[13] I. M. Vinogradov, *Some theorems concerning the theory of primes*, Recueil Mathématique 2 (44), 2 (1937), pp. 179–195.
[14] — *The method of trigonometrical sums in the theory of numbers*, translated from the Russian, revised and annotated by K. F. Roth and A. Davenport, Interscience Publishers, 1954.

THE DEPARTMENT OF PURE MATHEMATICS
SHEFFIELD UNIVERSITY, Great Britain

Received on 30.3.1971 (149)

ACTA ARITHMETICA
XXII (1972)

Sur les systèmes complets de restes modulo les idéaux d'un corps de nombres

par

D. Barsky (Paris)

Monsieur Schinzel a posé la question suivante: soient K un corps de nombres, A son anneau des entiers, existe-t-il une suite d'entiers de K $a_0, a_1, \ldots$ telle que $a_0, a_1, \ldots, a_{N(\boldsymbol{m})-1}$ forment un système complet de restes modulo $\boldsymbol{m}$ pour tout idéal entier $\boldsymbol{m}$ de A de norme $N(\boldsymbol{m})$? (cf. [4]).

Nous allons montrer que la réponse est négative si $K \neq Q$.

Notations: K désigne un corps de nombres, A est son anneau des entiers; on désigne par $\boldsymbol{m}$ un idéal entier de A de norme m. On désigne par $v_{\boldsymbol{m}}(x)$ l'exposant de la plus grande puissance de $\boldsymbol{m}$ qui divise l'idéal (x) engendré par x (x est un élément de A), $v_m(n)$ est l'exposant de la plus haute puissance de m qui divise l'entier naturel n (si $\boldsymbol{m}$ est premier $v_{\boldsymbol{m}}(x)$ est la valuation $\boldsymbol{m}$-adique de x, si m est un nombre premier $v_m(n)$ est la valuation m-adique de n). Si a et b sont des entiers naturels $[a/b]$ désigne la partie entière de a/b, c'est-à-dire que $[a/b]$ est un entier tel que: $[a/b] \leqslant a/b < [a/b]+1$. $\boldsymbol{N}$ désigne l'ensemble des entiers naturels.

Définition. On dira qu'une suite d'entiers $a_0, a_1, \ldots$ d'un corps de nombres $K \neq Q$ *possède la propriété* P pour les idéaux $\boldsymbol{m}'$ et $\boldsymbol{m}''$ de même norme m si $a_0, a_1, \ldots, a_{m^h-1}$ forment un système complet de restes modulo $\boldsymbol{m}'^r \boldsymbol{m}''^s$ pour tout couple d'entiers positifs ou nuls r et s tels que $r+s = h$.

Il est clair que si une suite $a_0, a_1, \ldots$ possède la propriété P, elle est injective.

Proposition 1. *Soit $a_0, a_1, \ldots$ une suite d'entiers d'un corps de nombres $K \neq Q$ possédant la propriété* P *pour deux idéaux premiers distincts $\boldsymbol{m}'$ et $\boldsymbol{m}''$ de même norme m. Alors, étant données deux applications non décroissantes u et t de $\boldsymbol{N}$ dans $\boldsymbol{N}$, telles que $u+t = w$ soit une application strictement croissante de $\boldsymbol{N}$ dans $\boldsymbol{N}$ et que $u(0) = t(0) = 0$, on peut définir une injection g de $\boldsymbol{N}$ dans $\boldsymbol{N}$ telle que si l'on pose $b_i = a_{g(i)}$ on ait:*

1° $m^h \leqslant i < m^{h+1} \Leftrightarrow m^{w(h)} \leqslant g(i) < m^{w(h)+1}$;

2° $v_{\boldsymbol{m}'}(b_i - b_j) \geqslant u(v_m(i-j))$ *et* $v_{\boldsymbol{m}''}(b_i - b_j) \geqslant t(v_m(i-j))$, $i \neq j$;

3° *Si u (resp. t) est strictement croissante alors on a:*

$$v_{\boldsymbol{m}'}(b_i - b_j) = u(v_m(i-j)) \quad (\text{resp. } v_{\boldsymbol{m}''}(b_i - b_j) = t(v_m(i-j))), \quad i \neq j.$$

Nous allons construire la suite $b_0, b_1, \ldots$ par récurrence sur h. Remarquons tout d'abord que $w(h) \geqslant h$ car w est une application strictement croissante de N dans N.

