[3] T. W. Cusick, *Diophantine approximation of ternary linear forms*, Math. Comp. 25 (1971), pp. 163–180.

[4] — *Formulas for some Diophantine approximation constants*, Math. Ann. 197 (1972), pp. 182–188.

[5] H. Davenport, *On a theorem of Furtwängler*, J. London Math. Soc. 30 (1955), pp. 186–195.

DEPARTMENT OF MATHEMATICS
STATE UNIVERSITY OF NEW YORK AT BUFFALO
Buffalo, New York

Received on 15. 2. 1973 (386)

Multiplication par un entier d'une fraction continue périodique

par

HENRI COHEN (Talence)

§ 1. Introduction et notations. Soit x un nombre rationnel. Il possède deux développements en fraction continue:

$$x = [a_0, \ldots, a_n] = [a_0, \ldots, a_n - 1, 1],$$

où $a_i \geqslant 1$ pour $i \geqslant 1$ et $a_n \geqslant 2$.

Nous poserons $\Psi(x) = n$; soit $L(x)$ le nombre de termes de la fraction continue représentant x de longueur impaire, et soit $[[x]]$ cette fraction continue. On a donc $L(x) = \Psi(x) + 1 + \varepsilon(\Psi(x))$ où $\varepsilon(n) = (1-(-1)^n)/2$. Remarquons pour la suite que Ψ et L sont des fonctions définies sur $\boldsymbol{Q}/\boldsymbol{Z}$.

Soit maintenant x un nombre quadratique, c'est-à-dire une racine réelle non rationnelle d'une équation du second degré à coefficients entiers. Le développement en fraction continue de x est périodique, et on écrira:

$$x = [b_0, b_1, \ldots, b_m, \overline{a_1, \ldots, a_n}] \quad \text{avec } a_i, b_i \geqslant 1 \text{ pour } i \geqslant 1$$

$(b_0, \ldots, b_m)$ est la partie non périodique et $(a_1, \ldots, a_n)$ la période.

Nous poserons $P(x) = n$; si on écrit

$$[a_1, \ldots, a_n] = \alpha/\gamma, \quad [a_1, \ldots, a_{n-1}] = \beta/\delta$$

avec $(\alpha, \gamma) = (\beta, \delta) = 1$; $\gamma, \delta \geqslant 0$, on a $\alpha\delta - \beta\gamma = (-1)^n$ et la matrice $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\boldsymbol{Z})$ sera appelée la matrice du nombre quadratique x, ou encore la matrice de la période $(a_1, \ldots, a_n)$ ou de la fraction continue $[a_1, \ldots, a_n]$.

Soit $N > 1$ un entier. Dans [4] M. Mendès France démontre que:

$$\sup_{x \in \boldsymbol{Q}} \big(\Psi(Nx)/\Psi(x)\big) = \sup_{0 \leqslant i < N} L(i/N)$$

et il trouve même plus précisément la valeur de $\sup_{\Psi(x)=n} \Psi(Nx)$.

Ici nous considérons le problème analogue où Q est remplacé par l'ensemble Q des nombres quadratiques et la fonction Ψ par la fonction période P. Nous cherchons à évaluer la quantité:

$$S(N, n) = \sup_{P(x)=n} P(Nx)$$

dont nous redémontrons l'existence (cf. Schinzel [5]).

Remarquons en passant que si on pose

$$S'(N, n) = \sup_{P(x)=n} P\left(\frac{x}{N}\right)$$

on a:

$$S'(N, n) = \sup_{P(x)=n} P\left(\frac{N}{x}\right) = \sup_{P(x)=n} P\left(N \cdot \frac{1}{x}\right) = \sup_{P(1/x)=n} P(nx)$$
$$= \sup_{P(x)=n} P(Nx) = S(N, n).$$

De plus nous montrons l'existence de la quantité

$$R(N) = \sup_{n\geqslant 1}\big(S(N, n)/n\big) = \sup_{x\in Q}\big(P(Nx)/P(x)\big).$$

Nous obtenons la valeur exacte de $R(N)$ pour une infinité de N, et nous conjecturons la valeur de $R(N)$ dans tous les cas. Une partie des résultats démontrés ici ont été cités dans H. Cohen [1].

§ 2. L'algorithme fondamental. Nous utiliserons l'algorithme de [4] pour multiplier une fraction continue par N. Nous l'énonçons sous une forme légèrement différente, facilement déductible de [4]:

THÉORÈME 2.1. *Soit $x = [a_0, \ldots, a_n, \ldots]$ un nombre réel. Posons $x_k = (1/N)\,[a_k, a_{k+1}, \ldots]$. Alors pour tout $k \geqslant 1$ on a:*

$$Nx = \big[[[c_0/d_0]], [[c_1/d_1]], \ldots, [[c_{k-1}/d_{k-1}]], c_k/d_k + 1/d_k^2 x_{k+1}\big]$$

où:

$$(1)\qquad \begin{cases} c_0 = Na_0,\ d_0 = 1, \\ c_{k+1} = \delta_k a_{k+1} + (N/d_k)(c_k/\delta_k)^{-1}, \\ d_{k+1} = N/\delta_k, \\ \delta_k = (c_k, d_k), \end{cases}$$

où l'inverse $(c_k/\delta_k)^{-1}$ est pris modulo (d_k/δ_k) et vérifie:

$$-d_k/\delta_k < (c_k/\delta_k)^{-1} \leqslant 0$$

(si $c_k = 0$ on a $\delta_k = d_k$, donc $(d_k/\delta_k) = 1$ et donc dans ce cas $(c_k/\delta_k)^{-1} = 0$ vérifie bien $(c_k/\delta_k)(c_k/\delta_k)^{-1} = 0 \equiv 1 \pmod{(d_k/\delta_k)}$).

Remarque 2.2. Les relations de récurrence (1) montrent immédiatement que $c_k/d_k > -1$ pour $k \geqslant 1$. Il en résulte que les coefficients de la fraction continue $\big[[[c_0/d_0]], \ldots, [[c_{k-1}/d_{k-1}]]\big]$ sont tous plus grands ou égaux à -1. Le théorème 2.1 ne fournit donc pas toujours un développement en fraction continue régulier (i.e. avec des termes $\geqslant 1$) de Nx. Toutefois, la proposition suivante montre que l'on peut utiliser le théorème 2.1 pour majorer la période de $P(Nx)$ quand x est un nombre quadratique:

PROPOSITION 2.3. *Si x est un nombre quadratique, le développement en fraction continue fourni par le théorème 2.1 est périodique et converge vers Nx quand $k\to\infty$. De plus sa période est supérieure ou égale à $P(Nx)$.*

Démonstration. Soit $x = [b_0, \ldots, b_m, \overline{a_1, \ldots, a_n}]$ le développement en fraction continue de x. Etudions l'algorithme pour $k > m$ (au-delà de b_m). Si $A = \sup_{1\leqslant i\leqslant n} a_i$, on a $-(N/\delta_k) \leqslant c_k \leqslant \delta_k A$ donc en particulier $-N < c_k \leqslant NA$; d'autre part $1 \leqslant d_k \leqslant N$. Enfin il n'y a que n résidus possibles de $k \pmod n$, correspondant à la période $a_1, \ldots, a_n$. En résumé il n'y a qu'un nombre fini de valeurs possibles pour le triplet $(c_k, d_k, k \bmod n)$ et au plus $nN^2(A+1)$. Il résulte donc immédiatement des récurrences (1) que le développement du théorème 2.1 est périodique, de période inférieure ou égale à $nN^2(A+1)\sup_{0\leqslant i<N} L(i/N)$. Bien sûr ceci est un très mauvais majorant; seule l'existence de la périodicité nous intéresse ici.

