Séminaire Delange-Pisot-Poitou. Théorie des nombres

Gérard Rauzy

Relations de récurrence modulo m

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 5 (1963-1964), exp. n° 2, p. 1-10

<http://www.numdam.org/item?id=SDPP_1963-1964__5__A2_0>

SéminaireDELANGE-PISOT
(Théorie des nombres)
5e année, 1963/64, n° 2

25 novembre 1963

RELATIONS DE RÉCURRENCE MODULO m

par Gérard RAUZY

1. Position du problème.

1.1. - Nous considérons une suite u_n vérifiant la relation de récurrence : $u_{n+s} = b_1 u_{n+s-1} + \dots + b_s u_n$ où les coefficients b_i sont des entiers. En supposant que u_n est entier pour $n = 0, \dots, s-1$, nous avons alors, quel que soit $n \geqslant 0$, u_n entier.

On dira que cette suite admet la période T mod m si

$$\exists\ n_1 \text{ tel que } \forall\ n \geqslant n_1,\ u_{n+T} = u_n \pmod m .$$

1° Considérons le "vecteur" $U_n = (u_n, \dots, u_{n+s-1})$ mod m, il ne peut prendra que m^s valeurs. Donc quand n prend les valeurs $0, \dots, m^s$, deux de ces valeurs sont égales, c'est-à-dire que :

$$\exists\ n_1 < m^s \text{ et } n_2 = n_1 + T \quad (T \geqslant 1) \text{ tels que } U_{n_1} = U_{n_2} \pmod m ,$$

on en déduit alors par récurrence que : $\forall\ n \geqslant n_1,\ u_{n+T} = u_n \pmod m$, c'est-à-dire que T est une période mod m.

1.3. - Nous désignerons par $T(m)$ le plus petit entier $T \geqslant 1$ tel que $U_{n_1+T} = U_{n_1} \pmod m$ et par $n_0(m)$ le plus petit n tel que $U_{n+T(m)} = U_n \pmod m$.

u_n admet donc la période $T(m)$ à partir du rang $n_0(m)$, et l'on a une majoration :

$$1 \leqslant n_0(m) + T(m) \leqslant m^s .$$

1.4. - Alors u_n admet la période T mod m $\Longleftrightarrow$ $T(m) \mid T$.

En effet supposons que u_n admette la période T, c'est-à-dire que :

$$\exists\ n_1 \text{ tel que } \forall\ n \geqslant n_1,\ u_{n+T} = u_n \pmod m .$$

Posons $T = qT(m) + r$ avec $0 \leqslant r < T(m)$.

Si $n_2 = \max(n_1, n_0(m))$, on a, $\forall\ n \geqslant n_2$, $u_{n+T(m)} = u_n \pmod m$, donc

$$u_{n+qT(m)+r} = u_{n+r} \pmod m, \text{ mais } u_{n+T} = u_n \pmod m ,$$

d'où finalement $u_{n+r} = u_n \pmod m$, $\forall\ n \geqslant n_2$.

Mais $\exists\ k$ tel que $\forall\ n \geqslant n_0$, $n + kT(m) \geqslant n_2$.

Donc si $n \geqslant n_0(m)$, $u_{n+kT(m)+r} = u_{n+kT(m)} \pmod m$, d'où $u_{n+r} = u_n \pmod m$. Soit finalement $U_{n_0} = U_{n_0+r}$ ce qui par définition de $T(m)$ et de $n_0(m)$, compte tenu de l'inégalité $0 \leqslant r < T(m)$, entraîne $r = 0$, c'est-à-dire $T(m) \mid T$. La réciproque est évidente.

1.5. - La recherche des périodes mod m se ramène donc au calcul de $T(m)$ et $n_0(m)$. Nous pouvons même supposer m de la forme p^λ où p est un nombre premier grâce au résultat suivant :

$$\begin{cases} T(a \wedge b) = T(a) \wedge T(b) \quad (\text{où } u \wedge v \text{ désigne le p. p. c. m. de } u \text{ et } v) \\ n_0(a \wedge b) \leqslant \max(n_0(a)\ ,\ n_0(b)) \ . \end{cases}$$

En effet, $\forall\ n \geqslant \max(u_0(a)\ ,\ n_0(b))$, $u_{n+T(a)\wedge T(b)} = u_n \begin{cases} \text{mod } a \\ \text{mod } b \end{cases} \Longrightarrow \text{mod } a \wedge b$ et réciproquement, si T est période mod $a \wedge b$, T est période mod a et mod b , donc $T(a) \mid T$, $T(b) \mid T$ ce qui entraîne bien $T(a) \wedge T(b) \mid T$.