Posons $b_0 = a_0, b_1 = a_1, \ldots, b_{m-1} = a_{m-1}$. Comme $a_0, a_1, \ldots, a_{m-1}$ forment un système complet de restes modulo $\boldsymbol{m}'$ et modulo $\boldsymbol{m}''$ on a bien:

$$v_{\boldsymbol{m}'}(b_i - b_j) = u(v_m(i-j)) = u(0) = 0, \qquad v_{\boldsymbol{m}''}(b_i - b_j) = t(v_m(i-j)) = t(0) = 0.$$

Supposons que l'on ait construit la suite $i \to b_i$ satisfaisant à 1° et 2° jusqu'à l'indice $m^h - 1$, montrons que l'on peut alors la construire jusqu'à l'indice $m^{h+1} - 1$.

$a_0, a_1, \ldots, a_{m^{w(h)+1}-1}$ forment un système complet de restes modulo $\boldsymbol{m}'^{u(h)}\boldsymbol{m}''^{t(h)+1}$ par hypothèse, ils peuvent se ranger en m systèmes complets de restes modulo $\boldsymbol{m}'^{u(h)}\boldsymbol{m}''^{t(h)}$ car on a un homomorphisme surjectif d'anneau, évident, de $A/\boldsymbol{m}'^{u(h)}\boldsymbol{m}''^{t(h)+1}$ sur $A/\boldsymbol{m}'^{u(h)}\boldsymbol{m}''^{t(h)}$. Or, par hypothèse $a_0, a_1, \ldots, a_{m^{w(h)}-1}$ forment un système complet de restes modulo $\boldsymbol{m}'^{u(h)}\boldsymbol{m}''^{t(h)}$, donc les $m-1$ systèmes complets de restes modulo $\boldsymbol{m}'^{u(h)}\boldsymbol{m}''^{t(h)}$ restants se trouvent dans la suite $a_{m^{w(h)}}, \ldots, a_{m^{w(h)+1}-1}$. Appelons $S_1, S_2, \ldots, S_{m-1}$ les $m-1$ systèmes complets de restes modulo $\boldsymbol{m}'^{u(h)}\boldsymbol{m}''^{t(h)}$ qui se trouvent dans la suite $a_{m^{w(h)}}, \ldots, a_{m^{w(h)+1}-1}$. Ecrivons pour $m^h \leqslant i < m^{h+1}$, $i = km^h + r$ avec $1 \leqslant k < m$ et $0 \leqslant r < m^h$, et choisissons b_i dans S_k de telle sorte que $b_i \equiv b_r \bmod \boldsymbol{m}'^{u(h)}\boldsymbol{m}''^{t(h)}$. Ce choix est toujours possible car S_k est un système complet de restes modulo $\boldsymbol{m}'^{u(h)}\boldsymbol{m}''^{t(h)}$. Ceci implique d'ailleurs que

$$v_{\boldsymbol{m}'}(b_i - b_r) = u(v_m(i-r)) = u(h) \quad \text{et} \quad v_{\boldsymbol{m}''}(b_i - b_r) = t(v_m(i-r)) = t(h),$$

en effet: b_i et b_r sont choisis dans $a_0, a_1, \ldots, a_{m^{w(h)+1}-1}$ qui forment un système complet de restes modulo $\boldsymbol{m}'^{u(h)}\boldsymbol{m}''^{t(h)+1}$ et modulo $\boldsymbol{m}'^{u(h)+1}\boldsymbol{m}''^{t(h)}$ d'après la propriété P et par conséquent $b_i \not\equiv b_r \bmod \boldsymbol{m}'^{u(h)}\boldsymbol{m}''^{t(h)+1}$ et $\bmod\, \boldsymbol{m}'^{u(h)+1}\boldsymbol{m}''^{t(h)}$ d'où les égalités annoncées. On voit facilement par récurrence que les b_i obtenus sont distincts car les S_k le sont puisque la suite $i \to a_i$ est injective.