L'assertion de convergence de la proposition 2.3 est valable pour tout nombre réel x: en effet, si dans l'égalité:

$$Nx = \big[[[c_0/d_0]], [[c_1/d_1]], \ldots, [[c_{k-1}/d_{k-1}]], c_k/d_k + 1/d_k^2 x_{k+1}\big]$$

on fait tendre le coefficient a_{k+1} vers l'infini, on a $x_{k+1}\to\infty$ et donc

$$N[a_0, a_1, \ldots, a_k] = \big[[[c_0/d_0]], \ldots, [[c_{k-1}/d_{k-1}]], [[c_k, d_k]]\big]$$

et quand $k\to\infty$ le premier membre tend vers Nx, donc le développement donné par le théorème 2.1 également.

Ecrivons donc $Nx = [b_0', \ldots, b_{m'}', \overline{a_1', \ldots, a_{n'}'}]$ où les b_i', a_i' sont donnés par le théorème 2.1 et vérifient donc $a_i' \geqslant -1$, $b_i' \geqslant -1$ pour $i \geqslant 1$. Dans [4] M. Mendès France démontre que si:

$y = [a_1', \ldots, a_{n'}', z]$ est un développement fourni par l'algorithme du théorème 2.1, avec $z \in \boldsymbol{R}$ quelconque, alors on peut réécrire y sous la forme $y = [a_1'', \ldots, a_{n''}'', z]$ avec cette fois-ci en développement régulier, i.e. $a_i'' \geqslant 1$ pour $i \geqslant 1$, et $n'' \leqslant n'$. La convergence du développement de Nx joint à ce résultat montre donc que $n' \geqslant P(Nx)$, d'où la proposition 2.3.

COROLLAIRE 2.4. *Appelons $P'(Nx)$ la période du développement fourni par le théorème 2.1. Alors:*

$$S(N, n) = \sup_{P(x)=n} P(Nx) = \sup_{P(x)=n} P'(Nx).$$

Démonstration. On a $\sup_{P(x)=n} P(Nx) \leqslant \sup_{P(x)=n} P'(Nx)$ d'après la proposition 2.3. Réciproquement les relations de récurrence (1) montrent que $c_{k+1} \geqslant a_{k+1} - N$ et $d_{k+1} \leqslant N$, donc on en déduit que si $a_k \geqslant 2N$ pour tout k, le développement fourni par le théorème 2.1 est régulier. Donc:

$$\sup_{P(x)=n} P(Nx) \geqslant \sup_{\substack{P(x)=n \\ (\forall k)(a_k \geqslant 2N)}} P(Nx) = \sup_{\substack{P(x)=n \\ (\forall k)(a_k \geqslant 2N)}} P'(Nx) = \sup_{P(x)=n} P'(Nx)$$

la dernière égalité provenant du fait que la longueur de la période du développement donné par le théorème 2.1 ne dépend que des coefficients $a_k \pmod N$ comme on le voit aisément. D'où le corollaire.

Remarque 2.5. On déduit du corollaire 2.4 que le problème du calcul de $S(N, n)$ pour N et n donnés revient à un calcul fini. En effet, on peut utiliser le développement du théorème 2.1, et d'autre part la longueur de la période fournie par ce développement ne dépend que des coefficients $(\bmod N)$. Il n'y a donc que N^n nombres à considérer pour calculer $S(N, n)$. Bien entendu cela deviendrait fastidieux pour n ou N grands.

§ 3. L'espace P_N. Il nous faut maintenant étudier les récurrences (1) de plus près. Quand N est un nombre premier, on obtient une simplification notable du fait que δ_k est toujours égal à 1 ou N. Il n'en est plus ainsi lorsque N est quelconque, et les calculs directs semblent impossibles. C'est pourquoi nous allons transposer ces récurrences à un nouvel espace, P_N, dans lequel nous les traiterons beaucoup plus facilement.

Géométriquement, P_N est la droite projective sur $\boldsymbol{Z}/N\boldsymbol{Z}$. Comme cette notion n'est peut être pas très familière quand N n'est pas premier, j'en rappellerai les définitions et propriétés essentielles.

Posons $E = \{(a, b) \in \boldsymbol{Z} \times \boldsymbol{Z} \mid \text{P.G.C.D.}(a, b) = 1\}$. Soit R_N la relation définie sur E par

$$(a, b) R_N (a', b') \Leftrightarrow ab' \equiv ba' \pmod N.$$

On vérifie que R_N est une relation d'équivalence sur E (mais pas sur $\boldsymbol{Z} \times \boldsymbol{Z}$ tout entier) et on pose:

$$P_N = E/R_N.$$

D'autre part il est facile de voir que les éléments de $\mathrm{GL}_2(\boldsymbol{Z})$ opèrent sur P_N par passage au quotient par R_N. Les applications (bijectives) de P_N dans P_N qu'ils définissent, s'appellent les homographies de P_N.

Proposition 3.1. *Soit $\Gamma(N)$ le groupe des matrices de $\mathrm{GL}_2(\boldsymbol{Z})$ qui deviennent scalaires modulo N*

$$\Gamma(N) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\boldsymbol{Z}) \mid \beta \equiv \gamma \equiv \alpha - \delta \equiv 0 \pmod N \right\}.$$

On a alors une suite exacte de groupes:

$$1 \to \Gamma(N) \xrightarrow{i} \mathrm{GL}_2(\boldsymbol{Z}) \xrightarrow{p} \mathrm{Aut}(P_N) \to 1$$

où $\mathrm{Aut}(P_N)$ désigne le groupe des homographies de P_N.

Démonstration. Par définition, p est surjective, i est injective. Calculons le noyau de p:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{Ker}\, p$$

si et seulement si:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} R_N \begin{pmatrix} a \\ b \end{pmatrix} \quad \text{pour tout } (a, b) \in E,$$

soit:

$$\gamma a^2 + (\delta - \alpha) ab + \beta b^2 \equiv 0 \pmod N \quad \text{pour tout } (a, b) \in E.$$

Mettant successivement $a = 1$, $b = 0$; $a = 0$, $b = 1$; $a = 1$, $b = 1$, on obtient la proposition.

Nous noterons désormais par $\overline{}$ le passage au quotient par R_N. Il est clair que l'application $a \to \overline{(a, 1)}$ définit une injection canonique de $\boldsymbol{Z}/N\boldsymbol{Z}$ dans P_N, et nous identifierons $\boldsymbol{Z}/N\boldsymbol{Z}$ à un sous-ensemble de P_N grâce à cette injection.

Enfin si $a \in \boldsymbol{Z}$ et $u \in P_N$, nous noterons $a + u^{-1}$ ou $a + 1/u$, le résultat de l'action de $\begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}$ sur u dans P_N.

Proposition 3.2. *Un système de représentants de $E \pmod{R_N}$ est fourni par l'ensemble des couples (a, c) d'entiers positifs tels que:*

$$(*) \qquad (a, c) = 1, \quad c \mid N,$$

a prend une fois toutes les valeurs modulo N/c telles que $(a, c) = 1$.

Pour démontrer cette proposition, démontrons d'abord un lemme:

Lemme 3.3. *Soient a, b, c trois entiers tels que $(a, b) = 1$. Il existe λ entier tel que $(a + \lambda b, c) = 1$.*

En effet, on voit aisément que $\lambda = \prod_{\substack{p \text{ premier} \\ p \mid c, p \nmid a}} p$ convient.

