot 31$, $64 = (2)^6$, $65 = 5 \cdot 13$, 67, $69 = 3 \cdot 23$, 71, 73, $74 = 2 \cdot 37$, $77 = 7 \cdot 11$, 79, $81 = (3)^4$, $82 = 2 \cdot 41$, 83, $85 = 5 \cdot 17$, $86 = 2 \cdot 43$, $87 = 3 \cdot 29$, 89, $91 = 7 \cdot 13$, $93 = 3 \cdot 31$, $94 = 2 \cdot 47$, $95 = 5 \cdot 19$, 97, 101, 103, $106 = 2 \cdot 53$, 107, 109, $111 = 3 \cdot 37$, 113, $115 = 5 \cdot 23$, $118 = 2 \cdot 59$, $119 = 7 \cdot 17$.

La partie (ii) du lemme, elle, montre que les 7 valeurs suivantes de p ne sont pas possibles:

$52 = (2)^2 \cdot 13$, $68 = (2)^2 \cdot 17$, $76 = (2)^2 \cdot 19$, $84 = (2)^2 \cdot 21$, $92 = (2)^2 \cdot 23$, $99 = (3)^2 \cdot 11$, $116 = (2)^2 \cdot 29$, $117 = (3)^2 \cdot 13$.

Ainsi en écartant les 54 valeurs de p couvertes par le lemme 3 restent à examiner les 17 valeurs suivantes de p:

50, 54, 56, 60, 66, 70, 72, 78, 80, 90, 96, 100, 102, 108, 110, 112, 114.

Considérant alors individuellement chacune des valeurs de p ci-dessus énumérées on peut pour chaque p donner une borne supérieure du $\inf_i(a_i, p)$ associé à un point A de $\mathscr{A}_5^p$ ce qui permet d'affirmer que seules certaines valeurs de q divisant p ($q \neq 1$) sont à considérer. Nous appelons ces valeurs de q des valeurs possibles. On a alors le

LEMME 4. *Pour $p = 60, 72, 96$ et 108 les seules valeurs possibles de q sont $2, 3$ et 4; pour $p = 90$ les seules valeurs possibles de q sont 2 et 3; pour $p = 80$ et 112 les seules valeurs possibles de q sont 2 et 4; pour $p = 50, 54, 56, 66, 70, 78, 100, 102, 110$ et 114 la seule valeur possible de q est 2.*

Notons la méthode employée pour prouver les lemmes 3 et 4. On associe toujours au point A de $\mathscr{A}_5^p$ considéré le point $A' = \{p; a_1', a_2', a_3', a_4', a_5'\}$ où les a_i' sont une permutation des a_i choisie de façon que l'on ait

$$(a_1', p) \leqslant (a_2', p) \leqslant (a_3', p) \leqslant (a_4', p) \leqslant (a_5', p).$$

D'après l'étude du problème des octaèdres en dimension 4, (a_5', p) doit être inférieur ou égal à $p_4 = 16$ et différent de $11, 13, 14$ ou 15; de plus deux des (a_i', p) ne peuvent être égaux sans être inférieurs ou égaux à $p_3 = 4$, trois des (a_i', p) ne peuvent être égaux sans être inférieurs ou égaux à $p_2 = 2$ et quatre des (a_i', p) ne peuvent être égaux sans être égaux à $p_1 = 1$.

Les preuves des deux lemmes se servent essentiellement de la remarque ci-dessus et de la décomposition explicite en produit de facteurs premiers des p entiers vérifiant $48 < p < 120$, l'examen de cette décomposition permettant pour chaque valeur de p d'aller plus loin que les résultats qu'on peut déduire de la proposition 6.

Nous donnons ci-dessous la preuve du lemme 3, laissant celle du lemme 4 à la patience du lecteur.

Preuve du lemme 3. (i) Si l'on a $p = r^k$ avec r premier et si (a_1', p) est différent de 1, r divise tous les (a_i', p) donc $(a_1, a_2, a_3, a_4, a_5, p)$ ce qui est exclu; si p est produit des deux nombres premiers distincts r et s, $r < s$, on a $s \geqslant 5$ pour $p \neq 6$; (a_i', p) ne peut prendre que les valeurs 1, r ou s et donc $(a_5', p) \leqslant s$; on ne peut avoir $(a_4', p) = (a_5', p) = s$ puisque $s \geqslant 5$ donc nécessairement $(a_4', p) \leqslant r$; on ne peut avoir $(a_1', p) = r$ donc nécessairement $(a_1', p) = 1$.