Montrons que la suite $b_0, b_1, \ldots, b_{m^{h+1}-1}$ ainsi construite vérifie les relations 1° et 2°.

Elle vérifie 1°:

Si $0 \leqslant i < m^h$, c'est l'hypothèse de récurrence.

Si $m^h \leqslant i < m^{h+1}$, alors par construction $m^{w(h)} \leqslant g(i) < m^{w(h)+1}$.

Elle vérifie 2°:

Si $0 \leqslant i < j < m^h$, c'est l'hypothèse de récurrence.

Si $m^h \leqslant i < j < m^{h+1}$, on écrit $i = km^h + r$, $j = k'm^h + s$ avec $1 \leqslant k, k' < m$ et $0 \leqslant r, s < m^h$. Par construction

$$v_{\boldsymbol{m}'}(b_i - b_r) = v_{\boldsymbol{m}'}(b_j - b_s) = u(h) \quad \text{et} \quad v_{\boldsymbol{m}''}(b_i - b_r) = v_{\boldsymbol{m}''}(b_j - b_s) = t(h).$$

On a

$$v_{\boldsymbol{m}'}(b_i - b_j) = v_{\boldsymbol{m}'}(b_i - b_r + b_r - b_s + b_s - b_j) \quad \text{et}$$
$$v_{\boldsymbol{m}''}(b_i - b_j) = v_{\boldsymbol{m}''}(b_i - b_r + b_r - b_s + b_s - b_j).$$

Si $r = s$ alors

$$v_{\boldsymbol{m}'}(b_i - b_j) = u(v_m(i-j)) = u(h) \quad \text{et} \quad v_{\boldsymbol{m}''}(b_i - b_j) = t(v_m(i-j)) = t(h),$$

en effet: d'après l'inégalité ultra-métrique on a

$$v_{\boldsymbol{m}'}(b_i - b_j) \geqslant u(h) \quad \text{et} \quad v_{\boldsymbol{m}''}(b_i - b_j) \geqslant t(h),$$

et comme par construction b_i et b_j sont choisis dans $a_0, a_1, \ldots, a_{m^{w(h)+1}-1}$,

$$b_i \not\equiv b_j \bmod \boldsymbol{m}'^{u(h)+1}\boldsymbol{m}''^{t(h)} \quad \text{et} \quad \bmod \boldsymbol{m}'^{u(h)}\boldsymbol{m}''^{t(h)+1};$$

on a donc bien les égalités annoncées. Si $r \neq s$,

$$v_{\boldsymbol{m}'}(b_r - b_s) \geqslant u(v_m(r-s)) \quad \text{et} \quad v_{\boldsymbol{m}''}(b_r - b_s) \geqslant t(v_m(r-s))$$

d'après l'hypothèse de récurrence,

$$u(v_m(r-s)) \leqslant u(h-1) \leqslant u(h) \quad \text{et} \quad t(v_m(r-s)) \leqslant t(h-1) \leqslant t(h)$$

d'après l'hypothèse faite sur u et t. Or

$$v_{\boldsymbol{m}'}(b_i - b_j) \geqslant \operatorname{Inf}(v_{\boldsymbol{m}'}(b_r - b_s), u(h)), \quad \text{si} \quad v_{\boldsymbol{m}'}(b_r - b_s) \geqslant u(h)$$

alors

$$v_{\boldsymbol{m}'}(b_i - b_j) \geqslant u(h) \geqslant u(v_m(r-s)) = u(v_m(i-j)), \quad \text{si} \quad v_{\boldsymbol{m}'}(b_r - b_s) < u(h)$$

alors

$$v_{\boldsymbol{m}'}(b_i - b_j) = v_{\boldsymbol{m}'}(b_r - b_s) \geqslant u(v_m(r-s)) = u(v_m(i-j)),$$

donc dans tous les cas on a bien

$$v_{\boldsymbol{m}'}(b_i - b_j) \geqslant u(v_m(i-j)),$$

on montrerait de même que l'on a

$$v_{\boldsymbol{m}''}(b_i - b_j) \geqslant t(v_m(i-j)).$$

Les relations 2° sont vérifiées dans ce cas aussi.