Démonstration de la proposition 3.2. Soit $\overline{(a', b')} \in P_N$, avec $(a', b') \in E$. Posons $d = (b', N)$. Il existe alors A, B tels que:

$$B \cdot (N/d) + A \cdot (b'/d) = 1$$

et l'ensemble des valeurs de A possibles est défini modulo N/d. Puisque $(A, N/d) = 1$, on peut appliquer le lemme 3.3 et on voit donc qu'il est possible de choisir A tel que $(A, N) = 1$ (et donc en particulier $(A, d) = 1$). On vérifie facilement que le couple $(a, c) = (a'A, d)$ vérifie $(a, c) = 1$,

$c|N$. De plus si $\overline{(a,c)} = \overline{(a',c')}$ avec $c|N$, $c'|N$, $(a,c)=1$, $(a',c')=1$, on a $ac' \equiv ca' \pmod N$ et donc puisque $(a,c)=(a',c')=1$:

$$ac' = ca' + \lambda N \text{ entraîne } c'|ca',$$

donc $c'|c$ et de même $c|c'$; donc $c=c'$, et on a donc $a \equiv a' \pmod{N/c}$, d'où la proposition.

PROPOSITION 3.4. *On a*:

$$\operatorname{Card} P_N = N \prod_{p|N} \left(1+\frac{1}{p}\right).$$

Démonstration. D'après la proposition 3.2, pour un c donné, a peut prendre une fois (mod N/c) toutes les valeurs telles que $(a,c)=1$, donc toutes les valeurs premières à $(c, N/c)$. Pour chaque c il y a donc

$$\varphi\big((c,N/c)\big)\frac{N/c}{(c,N/c)} \text{ représentants},$$

donc:

$$f(N) = \operatorname{card} P_N = \sum_{d|N} \varphi\big((d,N/d)\big)\frac{N/d}{(d,N/d)}.$$

On vérifie par les moyens habituels que $f(N)$ est multiplicative, et d'autre part que $f(p^s) = p^s + p^{s-1}$, d'où la proposition.

Nous allons maintenant construire une application Φ_N: $P_N \to \boldsymbol{Q}/\boldsymbol{Z}$ grâce à laquelle nous transposerons dans P_N les récurrences (1).

PROPOSITION 3.5. *Il existe une application*

$$\Phi_N\colon P_N \to \boldsymbol{Q}/\boldsymbol{Z}$$

définie de la façon suivante: *si* $(a,c)\in E$, $c|N$ *on a* $\Phi_N\big(\overline{(a,c)}\big) = a/(N/c) \pmod 1$. *Son image est l'ensemble des nombres rationnels* $a/N \pmod 1$ *avec* $0 \leqslant a < N$.

Démonstration. La proposition 3.2 montre que si $\overline{(a,c)} = \overline{(a',c')}$ avec $(a,c)=1$, $(a',c')=1$, $c|N$, $c'|N$, on a $c=c'$ et $a \equiv a' \pmod{N/c}$ donc $a/(N/c) \equiv a'/(N/c') \pmod 1$, d'où l'existence de l'application. Le reste de la proposition résulte du fait que $\Phi_N\big(\overline{(a,1)}\big) = a/N$.

Nous pouvons maintenant terminer le programme que nous nous sommes imposés au début de ce paragraphe, i.e. transposer à P_N les récurrences (1):

THÉORÈME 3.6. *Gardons les notations du théorème* 2.1. *Soit* (u_k) *la suite d'éléments de* P_N *définie par*

$$u_0 = \overline{(1,N)}, \qquad u_{k+1} = a_{k+1} + u_k^{-1}. \tag{2}$$

Alors on a:

$$u_k = \overline{(e_k, N/d_k)}$$

où $(e_k, N/d_k)\in E$ *et* $e_k \equiv c_k \pmod{d_k}$, *ou encore*:

$$\Phi_N(u_k) \equiv c_k/d_k \pmod 1 \quad \textit{pour tout } k \geqslant 0.$$

Démonstration. Pour $k=0$ on a bien $d_0=1$ et $e_0 = 1 \equiv c_0 = Na_0 \pmod 1$. Supposons maintenant $k>0$ et que:

$$u_k = \overline{(e_k, N/d_k)}, \qquad (e_k, N/d_k) = 1 \quad \text{et} \quad e_k \equiv c_k \pmod{d_k}.$$

Par définition, on a:

$$u_{k+1} = \overline{(a_{k+1}e_k + N/d_k,\ e_k)}.$$

Par hypothèse de récurrence, on a:

$$(e_k, N) = (e_k, N/d_k)\cdot(e_k, d_k) = (e_k, d_k) = (c_k, d_k) = \delta_k.$$

Comme dans la démonstration de la proposition 3.2, soit A un entier tel que:

$$A(e_k/\delta_k) \equiv 1 \pmod{N/\delta_k} \quad \text{et} \quad (A, N) = 1.$$

On a alors (cf. proposition 3.2):

$$u_{k+1} = \overline{\big(A(a_{k+1}e_k + N/d_k),\ \delta_k\big)}.$$

D'autre part $A(c_k/\delta_k) \equiv 1 \big(\bmod (d_k/\delta_k)\big)$ puisque $d_k|N$ et $e_k \equiv c_k \pmod{d_k}$, donc $A \equiv (c_k/\delta_k)^{-1} \big(\bmod (d_k/\delta_k)\big)$.

Par ailleurs $Ae_k \equiv \delta_k \pmod N$, donc en définitive:

$$A(a_{k+1}e_k + N/d_k) \equiv a_{k+1}\delta_k + (c_k/\delta_k)^{-1}(N/d_k) \big(\bmod (N/\delta_k)\big)$$

et le théorème 3.6 résulte immédiatement des récurrences (1).

Le théorème 3.6 montre donc l'utilité de l'espace P_N qui a réduit les récurrences (1) à la récurrence (2), beaucoup plus maniable, et qui peut encore s'écrire:

$$u_k = a_k + \frac{1|}{|a_{k-1}} + \frac{1|}{|a_{k-2}} + \ldots + \frac{1|}{|a_1} \pmod N. \tag{3}$$

§ 4. Application au calcul de $P(Nx)$. Revenons maintenant à notre problème initial qui est de calculer $P(Nx)$. Nous avons le théorème suivant:

THÉORÈME 4.1. *Soit* $x = [b_0, \ldots, b_m, \overline{a_1, \ldots, a_n}]$ *un nombre quadratique, M la matrice de x. Soit* $(u_k)_{k\geqslant 0}$ *la suite d'éléments de* P_N *associée au nombre x par le théorème* 3.6, *et posons* $v_j = u_{m+j}$ *pour* $j \geqslant 0$. *Soit* $\lambda_0(M) = \lambda_0(N,M)$ *le plus petit entier* >0 *tel que* $M^{\lambda_0(N,M)} \in \Gamma(N)$. *Alors*:

$$P'(Nx) \textit{ divise } \sum_{1\leqslant k\leqslant n\lambda_0(N,M)} L\big(\Phi_N(v_k)\big)$$

et en particulier:

$$P(Nx) \leqslant \sum_{1\leqslant k\leqslant n\lambda_0(N,M)} L\big(\Phi_N(v_k)\big). \tag{4}$$

Démonstration. Posons $a_{\lambda n+k} = a_k$ pour $1 \leqslant k \leqslant n$ et $\lambda > 0$. Le théorème 3.6 montre que:

$$v_k = a_k + \frac{1|}{|a_{k+1}} + \ldots + \frac{1|}{|a_1} + \frac{1|}{|v_0}.$$

Si k_0 est le plus petit $k > 0$ tel que $v_{k_0} = v_0$ et $n \mid k_0$, alors il est clair que $v_{k+s,k_0} = v_k$ pour tous s, k donc v_k est périodique de période k_0. Inversement, si $v_k = v_{k'}$ et $k \equiv k' \pmod n$, les homographies étant bijectives dans P_N on en déduit $v_{|k-k'|} = v_0$. D'autre part, si $v_{k_0} = v_0$ on déduit avec les notations du théorème 2.1 que $d_{k_0+m} = d_m$ et $c_{k_0+m} \equiv c_m \pmod{d_m}$ ce qui entraîne comme on le voit facilement:

$$d_{k_0+m+j} = d_{m+j}, \qquad c_{k_0+m+j} = d_{m+j} \quad \text{pour tout } j \geqslant 1$$

et donc la périodicité des (v_j) est équivalente à celle des (c_{m+j}, d_{m+j}). Enfin la théorie formelle des fractions continues montre que $v_{k+n} = M(v_k)$[1] et donc $v_{\lambda n} = M^\lambda(v_0)$, d'où le théorème 4.1.