1.6. - Posons alors pour T entier $\geqslant 1$,

$$\rho_u(T) = \overline{\lim_{n\to\infty}} \left| u_{n+T} - u_n \right|_p \quad (\text{l'indice } u \text{ rappelant la suite utilisée}) .$$

Si $\rho_u(T) > 0$, la valuation p-adique étant discrète, $\exists\ n$ tel que $\left| u_{n+T} - u_n \right|_p = \rho_u(T)$, nous désignerons par $n_u(T)$ le plus petit n tel que cette égalité soit satisfaite.

On voit alors que $T(p^\lambda)$ est le plus petit T tel que $\rho_u(T) \leqslant p^{-\lambda}$

et que $n_0(p^\lambda) = n_u(T(p^\lambda))$ (si $\rho_u(T(p^\lambda)) > 0$).

Si au contraire il existe T tel que $\rho_u(T) = 0$, on voit que T est période mod p^λ quel que soit λ (mais le rang à partir duquel T est période peut dépendre de λ).

On est donc ramené à l'étude de la fonction $\rho_u(T)$.

1.7. - Si $p \mid b_i$ quel que soit $i = 1\ ,\ \ldots\ ,\ s$, alors $p^k \mid u_n$ pourvu que $\frac{n}{s} \geqslant k$. Nous supposerons donc que $\exists\ i$ tel que $p \nmid b_i$, nous pouvons alors définir t tel que : $1 \leqslant t \leqslant s$ et, quel que soit $\sigma > t$, $\left| b_\sigma \right|_p < 1$, mais $\left| b_t \right| = 1$.

Nous supposerons d'autre part que la relation de récurrence est bien d'ordre s, c'est-à-dire que $b_s \neq 0$ et que, d'autre part, la suite u_n envisagée ne satisfait pas à une relation de récurrence d'ordre inférieur. Dans l'hypothèse faite ($b_s \neq 0$), On sait que la condition nécessaire et suffisante pour qu'il en soit ainsi est que le déterminant :

$$\begin{vmatrix} u_0 & u_{s-1} \\ u_{s-1} & u_{2(s-1)} \end{vmatrix} \neq 0$$

1.8. - Ceci nous conduit à introduire les matrices à coefficients dans $\underset{\sim}{Q}$:

$$\mathcal{U}_n = \begin{pmatrix} u_n & \cdots & u_{n+s-1} \\ u_{n+s-1} & \cdots & u_{n+2s-2} \end{pmatrix}$$

et les vecteurs :

$$U_n = \begin{pmatrix} u_n \\ u_{n+s-1} \end{pmatrix}$$

Si nous désignons alors par $\mathcal{M}$ la matrice :

$$\mathcal{M} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ \vdots & & & 0 \\ 0 & & 0 & 1 \\ b_s & \cdots & & b_1 \end{pmatrix}$$

on aura : $U_{n+1} = \mathcal{M}U_n$ et $\mathcal{U}_{n+1} = \mathcal{M}\mathcal{U}_n$.

On voit aisément que $\det(\mathcal{M} - z\mathcal{J}) = (-1)^s (z^s - b_1 z^{s-1} \cdots b_s)$.

Donc, les valeurs propres de $\mathcal{M}$ sont les racines du polynôme $P(z) = z^s - b_1 z^{s-1} \cdots b_s$, il en résulte que <u>le maximum de leurs valeurs absolues est égal à</u> $\max|b_i|^{1/i} = 1$ (polygone de Newton).

1.9. - Tout ce que nous allons faire pourrait l'être en supposant les b_i et les u_n dans un surcorps K de $\underset{\sim}{Q}_p$ en gardant les hypothèses $\max_{i=1,\ldots,s} |b_i| = 1$ et $\max_{i=0,\ldots,s-1} |u_i| = 1$ à condition toutefois que la valeur absolue sur K soit discrète et que le corps des restes de K soit fini.