Si $0 \leqslant j < m^h \leqslant i < m^{h+1}$, on écrit $i = km^h + r$ avec $1 \leqslant k < m$ et $0 \leqslant r < m^h$. Par construction on a

$$v_{m'}(b_i - b_r) = u\big(v_m(i-r)\big) \quad \text{et} \quad v_{m''}(b_i - b_r) = t\big(v_m(i-r)\big).$$

Si $r = j$ les relations 2° sont vérifiées. Si $r \neq j$ on écrit

$$v_{m'}(b_i - b_j) = v_{m'}(b_i - b_r + b_r - b_j) \quad \text{et} \quad v_{m''}(b_i - b_j) = v_{m''}(b_i - b_r + b_r - b_j).$$

On a donc

$$v_{m'}(b_i - b_j) \geqslant \operatorname{Inf}\big(v_{m'}(b_r - b_j),\, u(h)\big)$$

on conclut comme si dessus et on a donc $v_{m'}(b_i - b_j) \geqslant u\big(v_m(i-j)\big)$ et de même $v_{m''}(b_i - b_j) \geqslant t\big(v_m(i-j)\big)$. Les relations 2° sont vérifiées dans ce cas aussi.

Les relations 1° et 2° sont vérifiées dans tous les cas.

Supposons que u soit strictement croissante et montrons que dans ce cas la relation 3° est vérifiée. Raisonnons par récurrence comme pour la démonstration de la relation 2°.

Si $0 \leqslant i < j < m^h$, la relation 3° est vraie d'après l'hypothèse de récurrence.

Si $m^h \leqslant i < j < m^{h+1}$, on écrit $i = km^h + r$ et $j = k'm^h + s$ avec $1 \leqslant k, k' < m$ et $0 \leqslant r, s < m^h$. Si $r = s$ on a, pour la même raison que ci dessus,

$$v_{m'}(b_i - b_j) = u\big(v_m(i-j)\big) = u(h)$$

et la relation 3° est vérifiée. Si $r \neq s$,

$$v_{m'}(b_i - b_j) = v_{m'}(b_i - b_r + b_r - b_s + b_s - b_j),$$

par construction on a

$$v_{m'}(b_i - b_r) = v_{m'}(b_j - b_s) = u(h),$$

et d'après l'hypothèse de récurrence et la croissance stricte de u on a

$$v_{m'}(b_r - b_s) = u\big(v_m(r-s)\big) \leqslant u(h-1) < u(h).$$

Par conséquent

$$v_{m'}(b_i - b_j) = v_{m'}(b_r - b_s) = u\big(v_m(r-s)\big) = u\big(v_m(i-j)\big).$$

La relation 3° est démontrée dans ce cas.

Si $0 \leqslant j < m^h \leqslant i < m^{h+1}$ on montre encore par un raisonnement analogue au précédent que l'on a $v_{m'}(b_i - b_j) = u\big(v_m(i-j)\big)$.

La proposition 1 est démontrée.

Corollaire 1. *Etant donnée une suite $a_0, a_1, \ldots$ d'entiers d'un corps de nombres $K \neq Q$ possédant la propriété* P *pour deux idéaux premiers distincts* $\boldsymbol{m}'$ *et* $\boldsymbol{m}''$ *de même norme m, on peut trouver une bijection g de* $\boldsymbol{N}$ *dans* $\boldsymbol{N}$ *telle que si l'on pose $b_i = a_{g(i)}$ on ait:*

1° $m^h \leqslant i < m^{h+1} \Leftrightarrow m^h \leqslant g(i) < m^{h+1}$,

2° $v_{m'}(b_i - b_j) \geqslant \big[\big(v_m(i-j)\big)/2\big]$ *et* $v_{m''}(b_i - b_j) \geqslant \big[\big(v_m(i-j)\big)/2\big]$.