Corollaire 4.2.

$$S(N, n) = \sup_{M \in \mathscr{M}} \sum_{1 \leqslant k \leqslant n\lambda_0(N,M)} L\big(\Phi_N(v_k)\big)$$

où $\mathscr{M}$ désigne la famille des matrices d'une période de longueur n.

Démonstration. Cela résulte immédiatement du théorème 4.1 et du corollaire 2.5, sachant que les a_i peuvent être changés d'un multiple arbitraire de N sans changer la périodicité des (v_k).

On peut déjà déduire du théorème 4.1 un excellent majorant pour $S(N, n)$ et $R(N)$:

Théorème 4.3. *$S(N, n)$ et $R(N)$ existent, et on a:*

$$S(N, n) \leqslant n \sum_{u \in P_N} L\big(\Phi_N(u)\big); \qquad R(N) \leqslant \sum_{u \in P_N} L\big(\Phi_N(u)\big).$$

Démonstration. Il suffit bien entendu de démontrer la première inégalité. Dans la démonstration du théorème 4.1 nous avons vu que $v_k = v_{k'}$ et $k \equiv k' \pmod n$ entraîne $v_{|k-k'|} = v_0$. Il en résulte que pour $0 \leqslant \lambda < \lambda_0(N, M)$ les $v_{\lambda n+k}$ avec k fixé sont des éléments distincts de P_N, donc:

$$\begin{aligned} S(N, n) &\leqslant \sup_{M \in \mathscr{M}} \sum_{1 \leqslant k \leqslant n\lambda_0(N,M)} L\big(\Phi_N(v_k)\big) = \sup_{M \in \mathscr{M}} \sum_{1 \leqslant k \leqslant n} \sum_{0 \leqslant \lambda < \lambda_0(N,M)} L\big(\Phi_N(v_{\lambda n+k})\big) \\ &\leqslant \sup_{M \in \mathscr{M}} \sum_{1 \leqslant k \leqslant n} \sum_{u \in P_N} L\big(\Phi_N(u)\big) = n \sum_{u \in P_N} L\big(\Phi_N(u)\big). \end{aligned}$$

On déduit par exemple du théorème 4.3:

(1) rappelons (cf. § 3) que les éléments de $\mathrm{GL}_2(\mathbf{Z})$ opèrent sur P_N par passage au quotient par R_N.

Corollaire 4.4. *Soit p un nombre premier. Alors:*

(a) $R(p^s) \leqslant \sum_{0 \leqslant a < p^s} L\left(\frac{a}{p^s}\right) + \sum_{0 \leqslant a < p^{s-1}} L\left(\frac{a}{p^{s-1}}\right)$;

(b) $R(2) \leqslant 5\ (5)$, $R(3) \leqslant 8\ (8)$, $R(4) \leqslant 14\ (14)$, $R(5) \leqslant 16\ (15)$, $R(6) \leqslant 28\ (28)$, $R(7) \leqslant 24\ (24)$, $R(8) \leqslant 36\ (26)$, $R(9) \leqslant 36\ (36)$

où les nombres entre parenthèses indiquent les vraies valeurs.

On voit donc que les majorants donnés par le théorème 4.3 semblent être très proches de la vérité. Nous verrons d'ailleurs (théorème 6.1) que ces majorants donnent la vraie valeur pour une infinité de couples (N, n) pour $S(N, n)$, pour une infinité de N pour $R(N)$.

§ 5. Etude de $\lambda_0(N, M)$. Pour obtenir une amélioration des majorants du théorème 4.3 il faut étudier plus en détail le nombre $\lambda_0(N, M)$.

Proposition 5.1. $M^\lambda \in \Gamma(N) \Leftrightarrow \lambda_0(N, M) \mid \lambda$.

Démonstration. Il est clair que si $M^\lambda \in \Gamma(N)$ et $M^{\lambda'} \in \Gamma(N)$ alors

$$M^{A\lambda+B\lambda'} = (M^\lambda)^A (M^{\lambda'})^B \in \Gamma(N)$$

donc l'ensemble des λ tels que $M^\lambda \in \Gamma(N)$ est un sous-groupe de $\mathbf{Z}$, égal à $\lambda_0(N, M)\mathbf{Z}$.

Proposition 5.2. $(N, N') = 1 \Rightarrow \lambda_0(NN', M) = [\lambda_0(N, M), \lambda_0(N', M)]$. (Ici $[a, b]$ signifie bien sûr le P.P.C.M. de a et b.)

Démonstration. D'après la proposition 5.1, on a:

$$M^\lambda \in \Gamma(NN') \Leftrightarrow M^\lambda \in \Gamma(N) \text{ et } M^\lambda \in \Gamma(N') \Leftrightarrow \lambda_0(N, M) \mid \lambda \text{ et } \lambda_0(N', M) \mid \lambda$$

d'où la proposition.

Cette proposition montre donc qu'il suffit d'étudier $\lambda_0(p^s, M)$ avec p premier. Le théorème suivant résume les résultats sur ce nombre (2):

Théorème 5.3. *Soit p un nombre premier, $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z})$ avec $\alpha\delta - \beta\gamma = \varepsilon = (-1)^n$. Posons:*

$$D(M) = D = (\alpha - \delta)^2 + 4\beta\gamma = (\alpha + \delta)^2 - 4\varepsilon = (\alpha + \delta)^2 + 4(-1)^{n-1}.$$

Alors $M^\lambda \in \Gamma(N)$ (i.e. $\lambda_0(p^6) \mid \lambda$) pour les valeurs de λ données par les tableaux suivants, où $\left(\frac{D}{p}\right)$ est le symbole de Legendre–Jacobi (3):

(2) Le cas $s = 1$ est traité dans Lehmer [3]. Pour la commodité du lecteur nous donnons la démonstration du cas général, qui est certainement classique.

(3) Nous n'utiliserons ce symbole qu'avec D au numérateur; ne pas confondre avec $\left(\frac{p-1}{2}\right)$ ou $\left(\frac{p+1}{2}\right)$ par exemple.

(a) *si* $p > 2$

	$\left(\frac{D}{p}\right) = +1$	$\left(\frac{D}{p}\right) = 0$	$\left(\frac{D}{p}\right) = -1$
$n\left(\frac{p-1}{2}\right)$ *impair*	$p^{s-1}(p-1)$		$p^{s-1}(p+1)$
$n\left(\frac{p-1}{2}\right)$ *pair*	$p^{s-1}\left(\frac{p-1}{2}\right)$	p^s	$p^{s-1}\left(\frac{p+1}{2}\right)$

(b) *si* $p = 2$

si $\left(\frac{D}{p}\right) = -1$ (*i.e.* $D \equiv 5 \pmod 8$):

	$s = 1$	$s = 2$	$s \geqslant 3$
n impair	3	6	$3 \cdot 2^{s-2}$
n pair	3	3	$3 \cdot 2^{s-3}$

si $\left(\frac{D}{p}\right) = 0$: *si* $D \equiv 0 \pmod 8$ 2^s

si $D \equiv 4 \pmod 8$: 2 *si* $s = 1$, 2^{s-1} *si* $s \geqslant 2$.