(ii) On a nécessairement $rs \leqslant 10$ car sinon $rst \geqslant (11)^2 > 120$. Comme l'hypothèse élimine pour (r, s) les couples $(2, 3)$ et $(2, 5)$ on a $r = s = 2$ ou $r = s = 3$; (a_i', p) peut prendre comme valeurs 1, r ou r^2 et on a nécessairement $(a_1', p) = 1$ car sinon r diviserait $(a_1, a_2, a_3, a_4, a_5, p)$.

(iii) On a $63 = (3)^2 \cdot 7$; les valeurs possibles pour (a_i', p) sont $1, 3, 7$ ou 9. On a $(a_5', p) \leqslant 9$; on ne peut avoir $(a_4', p) = 9$ donc $(a_4', p) \leqslant 7$; on ne peut avoir $(a_3', p) = (a_4', p) = 7$ donc $(a_3', p) \leqslant 3$; on ne peut avoir $(a_1', p) = (a_3', p) = 3$ donc $(a_1', p) = 1$.

On a $75 = 3 \cdot (5)^2$; les valeurs possibles pour (a_i', p) sont $1, 3$ ou 5. On a $(a_5', p) \leqslant 5$; on ne peut avoir $(a_4', p) = 5$ donc $(a_4', p) \leqslant 3$; on ne peut avoir $(a_2', p) = 3$ donc $(a_2', p) = 1$.

On a $88 = (2)^3 \cdot 11$ et les valeurs possibles pour (a_i', p) sont $1, 2, (2)^2$ ou $(2)^3$ d'ou $(a_1', p) = 1$.

On a $98 = 2 \cdot (7)^2$; les valeurs possibles pour (a_i', p) sont $1, 2$ ou 7; on en déduit $(a_4', p) \leqslant 2$ et $(a_1', p) = 1$.

On a $104 = (2)^3 \cdot 13$ et les valeurs possibles pour (a_i', p) sont $1, 2, (2)^2$ ou $(2)^3$ d'où $(a_1', p) = 1$.

On a $105 = 3 \cdot 5 \cdot 7$; les valeurs possibles pour (a_i', p) sont $1, 3, 5$ ou 7. On a $(a_5', p) \leqslant 7$ puis $(a_4', p) \leqslant 5$ puis $(a_3', p) \leqslant 3$ et $(a_1', p) \leqslant 1$.

Indiquons maintenant le résultat final.

Les calculs fondés sur les considérations précédentes montrent que $\bigcup_{\substack{48<p<120 \\ q>1, q|p}} \mathscr{A}_{5q}^p$ est vide. On peut donc énoncer le

THÉORÈME 3. *On a $p_{51} = p_5 = 48$, $\overline{p}_5 = \overline{p}_{51} = 41$.*

Notons que le temps de calcul pour vérifier qu'aucun point d'ordre supérieur à 48 ne peut appartenir à un réseau contenant les sommets de Ω_5 et permis pour Ω_5 est bien plus important que celui nécessaire à la détermination des points semi-admis d'ordre inférieur ou égal à 48.

Nous n'avons pas cru devoir surcharger ce texte d'une liste de tous les cycles des points de $\mathscr{A}_5$.

Remarque. 1. Pour évaluer le temps que demandent les calculs à la machine, il est utile de connaître le nombre d'éléments $\Phi(n)$, resp. $\Psi(n)$ de $\hat{\mathscr{A}}_n$, resp. $\hat{\mathscr{A}}_{n1}$. On trouve

$$\Phi(n) = \frac{2}{(n+1)!} \prod_{i=-1}^{n} \left(\frac{n!}{2} + i\right), \qquad \Psi(n) = \frac{2}{n!} \prod_{i=-1}^{n-1} \left(\frac{n!}{2} + i\right).$$

Les quotients $\Psi(6)/\Psi(5)$ et $\Phi(6)/\Phi(5)$ sont de l'ordre de plusieurs millions ce qui exclut toute possibilité de determination complète du cas $n = 6$ à l'aide des moyens techniques existant actuellement.