On applique la proposition 1 avec $u(h) = [h/2]$, $t(h) = h - [h/2]$ et $w(h) = h$. On en déduit qu'il existe une injection g de $\boldsymbol{N}$ dans $\boldsymbol{N}$ telle que:

1° $m^h \leqslant i < m^{h+1} \Rightarrow m^h \leqslant g(i) < m^{h+1}$,

2° $v_{m'}(b_i - b_j) \geqslant \big[\big(v_m(i-j)\big)/2\big]$ et

$$v_{m''}(b_i - b_j) \geqslant v_m(i-j) - \big[\big(v_m(i-j)\big)/2\big] \geqslant \big[\big(v_m(i-j)\big)/2\big].$$

Il est clair que l'injection g est en fait une bijection car la restriction de g à l'intervalle $m^h \leqslant i < m^{h+1}$ est une bijection comme le montre la relation 1°.

Le corollaire 1 est démontré.

Corollaire 2. *Etant donnée une suite d'entiers $a_0, a_1, \ldots$ d'un corps de nombres $K \neq Q$ possédant la propriété* P *pour deux idéaux premiers distincts* $\boldsymbol{m}'$ *et* $\boldsymbol{m}''$ *de même norme m, on peut trouver une injection g de N dans N telle que si l'on pose $c_i = a_{g(i)}$ on ait:*

1° $m^h \leqslant i < m^{h+1} \Leftrightarrow m^{2h} \leqslant g(i) < m^{2h+1}$,

2° $v_{m'}(c_i - c_j) = v_{m''}(c_i - c_j) = v_m(i-j)$.

On applique la proposition 1 avec $u(h) = t(h) = h$ et $w(h) = 2h$ qui sont strictement croissantes et le corollaire 2 est démontré.

On note A' (resp. A''), A muni de la topologie $\boldsymbol{m}'$-adique (resp. $\boldsymbol{m}''$-adique). $\hat{A}'$ (resp. $\hat{A}''$) désigne le complété de A pour la topologie $\boldsymbol{m}'$-adique (resp. $\boldsymbol{m}''$-adique). Si B est un sous-ensemble de A, on note B' (resp. B'', resp. $\hat{B}'$, resp. $\hat{B}''$) B muni de la topologie $\boldsymbol{m}'$-adique (resp. $\boldsymbol{m}''$-adique, resp. l'adhérence de B' dans $\hat{A}'$, resp. l'adhérence de B'' dans $\hat{A}''$). On appelle E le sous-ensemble de A constituté par la suite $b_0, b_1, \ldots$ définie au corollaire 1, on appelle E_1 le sous ensemble de A constitué par la suite $c_0, c_1, \ldots$ définie au corollaire 2. Il est clair que l'on a $\hat{E}' = \hat{E}_1' = \hat{A}'$ et $\hat{E}'' = \hat{E}_1'' = \hat{A}''$ (cf. [1]).

On définit une application e' de E' dans E_1' (resp. e'' de E'' dans E_1'') en posant $e'(b_i) = c_i$ (resp. $e''(b_i) = c_i$). Il est clair que e' et e'' sont des bijections car les suites $i \to b_i$ et $i \to c_i$ sont injectives. On pose $f' = e'^{-1}$ et $f'' = e''^{-1}$.