Démonstration. (a) Remarquons d'abord que $n\left(\frac{p-1}{2}\right)$ impair implique n impair et $p \equiv 3 \pmod 4$, donc $D = (\alpha+\delta)^2+4 \equiv 0 \pmod p$ est impossible car sinon -4 serait résidu quadratique (mod p). C'est pourquoi la case: $n\left(\frac{p-1}{2}\right)$ impair et $\left(\frac{D}{p}\right) = 0$ n'existe pas.

Nous poserons:

$$T = (\alpha+\delta)/2, \qquad \Delta = T^2 - \varepsilon = D/4$$

et enfin:

$$r_M(k) = r(k) = \left((T+\sqrt{\Delta})^k - (T-\sqrt{\Delta})^k\right)/2\sqrt{\Delta},$$

$$s_M(k) = s(k) = \left((T+\sqrt{\Delta})^k + (T-\sqrt{\Delta})^k\right)/2.$$

Enfin pour toute matrice $S \in \mathrm{GL}_2(\mathbf{Z})$ nous poserons:

$$S = \begin{pmatrix} \alpha(S) & \beta(S) \\ \gamma(S) & \delta(S) \end{pmatrix}.$$

Lemme 5.4. *On a pour tout* k *entier*:

$$\begin{aligned} \alpha(M^k) &= s(k) + \frac{\alpha-\delta}{2} r(k), \qquad \beta(M^k) = \beta r(k), \\ \gamma(M^k) &= \gamma r(k), \qquad \delta(M^k) = s(k) - \frac{\alpha-\delta}{2} r(k). \end{aligned} \tag{5}$$

En particulier si $M \in \Gamma(p^a)$ *mais* $M \notin \Gamma(p^{a+1})$, *pour tout* $s \geqslant a$

$$M^k \in \Gamma(p^s) \Leftrightarrow r(k) \equiv 0 \pmod{p^{s-a}}.$$

Démonstration. Il est facile de voir que (5) est satisfait pour $k = 0$ et 1. D'autre part l'équation caractéristique de la matrice M est:

$$M^2 - 2T \cdot M + \varepsilon I_2 = 0,$$

les deux membres des égalités de (5) vérifient donc la relation de récurrence:

$$u_k - 2Tu_{k-1} + \varepsilon u_{k-2} = 0.$$

Par suite (5) est vrai pour tout k. Le reste du lemme résulte facilement des définitions.

Lemme 5.5. *Le théorème* 5.3 *est vrai pour* $p > 2$, $s = 1$.

Démonstration. En utilisant le développement du binôme on voit que

$$r(p) \equiv \Delta^{(p-1)/2} \pmod p, \qquad s(p) \equiv T \pmod p.$$

(Des congruences faisant interfenir Δ et T seront considérées comme étant dans $\mathbf{Z}[\frac{1}{2}]$.) Il en résulte que:

(i) si $\left(\frac{D}{p}\right) = 0$, alors $r(p) \equiv 0 \pmod p$, d'où le lemme dans ce cas;

(ii) si $\left(\frac{D}{p}\right) = +1$, $\Delta^{(p-1)/2} \equiv 1 \pmod p$, donc $M^p \equiv \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \pmod p$ et donc $M^{p-1} \equiv I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \Gamma(p)$.

Si de plus $n\left((p-1)/2\right)$ est pair, on a:

$$\alpha(M^{(p-1)/2})\,\delta(M^{(p-1)/2}) - \beta(M^{(p-1)/2})\,\gamma(M^{(p-1)/2}) = (-1)^{n((p-1)/2)} = 1$$

et d'autre part, puisque $M^{p-1} = (M^{(p-1)/2})^2$:

$$\alpha^2(M^{(p-1)/2}) + \beta(M^{(p-1)/2})\,\gamma(M^{(p-1)/2}) \equiv 1 \pmod p$$

d'où en ajoutant:

$$\alpha(M^{(p-1)/2})\left(\alpha(M^{(p-1)/2}) + \delta(M^{(p-1)/2})\right) \equiv 2 \pmod p$$

et donc:

$$\alpha(M^{(p-1)/2}) + \delta(M^{(p-1)/2}) \not\equiv 0 \pmod p.$$

Or par définition, puisque $M \notin \Gamma(p)$ (sinon $\left(\frac{D}{p}\right) = 0$) on a:

$$r(p-1) = 2r\left(\frac{p-1}{2}\right) s\left(\frac{p-1}{2}\right) = r\left(\frac{p-1}{2}\right)\left(\alpha(M^{(p-1)/2}) + \delta(M^{(p-1)/2})\right)$$
$$\equiv 0 \pmod{p}$$

donc d'après ce qui précède:

$$r\left(\frac{p-1}{2}\right) \equiv 0 \pmod{p}$$

d'où le lemme dans ce cas.

(iii) Le cas $\left(\frac{D}{p}\right) = -1$ se démontre de façon analogue en remplaçant $p-1$ par $p+1$.

LEMME 5.6. *Soit $v_p(x)$ la valuation p-adique de x (i.e.: $p^{v_p(x)} | x$ mais $p^{v_p(x)+1} \nmid x$). Supposons que $p | D(M)$. Alors pour $s \geqslant 0$:*

$$v_p\left(r_M(p^s)\right) = s.$$

Démonstration. C'est vrai pour $s = 0$ trivialement. Pour $s = 1$, on a:

$$r_M(p) \equiv pT^{p-1} \pmod{p^2} \text{ puisque } p | D(M).$$

D'autre part puisque $v_p\left(D(M)\right) = v_p(T^2 - \varepsilon) \geqslant 1$ on a $v_p(T^2) = v_p(T^{p-1}) = 0$, d'où $v_p\left(r_M(p)\right) = 1$. On remarque maintenant que:

$$D(M^p) = D(M)\left(r_M(p)\right)^2,$$

donc en particulier $p | D(M) \Rightarrow p | D(M^{p^s})$ pour tout $s \geqslant 1$.

Enfin, on déduit de (5) que pour une matrice quelconque (i.e. $\in M_2(\boldsymbol{R})$):

$$\beta(M^{p^s}) = \beta(M) r_M(p^s) = \beta(M^{p^{s-1}}) r_{M^{p^{s-1}}}(p) = \beta(M) r_M(p^{s-1}) r_{M^{p^{s-1}}}(p)$$

donc:

$$r_M(p^s) = r_M(p^{s-1}) r_{M^{p^{s-1}}}(p)$$

pour $\beta(M) \neq 0$, et par continuité ceci est vrai pour tout M (bien sûr on peut aussi démontrer cette relation directement). Il résulte de ceci et des remarques précédentes que:

$$v_p\left(r_M(p^s)\right) = v_p\left(r_M(p^{s-1})\right) + 1$$

d'où le lemme 5.6.

On peut maintenant terminer la démonstration du théorème 5.3 dans le cas $p > 2$: si $M^k \in \Gamma(p)$ alors $p | D(M^k)$ et $(M^k)^{p^{s-1}} \in \Gamma(p^s)$ d'après le lemme 5.6. Le cas $p > 2$ résulte donc immédiatement du lemme 5.5.

Remarquons au passage le corollaire suivant:

COROLLAIRE 5.7. *Supposons que $M^{\lambda_0(p,M)} \in \Gamma(p^a)$ mais $\notin \Gamma(p^{a+1})$. Alors:*

$$\lambda_0(p^s, M) = \lambda_0(p, M) p^{s-a}.$$

Démonstration. Ceci résulte immédiatement des lemmes 5.4 et 5.6 et des considérations précédentes.

Démonstration de (b): $p = 2$.