2. Les résultats obtenus pour $n = 3, 4, 5$ montrent que pour ces valeurs de n, $n! - 1$ est une borne supérieure de p_n qui n'est pas très bonne. La détermination éventuelle de p_n pour $n \geqslant 6$ serait facilitée si l'on pouvait trouver une borne supérieure meilleure. Comme on a prouvé dans [2] que l'on a $m_n \leqslant \eta(\Omega_n) n!$ où $\eta(\Omega_n)$ est la densité d'empilement régulier de Ω_n, il suffirait pour cela de donner de $\eta(\Omega_n)$ une borne supérieure meilleure que 1. Les seuls résultats de cette nature que l'on connaisse dus à Blichfeldt [3] et à Rankin [7] ne sont valables que pour n suffisamment grand.

Travaux cités

[1] R. Bantegnie, *A propos d'un problème de Mordell sur les octaèdres latticiels*, J. London Math. Soc. 37 (1962), p. 320-328.

[2] — *Sur l'indice de certains réseaux de R^4 permis pour un octaèdre*, Can. J. Math. 17 (1965), p. 725-730.

[3] H. F. Blichfeldt, *A new upper bound to the minimum value of the sum of linear homogeneous forms*, Mh. Math. 43 (1936), p. 410-414.

[4] J. Laub, *Über Punktgitter*, Veroff. Math. Inst. T. H. Braunsweig (1946), 51 p.

[5] H. Minkowski, *Diophantische Approximationen*, Leipzig (1907).

[6] L. J. Mordell, *Lattice Octahedra*, Can. J. Math. 12 (1960), p. 297-302.

[7] R. A. Rankin, *On sums of powers of linear forms III*, Proc. Kon. Ned. Akad. Wet. 51 (1948), p. 846-853.

[8] K. H. Wolff, *Über kritische Gitter im vierdimensionalen Raum*, Mh. Math. 58 (1954), p. 38-56.

Reçu par la Rédaction le 6. 6. 1967

ACTA ARITHMETICA
XIV (1968)

Extensions of a theorem of Hardy

by

B. Berlowitz (Berkeley, Cal.)

The functional equation for the Riemann zeta function may be written, setting

$$f(s) = \pi^{-\frac{1}{2}s}\Gamma(\tfrac{1}{2}s)\zeta(s), \quad \text{as} \quad f(s) = f(1-s).$$

Since the functions defining $f(s)$ are real on the real axis, by the Schwartz reflection principle, $f(s)$ assumes complex conjugate values at complex conjugate points; this together with the functional equation shows that $f(s)$ is real valued on the critical line $\sigma = \frac{1}{2}$. Hardy has shown in [1] that the real valued function $f(\frac{1}{2}+it)$ vanishes infinitely often as $t\to\infty$, and significant quantitative results have been obtained, first by Hardy-Littlewood [2] and then by A. Selberg [4]. These zeros of $f(\frac{1}{2}+it)$ must of course be zeros of $\zeta(s)$.

The purpose of this paper is to show, by simple extensions of ideas of Hardy and Ramanujan, that given any real λ, $0<\lambda<1$, the real and imaginary parts of $f(\lambda+it)$ vanish infinitely often as $t\to\infty$. This is very far from determining whether or not $f(s)$ itself ever vanishes on any $\sigma=\lambda$, $\lambda\neq\frac{1}{2}$.

1. We begin by writing, for $0<\lambda<1$,

$$\mathrm{Re} f(\lambda+it) = \tfrac{1}{2}[f(\lambda+it)+f(\lambda-it)]$$

since $f(s)$ assumes complex conjugate values at complex conjugate points. It is clear from this relation that $\mathrm{Re} f(\lambda+it)$ is an even function of t. Using the functional equation, $f(\lambda-it) = f(1-\lambda+it)$, we obtain

$$\mathrm{Re} f(\lambda+it) = \tfrac{1}{2}[f(\lambda+it)+f(1-\lambda+it)].$$

Consider the function, for, say, positive real x,

$$\Psi_\lambda(x) = \int_0^\infty \mathrm{Re} f(\lambda+it)\cos xt\,dt.$$

Since $\cos xt$ is also an even function of t, we may write

$$\Psi_\lambda(x) = \tfrac{1}{2}\int_{-\infty}^{\infty} \mathrm{Re} f(\lambda+it)\cos xt\,dt = \tfrac{1}{2}\int_{-\infty}^{\infty} \mathrm{Re} f(\lambda+it)\,y^{it}\,dt$$