Proposition 2. (a) *L'application f' (resp. f'') est une application uniformément continue de E_1' dans E' (resp. de E_1'' dans E'').*

(b) *L'application e' (resp. e'') est une application continue de E' dans E_1' (resp. de E'' dans E_1'').*

Le (a) est évident car on a

$$v_{m'}(b_i - b_j) \geqslant \big[\big(v_m(i-j)\big)/2\big] = \big[\big(v_{m'}(c_i - c_j)\big)/2\big]$$

et

$$v_{m''}(b_i - b_j) \geqslant \big[\big(v_m(i-j)\big)/2\big] = \big[\big(v_{m''}(c_i - c_j)\big)/2\big].$$

Démontrons le (b). f' est une application uniformément continue de E'_1 dans E', elle se prolonge en une application uniformément continue de $\hat{A}'$ dans $\hat{A}'$ que l'on note $\hat{f}'$. Comme $\hat{A}'$ est compact $\hat{f}'$ est une application fermée de $\hat{A}'$ dans $\hat{A}'$. Donc l'image par $\hat{f}'$ d'un fermé de $\hat{A}'$ est un fermé de $\hat{A}'$, comme les fermés de E'_1 (resp. E') sont l'intersection des fermés de $\hat{A}'$, avec E'_1 (resp. E'), on en déduit immédiatement que $e' = f'^{-1}$ est une application continue de E' dans E'_1.

On appelle i l'application de E' dans E'' définie par $i(b_k) = b_k$ et j l'application de E'_1 dans E''_1 définie par $j(c_k) = c_k$.

Proposition 3. (a) *L'application i est une application continue de E' dans E''.*

(b) *L'application i se prolonge de manière unique en une application continue de $\hat{A}'$ dans $\hat{A}''$.*

L'application j est une application uniformément continue de E'_1 dans E''_1 car

$$v_{\boldsymbol{m}'}(c_i - c_j) = v_{\boldsymbol{m}''}(c_i - c_j) = v_m(i-j).$$

Elle se prolonge donc de manière unique en une application continue (en fait uniformément continue) de $\hat{A}'$ dans $\hat{A}''$, on note $\hat{j}$ ce prolongement. Comme

$$i = f'' \circ j \circ e', \quad E' \xrightarrow[e']{} E'_1 \xrightarrow[j]{} E''_1 \xrightarrow[f'']{} E'',$$

on en déduit que i est une application continue de E' dans E''. Le (a) est démontré.

i est un prolongement continu de j. En effet $E'_1 \subset E' \subset \hat{A}'$ et sur E'_1 on a $i(c_k) = j(c_k) = c_k$ parce que $c_k = b_{g(k)}$, où g est une injection de N dans N, et $i(c_k) = i(b_{g(k)}) = b_{g(k)} = c_k$. Donc sur E' i coïncide avec $\hat{j}$, donc i peut se prolonger en une application continue de $\hat{A}'$ dans $\hat{A}''$: il suffit de prendre $\hat{j}$ comme prolongement. L'unicité relève des théorèmes généraux sur le prolongement des fonctions continues car $\hat{E}' = \hat{E}'_1 = \hat{A}'$. Le (b) est démontré.

On notera encore i le prolongement de i à A'. On a montré que i est une application uniformément continue de A' dans A''.

Théorème 1. *Dans aucun corps de nombres $K \neq Q$ il n'existe de suite $a_0, a_1, \ldots$ d'entiers possédant la propriété P pour deux idéaux premiers distincts $\boldsymbol{m}'$ et $\boldsymbol{m}''$ de même norme m.*

S'il existait une telle suite dans un corps de nombres $K \neq Q$, le corollaire 1 de la proposition 1 et la proposition 3 montrent que, si l'on appelle E l'ensemble $a_0, a_1, \ldots$, l'application identique de E que l'on appelle i est une application continue de E' dans E'' qui se prolonge de manière unique en une application continue de $\hat{A}'$, dans $\hat{A}''$ que l'on appelle encore i.