(i) Si $D \equiv 5 \pmod 8$, i.e. $\alpha + \delta$ impair, on a:

$$r(3) = 3T^2 + \Delta = 4T^2 - \varepsilon = (\alpha+\delta)^2 - \varepsilon.$$

Si n est impair, $\varepsilon = -1$:

$$r(3) = (\alpha+\delta)^2 + 1$$

et on a: $v_2\left(r(3)\right) = 1$.

D'autre part $r(6) = r(3)\left(\alpha(M^3) + \delta(M^3)\right)$ et:

$$\alpha(M^3) + \delta(M^3) = (\alpha+\delta)\left((\alpha+\delta)^2 + 3\right),$$

donc: $v_2\left(\alpha(M^3) + \delta(M^3)\right) = 2$, d'où: $v_2\left(r(6)\right) = 3$.

On montre alors facilement comme pour le corollaire 5.7 que $v_2\left(r(3 \cdot 2^{s-1})\right) = s+1$.

Si n est pair, $\varepsilon = +1$, $r(3) = (\alpha+\delta)^2 - 1 \equiv 0 \pmod 8$ et par récurrence on voit aisément que $r(3 \cdot 2^{s-1}) \equiv 0 \pmod{2^{s+2}}$, d'où le théorème 5.3 dans ce cas.

(ii) Si $D \equiv 0 \pmod 8$, on a: $v_2(\alpha+\delta) = 1$, d'où $v_2\left(r(2)\right) = 1$ et comme précédemment par récurrence: $v_2\left(r(2^s)\right) = s$.

Si $D \equiv 4 \pmod 8$. Ici $\alpha + \delta \equiv 0 \pmod 4$, donc $r(2) \equiv 0 \pmod 4$ et par récurrence $r(2^s) \equiv 0 \pmod{2^{s+1}}$, d'où le théorème 5.3.

§ 6. Calcul de $S(p^s, n)$ et $R(p^s)$ avec $n\left(\frac{p-1}{2}\right)$ impair.

Avant d'améliorer les majorants donnés par le théorème 4.3 et le corollaire 4.4 nous allons montrer que ces majorations sont en fait des égalités pour une infinité de (N, n).

Posons pour simplifier les notations $F(m) = \sum_{0 \leqslant a < m} L(a/m)$.

THÉORÈME 6.1. *Soit p un nombre premier $p \equiv 3 \pmod 4$. On a*

$$S(p^s, n) = n\left(F(p^s) + F(p^{s-1})\right)$$

si n est impair, et

$$R(p^s) = F(p^s) + F(p^{s-1}).$$

Démonstration. Nous avons vu que $\mathrm{Card} P_{x^s} = p^{s-1}(p+1)$. Si on peut trouver une matrice M d'un nombre quadratique x de période n, telle que

$$\lambda_0(p^s, M) = p^{s-1}(p+1)$$

il résultera du corollaire 4.2 et du théorème 4.3 que:

$$S(N,n) = n \sum_{u \in P_N} L\big(\Phi_N(u)\big),$$

d'où le théorème 6.1.

D'après le théorème 5.3 une telle matrice n'existe que si $p \equiv 3 \pmod 4$ et $\det(M) = -1$, $\left(\frac{D(M)}{p}\right) = -1$. Montrons l'existence d'une telle matrice.

LEMME 6.2. *Soit M une matrice telle que $v_p\big(r_M(p+1)\big) = 1$ et $\lambda_0(p, M) = p+1$. Alors:*

$$\lambda_0(p^s, M) = p^{s-1}(p+1).$$

Démonstration. L'hypothèse signifie que $M^{p+1} \in \Gamma'(p)$, mais $M^{p+1} \notin \Gamma'(p^2)$. Le lemme découle donc immédiatement du corollaire 5.7 appliqué avec $a = 1$.

LEMME 6.3. *Il existe a entier tel que la matrice $M = \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}$ vérifie les conditions du lemme* 6.2.

Démonstration. Considérons l'application norme (définie puisque $p \equiv 3 \pmod 4$)

$$\mathcal{N}: \big((\boldsymbol{Z}/p\boldsymbol{Z})[\sqrt{-1}]\big)^* \to (\boldsymbol{Z}/p\boldsymbol{Z})^*,$$

$$x + iy \longrightarrow x^2 + y^2.$$

D'après la théorie élémentaire des corps finis $\mathcal{N}$ est surjective. L'application $\mathcal{N}^2$ a donc comme image le sous-groupe à $(p-1)/2$ éléments des résidus quadratiques non nuls dans $(\boldsymbol{Z}/p\boldsymbol{Z})$ et son noyau, ensemble des éléments de norme ± 1, est donc un groupe à $(p^2-1)/\big((p-1)/2\big) = 2(p+1)$ éléments, cyclique comme sous-groupe d'un groupe cyclique. Soit z un générateur, et choisissons

$$a \equiv (z+\bar{z})/2 \pmod p,$$

ce qui laisse encore la possibilité de changer a d'un multiple de p.

z étant de norme -1 (sinon il n'y aurait pas d'éléments de norme -1, contredisant la surjectivité de $\mathcal{N}$) est racine de:

$$z^2 - az - 1 = 0$$

ce qui peut aussi s'écrire avec des notations antérieures $z^2 - 2Tz + \varepsilon = 0$, équation caractéristique de la matrice M. On a donc $z = T \pm \sqrt{\Delta}$. D'autre part:

$$r(k) \equiv 0 \pmod p \Leftrightarrow T + \sqrt{\Delta})^k \equiv (T - \sqrt{\Delta})^k \pmod p \Leftrightarrow z^{2k} \equiv (-1)^k \pmod p.$$

De plus: $r(k) \equiv 0 \pmod p \Rightarrow z^{4k} \equiv 1 \pmod p \Rightarrow 2p+2 \mid 4k \Rightarrow \frac{p+1}{2} \mid k \Rightarrow k$ pair (puisque $p \equiv 3 \pmod 4) \Rightarrow z^{2k} \equiv 1 \pmod p \Rightarrow (p+1) \mid k$ et réciproquement $p+1 \mid k \Rightarrow r(k) \equiv 0 \pmod p$ trivialement, ce qui montre que $\lambda_0(p, M) = p+1$.

Supposons maintenant que pour le a choisi, on ait:

$$v_p\big(r(p+1)\big) \geqslant 2.$$

Posons pour le reste de cette démonstration:

$$r_a(k) = r_M(k) \quad \text{où} \quad M = \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}.$$

Le développement du binôme montre immédiatement que:

$$r_a(p+1) = \left(\frac{a}{2}\right)^p + \frac{a}{2}\left(\frac{a^2}{4}+1\right)^{(p-1)/2} + pX(a).$$

Dérivant par rapport à a on en déduit

$$r'_a(p+1) = \frac{p}{2}\left(\frac{a}{2}\right)^{p-1} + \frac{p-1}{2}\left(\frac{a^2}{4}\right)\left(\frac{a^2}{4}+1\right)^{(p-3)/2} + pX'(a) \not\equiv 0 \pmod p$$

puisque $\frac{a^2}{4}+1 \not\equiv 0 \pmod p$ (car $p \equiv 3 \pmod 4$) et $a \not\equiv 0 \pmod p$ car sinon $z^2 = 1$ et z est de norme 1.

Il résulte de la formule de Taylor appliquée à $r_a(p+1)$ considérée comme polynôme en a que:

$$r_{a+p}(p+1) \equiv r_a(p+1) + pr'_a(p+1) \equiv pr'_a(p+1) \pmod{p^2}$$

donc $v_p\big(r_{a+p}(p+1)\big) = 1$, d'où le lemme 6.3.