2. Valeur absolue sur les matrices à coefficients dans un corps p-adique.

2.1. - Etant donnée une matrice $\mathfrak{A} = (a_{ij})$ $(i = 0, \ldots, s-1,$ $j = 0, \ldots, s-1)$, nous notons $|\mathfrak{A}|_p = \max_{i,j} |a_{ij}|_p$. On a alors trivialement $|\mathfrak{A}| = 0 \iff \mathfrak{A} = 0$

$$\begin{cases} |c\mathfrak{A}| = |c|\,|\mathfrak{A}|\ , \quad \forall\ c \text{ scalaire}, \\ |\mathfrak{A} + \mathfrak{B}| \leqslant \max(|\mathfrak{A}|\ ,\ |\mathfrak{B}|)\ . \end{cases}$$

2.2. - Soit $\mathfrak{A} = (a_{ij})$, $\mathfrak{B} = (b_{ij})$, $\mathfrak{C} = (c_{ij}) = \mathfrak{A}\mathfrak{B}$.

$$c_{ij} = \sum_k a_{ik}\, b_{kj}\ , \quad \text{d'où} \quad |c_{ij}| \leqslant \max_k |a_{ik}|\ |b_{kj}| \leqslant \max_k |a_{ik}| \max_k |b_{kj}) \leqslant |\mathfrak{A}|\ |\mathfrak{B}|$$

donc $|\mathfrak{A}\mathfrak{B}| \leqslant |\mathfrak{A}|\ |\mathfrak{B}|$.

2.3. - Mais nous aurons besoin d'une majoration dans l'autre sens.

Supposons $\mathfrak{A}$ inversible, c'est-à-dire $\det \mathfrak{A} \neq 0$, alors $\mathfrak{A}^{-1} = (a'_{ij})$ avec $a'_{ij} = \dfrac{A_{ji}}{\det \mathfrak{A}}$, A_{ji} étant le mineur de a_{ji} dans $\mathfrak{A}$; c'est donc un déterminant d'ordre $s-1$, c'est-à-dire un polynôme à coefficients entiers homogène de degré $s-1$ par rapport au coefficient de $\mathfrak{A}$.

On a donc

$$|A_{ji}| \leqslant |\mathfrak{A}|^{s-1} \implies |\mathfrak{A}^{-1}| \leqslant |\mathfrak{A}|^{s-1}/|\det \mathfrak{A}|\ ,$$

mais alors

$$|\mathfrak{B}| = |\mathfrak{A}^{-1}\, c| \leqslant |\mathfrak{A}|^{s-1}\ |c|/|\det \mathfrak{A}| \quad \text{soit} \quad |c| \geqslant \frac{|\mathfrak{B}|\ |\det \mathfrak{A}|}{|\mathfrak{A}|^{s-1}}$$

(il est aisé de voir que l'on peut trouver $\mathfrak{A}$ et $\mathfrak{B}$ tel que l'on ait égalité).

On peut faire le même raisonnement en remplaçant $\mathfrak{A}$ par $\mathfrak{B}$, et la majoration s'étend bien entendu au cas $\det \mathfrak{A} = 0$, à condition que $\mathfrak{A} \neq 0$. On a donc en supposant $\mathfrak{A} \neq 0$, $\mathfrak{B} \neq 0$

$$\max \left(\frac{|\det \mathfrak{A}|}{|\mathfrak{A}|^s}\ ,\ \frac{|\det \mathfrak{B}|}{|\mathfrak{B}|^s} \right) \leqslant \frac{|\mathfrak{A}\mathfrak{B}|}{|\mathfrak{A}|\ |\mathfrak{B}|} \leqslant 1\ .$$

3. Valeurs absolues des puissances d'une matrice carrée.

3.1. - Soit $\mathfrak{A}$ une matrice carrée. On à évidemment $|\mathfrak{A}^n| \leqslant |\mathfrak{A}|^n$, donc $\overline{\lim}\ |\mathfrak{A}^n|^{1/n} \leqslant |\mathfrak{A}|$. On posera

$$\|\mathfrak{a}\| = \overline{\lim}\, |\mathfrak{a}^n|^{1/n} \text{ , donc } \|\mathfrak{a}\| \leqslant |\mathfrak{a}| \text{ .}$$