Calculons $i(x)$ pour un élément $x \in A'$. E possède la propriété suivante $a_0, a_1, \ldots, a_{m^{2h}-1}$ est un système complet de restes modulo $\boldsymbol{m}'^h \boldsymbol{m}''^h$ pour tout entier $h \geqslant 0$. On peut associer à tout élément $x \in A$ une suite $h \to a_{i_h}$ extraite de la suite $a_0, a_1, \ldots$ telle que

$$v_{\boldsymbol{m}'}(x - a_{i_h}) \geqslant h \quad \text{et} \quad v_{\boldsymbol{m}''}(x - a_{i_h}) \geqslant h.$$

En effet il suffit de choisir a_{i_h} dans $a_0, a_1, \ldots, a_{m^{2h}-1}$ de telle sorte que $x \equiv a_{i_h} \bmod \boldsymbol{m}'^h \boldsymbol{m}''^h$, ce choix est toujours possible et il est unique car $a_0, a_1, \ldots, a_{m^{2h}-1}$ est un système complet de restes modulo $\boldsymbol{m}'^h \boldsymbol{m}''^h$. On notera $\lim_{h\to\infty} {}_{\boldsymbol{m}'}(a_{i_h})$ (resp. $\lim_{h\to\infty} {}_{\boldsymbol{m}''}(a_{i_h})$) la limite de la suite $h \to a_{i_h}$ pour la topologie $\boldsymbol{m}'$-adique (resp. $\boldsymbol{m}''$-adique). On a donc $\lim_{h\to\infty} {}_{\boldsymbol{m}'}(a_{i_h}) = \lim_{h\to\infty} {}_{\boldsymbol{m}''}(a_{i_h}) = x$. Comme i est une application continue de A' dans A'' on a:

$$i(x) = i\big(\lim_{h\to\infty} {}_{\boldsymbol{m}'}(a_{i_h})\big) = \lim_{h\to\infty} {}_{\boldsymbol{m}''}\big(i(a_{i_h})\big) = \lim_{h\to\infty} {}_{\boldsymbol{m}''}(a_{i_h}) = x;$$

Le prolongement de i à A est encore l'identité et c'est une application continue de A' sur A'', ce qui est absurde car les topologies $\boldsymbol{m}'$-adique et $\boldsymbol{m}''$-adique ne sont pas comparables.

Proposition 4. *Dans tout corps de nombres $K \neq Q$ il existe deux idéaux premiers distincts $\boldsymbol{m}'$ et $\boldsymbol{m}''$ de même norme m.*

Nous allons montrer qu'il existe toujours dans K deux idéaux premiers distincts $\boldsymbol{m}'$ et $\boldsymbol{m}''$ de degré 1 et de même norme m. Soit K' le plus petit corps galoisien contenant K. Il y a une infinité de nombres premiers p qui se décomposent totalement dans K' (cf. [3]). Soit p un nombre premier qui se décompose totalement dans K' et qui ne se ramifie pas dans K (il y en a une infinité). Si n' (resp. n) est le degré de K' (resp. K) sur Q, on a dans K' $p = \boldsymbol{P}'_1 \boldsymbol{P}'_2 \ldots \boldsymbol{P}'_{n'}$ ($\boldsymbol{P}'_i$, $i = 1, \ldots, n'$, est un idéal premier de K' au dessus de p) et dans K $p = \boldsymbol{P}_1 \boldsymbol{P}_2 \ldots \boldsymbol{P}_r$ ($r \leqslant n$) ($\boldsymbol{P}_i$, $i = 1, \ldots, r$, est un idéal premier de K au dessus de p). On a $N_{K'/Q}(\boldsymbol{P}'_i) = p$, $N_{K'/K}(\boldsymbol{P}'_i) = \boldsymbol{P}^f_j$, $N_{K/Q}(\boldsymbol{P}_j) = p^{f'}$ ($N_{K/Q}(\boldsymbol{P})$ est la norme de $\boldsymbol{P}$ relativement à Q, $N_{K'/K}(\boldsymbol{P}')$ est la norme de $\boldsymbol{P}'$ relativement à K, cf. [5]). La transitivité de la norme implique que $f = f' = 1$ en effet:

$$p = N_{K'/Q}(\boldsymbol{P}'_i) = N_{K/Q}\big(N_{K'/K}(\boldsymbol{P}'_i)\big) = N_{K/Q}(\boldsymbol{P}^f_j) = p^{ff'}$$

et par conséquent $f = f' = 1$ et $r = n$, et, comme $K \neq Q$, $n \geqslant 2$ et le théorème est démontré.