On peut maintenant achever la démonstration du théorème 6.1: soit x un nombre quadratique dont la période est

$$(a, 0, 0, \ldots, 0) \ (n-1 \text{ zéros}).$$

(Rappelons que le calcul de $\lambda_0(N, M)$ ne dépend que des coefficients de la période modulo N, donc les 0 ne sont pas gênants.)

On vérifie facilement que la matrice de x est $\begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}$ et le théorème 6.1 découle immédiatement des lemmes 6.2 et 6.3.

COROLLAIRE 6.4. *Soit p un nombre premier $p \equiv 7 \pmod{12}$. On a:*

$$S(2p^s, n) = n\big(F(2p^s) + F(p^s) + F(2p^{s-1}) + F(p^{s-1})\big)$$

si n est impair, et

$$R(2p^s) = F(2p^s) + F(p^s) + F(2p^{s-1}) + F(p^{s-1}).$$

Démonstration. Il est facile de voir que les membres de droite de ces égalités sont également les majorants du théorème 4.3. Il suffit donc à nouveau de montrer l'existence d'un quadratique x dont la matrice M vérifie $\lambda_0(2p^s, M) = 3p^{s-1}(p+1)$. Or d'après la démonstration du théorème 6.1, il existe un a tel que la matrice $M = \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}$ vérifie:

$$\lambda_0(p^s, M) = p^{s-1}(p+1).$$

D'autre part on peut faire varier a d'un multiple de p^s sans changer cette égalité, et on peut donc supposer a impair, ce qui entraîne $D(M) = a^2+4 \equiv 5 \pmod 8$. Se reportant aux tableaux du théorème 5.3 on voit que $\lambda_0(2, M) \mid 3$ et puisque $M \notin \Gamma(2)$ trivialement, il en résulte que $\lambda_0(2, M) = 3$. L'hypothèse $p \equiv 7 \pmod{12}$ entraînant que $(p^{s-1}(p+1), 3) = 1$ la proposition 5.2 montre que:

$$\lambda_0(2p^s, M) = 3p^{s-1}(p+1)$$

d'où le corollaire.

Je laisse au lecteur le soin de montrer qu'en dehors de quelques valeurs particulières, le théorème 6.1 et le corollaire 6.4 sont les seuls cas où les majorants du théorème 4.3 soient exacts.

Corollaire 6.5. *En dehors des cas* $N = p^s$ *avec* $p \equiv 3 \pmod 4$ *et* $N = 2 \cdot p^s$ *avec* $p \equiv 7 \pmod{12}$ *les majorants du théorème* 4.3 *ne sont exacts que dans les cas suivants:*

$N = 2$: $S(2, n) = 5n$ *pour tout* n; $R(2) = 5$,
$N = 4$: $S(4, n) = 14n$ *pour* n *impair*; $R(4) = 14$,
$N = 6$: $S(6, n) = 28n$ *pour* n *impair*; $R(6) = 28$.

§ 7. Amelioration des majorants et conjectures. Vu le corollaire 6.5, il faut chercher à améliorer les majorants du théorème 4.3 dans les autres cas. Pour l'instant nous restons dans le cas $N = p^s$ qui est le plus facilement traitable.

Théorème 7.1. *Supposons que la condition suivante soit vérifiée:*

(C) *Pour tout* c *tel que* $0 \leqslant c < p$, *on a:*

$$A(c) = \sum_{0 \leqslant \lambda < p^{s-1}} L\big((c+\lambda p)/p^s\big) \geqslant F(p^{s-1}),$$

i. e.: $\inf\limits_{0 \leqslant c < p} A(c) = A(0) = F(p^{s-1})$.

Alors pour tout nombre premier $p > 2$ *et* n *pair, on a:*

$$S(p^s, n) = nF(p^s).$$

Démonstration. Considérons d'abord le cas $s = 1$. Pour toute matrice $M \in \mathrm{SL}_2(\boldsymbol{Z})$, on a $\lambda_0(p, M) \leqslant p$, donc si M est la matrice d'un quadratique x, on aura:

$$P(px) \leqslant n\Big(\sum_{u \in P_p} L\big(\Phi_N(u)\big) - 1\Big) = nF(p).$$

D'autre part il est clair que si $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, correspondant à un quadratique x de période $(1, 0, \ldots, 0)$ avec $n-1$ zéros, on a $\lambda_0(p, M) = p$ et de plus avec les notations du théorème 4.1:

$$P(px) = n\Big(\sum_{u \in P_p} L\big(\Phi_N(u)\big) - 1\Big) = nF(p).$$

Il résulte de ceci que le théorème 7.1 est vrai pour $s = 1$, sans même la condition (C) (qui est trivialement vérifiée pour $s = 1$). Si $s > 1$ et M est la même matrice que précédemment, on vérifie à nouveau que $P(p^s x) = nF(p^s)$, donc que:

$$S(p^s, n) \geqslant nF(p^s).$$

D'autre part, utilisant la surjection canonique

$$P_{p^s} \to P_p$$

on voit aisément que pour toute matrice M d'un quadratique x, il existe des c_i tels que:

$$P(p^s x) \leqslant \sum_{0 \leqslant i < n} \Big(\sum_{u \in P_{p^s}} L\big(\Phi_N(u)\big) - \sum_{0 \leqslant \lambda < p^{s-1}} L\big((c_i + \lambda p)/p^s\big) \Big)$$

d'où le théorème 7.1.

Remarque 7.2. Je conjecture que la condition (C) est toujours vérifiée. On peut justifier cette conjecture de la façon suivante: pour $c \neq 0$, $A(c)$ est une somme de p^{s-1} longueurs de fractions continues de dénominateur égal à p^s. Au vu des récents résultats d'Heilbronn [2], il est raisonnable de penser que $A(c) \sim \dfrac{12 \operatorname{Log} 2}{\pi^2} s p^{s-1} \operatorname{Log} p$, pour $c \neq 0$. Par contre, pour $c = 0$, $A(0) = F(p^{s-1})$ est une somme de p^{s-1} longueurs de fractions continues de dénominateur inférieur ou égal à p^{s-1}. Le résultat d'Heilbronn montre d'ailleurs que

$$A(0) \sim \frac{12 \operatorname{Log} 2}{\pi^2} (s-1) p^{s-1} \operatorname{Log} p$$

ce qui rend donc la conjecture très plausible. Ceci est en fait confirmé par des recherches sur ordinateur.

En utilisant des méthodes semblables à celles du théorème 7.1 je conjecture plus généralement:

CONJECTURE 7.3. Si n est pair, alors:

(a) Si $N \not\equiv \pm 2 \pmod{12}$ $\quad S(N,n) = nF(N)$;

(b) Si $N \equiv \pm 2 \pmod{12}$ $\quad S(N,n) = n\big(F(N)+F(N/2)\big)$.

Cette conjecture résulterait de la démonstration de conditions analogues à la condition (C).

Comme première étape vers cette conjecture, je laisse le soin au lecteur de démontrer la:

PROPOSITION 7.4. *Si n est pair, alors $S(N,n) \geqslant nF(N)$.*

CONJECTURE 7.5. Si n est impair, soit $p \equiv 1 \pmod 4$ est premier, soit $p = 2$ et $s \geqslant 3$, alors:

$$S(p^s,n) = nF(p^s)+F(p^{s-1}) - \sum_{0 \leqslant \lambda < p^{s-1}} L\big((i+\lambda p)/p^s\big)$$

où i est la racine de $-1 \bmod p$ qui rend cette expression maximale.

Je sais démontrer cette conjecture dans le cas $s = 1$, et dans ce cas i est la racine de $-1 \bmod p$ telle que $0 < i \leqslant p/2$. C'est peut être le cas pour s quelconque.

Il semble très difficile de formuler une conjecture analogue à la conjecture 7.3 quand n est impair.

§ 8. Conjecture sur $R(N)$-conclusion. En analysant de près les résultats du théorème 5.3 et en utilisant des techniques semblables à celles du paragraphe précédent, on est amené à formuler la conjecture suivante sur la valeur exacte de $R(N)$:

CONJECTURE 8.1. Appelons $W(N)$ l'ensemble des diviseurs premiers p de N tels que $p \equiv 3 \pmod 4$, et $\omega(N) = \operatorname{Card} W(N)$. Alors $R(N)$ est donné par les formules suivantes:

(a) si $N \equiv 0 \pmod{12}$

$$R(N) = F(N).$$

(b) si $N \equiv \pm 1, \pm 5 \pmod{12}$

$$R(N) = \begin{cases} F(N)+F(N/p) \text{ si } \omega(N) = 1 \text{ et si } p \in W(N) \text{ vérifie } (p+1, N) = 1; \\ F(N) \text{ sinon.} \end{cases}$$

(c) si $N \equiv \pm 2 \pmod{12}$

$$R(N) = \begin{cases} F(N)+F(N/2)+F(N/p)+F(N/2p) \\ \quad \text{si } \omega(N) = 1 \text{ et si } p \in W(N) \text{ vérifie } (p+1, 3N/2) = 1; \\ F(N)+F(N/2) \text{ sinon.} \end{cases}$$

(d) si $N \equiv \pm 3 \pmod{12}$

$$R(N) = \begin{cases} F(N)+F(N/3) \text{ si } W(N) = \{3\}; \\ F(N) \text{ sinon.} \end{cases}$$

(e) si $N \equiv \pm 4 \pmod{12}$

$$R(N) = \begin{cases} F(N)+F(N/2) \text{ si } 8 \nmid N \text{ et } W(N) = \emptyset; \\ F(N) \text{ sinon.} \end{cases}$$

(f) si $N \equiv 6 \pmod{12}$

$$R(N) = \begin{cases} F(N)+F(N/2)+F(N/3)+F(N/6) \text{ si } W(N/3) = \emptyset; \\ F(N) \text{ sinon.} \end{cases}$$

Dans cette direction, il n'est pas difficile de montrer par exemple que si $\omega(N) \geqslant 2$, alors

$$R(N) = \begin{cases} F(N)+F(N/2) \text{ si } N \equiv \pm 2 \pmod{12}; \\ F(N) \text{ sinon.} \end{cases}$$

D'autre part il résulte immédiatement de la proposition 7.4 que $R(N) \geqslant F(N)$.

La conjecture générale semble assez difficile à démontrer; je pense d'ailleurs que la valeur exacte de $R(N)$ a peu d'intérêt, et que seuls les majorants du théorème 4.3 sont intéressants théoriquement. Cette conjecture est vérifiée numériquement pour les petites valeurs de N comme le montre la table des valeurs de $R(N)$ ci-dessous:

$R(1) = 1$,	$R(2) = 5$,	$R(3) = 8$,	$R(4) = 14$,	$R(5) = 15$,
$R(6) = 28$,	$R(7) = 24$,	$R(8) = 26$,	$R(9) = 36$,	$R(10) = 47$,
$R(11) = 44$,	$R(12) = 38$,	$R(13) = 51$,	$R(14) = 80$,	$R(15) = 68$,
$R(16) = 58$,	$R(17) = 71$,	$R(18) = 68$,	$R(19) = 84$,	$R(20) = 106$,
$R(21) = 81$,	$R(22) = 131$,	$R(23) = 108$,	$R(24) = 90$,	$R(25) = 105$,
$R(26) = 163$,	$R(27) = 144$,	$R(28) = 114$,	$R(29) = 139$,	$R(30) = 216$.

Pour terminer, étudions le comportement de $R(N)$ quand $N \to \infty$.

PROPOSITION 8.2. $R(N) = O(N \operatorname{Log} N)$. *Plus précisément, il existe $A, B > 0$ tels que:*

$$AN \operatorname{Log} N < R(N) < BN \operatorname{Log} N.$$

Démonstration. Il est facile de voir que le théorème 5.3 et la proposition 5.2 entraînent que $\lambda_0(N, M) \leqslant 2N$ pour toute matrice M. Utilisant le fait que $L(a/N) = O(\operatorname{Log} N)$ il résulte du corollaire 4.2 que $R(N) = O(N \operatorname{Log} N)$. La proposition résulte alors de $R(N) \geqslant F(N)$ et de $F(N) > AN \operatorname{Log} N$ pour un $A > 0$ (voir par exemple Heilbronn [2]).

Bibliographie

[1] H. Cohen, *Multiplication par un entier d'une fraction continue périodique*, CRAS, 276 (19 février 1973), p. 595–598.

[2] H. Heilbronn, *On the average length of a class of finite continued fractions*, Abhandlungen Zahlentheorie und Analysis, Berlin 1968, p. 87–96 (édité par Turán en souvenir de Landau).

[3] D. H. Lehmer, *An extended theory of Lucas functions*, Ann. of Math. 31 (1930), p. 419–449.
[4] M. Mendès France, *Sur les fractions continues limitées*, Acta Arith. 23 (1973), p. 207–215.
[5] A. Schinzel, *On some problems of the arithmetical theory of continued fractions*, *I*, Acta Arith. 6 (1961), p. 394–413; *II*, Ibid. 7 (1962), p. 288–298.

Reçu le 22. 6. 1973 (430)

ACTA ARITHMETICA
XXVI (1974)

Note on sequences well-spaced and well-distributed among congruence classes

by

S. L. G. Choi (Vancouver, Canada)

Let

$$a_1 < a_2 < \dots \tag{1}$$

be an infinite sequence of positive integers with asymptotic density (1) δ. Then it is said to be a *well-spaced sequence* if there exists a constant $C = C(\delta)$, depending only on δ, so that

$$\sup_{i \geqslant 1}(a_{i+1} - a_i) < C.$$

Suppose $0 < \eta < 1$. Then the sequence (1) of asymptotic density δ is said to be (η)-*well-distributed* among congruence classes if there exists an absolute constant K so that for all $m \leqslant Kn^{1-\eta}$, we have

$$\Big| \sum_{\substack{a_i \equiv a (m) \\ a_i \leqslant n}} 1 - \delta n m^{-1} \Big| \doteq o(\delta n m^{-1}); \qquad a = 0, \dots, m-1$$

as $n \to \infty$.

Henceforth we shall refer to a sequence which is well-spaced and (η)-well-distributed among congruence classes as an η-*sequence*.

One question that naturally presents itself is whether the function $f_\eta(\delta)$, which denotes (2) $\inf_{\mathscr{A}} \overline{\lim} A_2(n) n^{-1}$, where the inf is taken over all η-sequences $\mathscr{A}$ with asymptotic density δ, tends to ∞ as $\delta \to 0$.

In this paper we shall prove the following theorem which shows that $f_{1/2}(\delta)$ is bounded for all $\delta > 0$. It is an open question whether there exists $\eta < \frac{1}{2}$ so that $f_\eta(\delta)$ remains bounded for all $\delta > 0$.

Theorem. *For every $\delta > 0$ there exists a $(\frac{1}{2})$-sequence $\mathscr{A}$ of asymptotic density δ such that*

$$\overline{\lim} A_2(n) n^{-1} \leqslant (2 + o(1))\,\delta. \tag{2}$$

(1) The asymptotic density of a sequence $\mathscr{A}$, if it exists, is defined to be $\lim_{\eta \to \infty} A(n) n^{-1}$, where $A(n)$ is the counting function of $\mathscr{A}$.

(2) $A_2(n)$ denotes the number of integers $\leqslant n$ of the form $a_i + a_j$ where $a_i, a_j \in \mathscr{A}$.