Théorème 2. *Il n'existe pas de corps de nombres $K \neq Q$ qui contiennent une suite d'entiers $a_0, a_1, \ldots$ telle que, pour tout idéal entier $\boldsymbol{m}$ de norme m de K, $a_0, a_1, \ldots, a_{m-1}$ forment un système complet de représentants de $A/\boldsymbol{m}$*

Supposons qu'il existe une telle suite dans un corps de nombres $K \neq Q$. Soient $\boldsymbol{m}'$ et $\boldsymbol{m}''$ deux idéaux premiers distincts de même norme m (proposition 4). Pour $\boldsymbol{m}'$ et $\boldsymbol{m}''$ la suite $a_0, a_1, \ldots$ possède la propriété P car $\boldsymbol{m}'^r \boldsymbol{m}''^s$ est un idéal entier $\boldsymbol{m}$ de K pour tout entier $r \geqslant 0$ et tout entier $s \geqslant 0$. On conclut avec le théorème 1.

Bibliographie

[1] Y. Amice, *Interpolation p-adique*, Bull. Soc. Math. France 92 (1964), p. 117–180.
[2] N. Bourbaki, *Topologie générale*, chapitre 1, 2 et 9.
[3] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press 1967.
[4] W. Narkiewicz, *Some unsolved problems*, Bull. Soc. Math. France, Mémoire 25(1971), p. 159–164.
[5] O. Zariski and P. Samuel, *Commutative Algebra*, t. 1, Van Nostrand 1965.

Reçu le 12.7.1971 (181)

ACTA ARITHMETICA
XXII (1972)

Une généralisation d'un théorème de Cugiani–Mahler

par

MAURICE MIGNOTTE (Paris)

I. INTRODUCTION

Dans l'ouvrage de Mahler [2], on trouve le théorème suivant qui généralise un résultat de Cugiani [1].

THÉORÈME. *Soit ξ un nombre algébrique non nul de degré f. On désigne par $g' \geqslant 2$ et $g'' \geqslant 2$ deux entiers premiers entre eux; par λ et μ deux réels vérifiant*

$$0 \leqslant \lambda \leqslant 1, \quad 0 \leqslant \mu \leqslant 1, \quad \lambda + \mu > 0;$$

par c_1, c_2 et c_3 trois constantes positives; par $\varepsilon(H)$ la fonction

$$\varepsilon(H) = 5\sqrt{\log(4f)}\,(\log\log\log H)^{-1/2},$$

et par $\Sigma = \{K^{(1)}, K^{(2)}, \ldots\}$ une suite infinie de rationnels distincts

$$K^{(h)} = \frac{P^{(h)}}{Q^{(h)}} \quad où \quad P^{(h)} \neq 0,\ Q^{(h)} \neq 0,\ (P^{(h)}, Q^{(h)}) = 1,$$

$$H^{(h)} = \max(|P^{(h)}|, |Q^{(h)}|) > \exp e,$$

tels que

$$|K^{(k)} - \xi| \leqslant c_1 H^{(k)-\lambda-\mu-\varepsilon(H^{(k)})} \tag{1}$$

et

$$|P^{(k)}|_{g'} \leqslant c_2 H^{(k)\lambda-1}, \qquad |Q^{(k)}|_{g''} \leqslant c_3 H^{(k)\mu-1}. \tag{2}$$

Alors

$$\limsup_{k\to\infty} \frac{\log H^{(k+1)}}{\log H^{(k)}} = \infty.$$

Notre but est de démontrer le théorème 1 qui est légèrement plus fort que le théorème précédent.

THÉORÈME 1. *Les notations et les hypothèses sont les mêmes que dans le théorème précédent sauf que l'on définit $\varepsilon(H)$ par*

$$\varepsilon(H) = 4\left(\frac{\log(f+2)\log 2}{a}\right)^{1/2} (\log\log\log H)^{-1/2}, \quad a \text{ réel},\ 0 < a < 6.$$