Plus généralement il existe une suite m_k telle que $\lim |\mathfrak{a}^{m_k}|^{1/m_k} = \|\mathfrak{a}\|$, soit une infinité de k , v_k prend la même valeur v , $0 \leqslant v < n$, en changeant au besoin la suite m_k , nous supposons que $v_k = v$ quel que soit k .

Supposons alors $\|\mathfrak{a}\| \neq 0$, on ne peut avoir $|\mathfrak{a}^v| = 0$ (sinon $\forall\ h \geqslant v$, $|\mathfrak{a}^h| = 0$, d'où $\|\mathfrak{a}\| = 0$). On peut écrire :

$$|\mathfrak{a}^{m_k}| \leqslant |\mathfrak{a}^v|\ |\mathfrak{a}^n|^{u_k} \text{ d'où } |\mathfrak{a}^{m_k}|^{1/m_k} \leqslant |\mathfrak{a}^v|^{1/m_k}\ |\mathfrak{a}^n|^{u_k/m_k} \text{ .}$$

Quand $k \to \infty$, $m_k \to \infty$, donc : $u_k/m_k \to 1/n$, on a donc à la limite puisque $|\mathfrak{a}^v| \neq 0$

$$\|\mathfrak{a}\| \leqslant |\mathfrak{a}^n|^{1/n} \text{ .}$$

Bien entendu cette égalité vaut aussi quand $\|\mathfrak{a}\| = 0$.

3.2. - Soit $A(z) = \det(\mathfrak{a} - z\mathfrak{J})$, le polynôme caractéristique de la matrice $\mathfrak{a}$ ($\mathfrak{J}$ matrice unité), $A(z) = (-1)^s z^s + a_1 z^{s-1} + \dots + a_s$.

On a donc : $(-1)^s \mathfrak{a}^{n+s} + a_1 \mathfrak{a}^{n+s-1} + \dots + a_s \mathfrak{a}^n = 0$, $\mathfrak{a}^n$ satisfait donc à une relation de récurrence linéaire à coefficients constants. Si θ_1 , ... , θ_k sont les racines distinctes de $A(z)$ avec comme ordres de multiplicité h_1 , ... , h_k on peut écrire

$$\mathfrak{a}^n = \sum_{i=1}^{k} \theta_i^n\, \mathfrak{P}_i(n) \text{ ,}$$

où les $\mathfrak{P}_i(n)$ sont des matrices polynomiales :

$$\mathfrak{P}_i(n) = \sum_{j=0}^{h_i-1} n^j\, \mathfrak{P}_{i,j} \text{ .}$$

On a donc si $\mu = \max_{i=1,\dots,k} |\theta_i| = \max_{i=1,\dots,s} |a_i|^{1/i}$, $C = \max_{i,j} |\mathfrak{P}_{i,j}|$

$$|\mathfrak{a}^n| \leqslant C\mu^n \text{ , d'où } \|\mathfrak{a}\| \leqslant \mu \text{ .}$$

3.3. - Considérons la série $\mathfrak{F}(z) = \sum_{n=0}^{\infty} \mathfrak{a}^n z^n$, elle est convergente (au sens de la métrique introduite) pour $|z| < \frac{1}{\|\mathfrak{a}\|}$ et l'on a trivialement dans ce disque $(\mathfrak{J} - z\mathfrak{a})\ \mathfrak{F}(z) = \mathfrak{J}$, donc en particulier

$$\det(\mathfrak{J} - z\mathfrak{a})\ \det \mathfrak{F}(z) = 1 \text{ soit } \det(\mathfrak{J} - z\mathfrak{a}) \neq 0 \text{ .}$$

En particulier, si θ est valeur propre, et si $\theta \neq 0$, comme $\det(\mathfrak{J} - \frac{1}{\theta}\mathfrak{a}) = 0$, on a nécessairement $\frac{1}{|\theta|} \geqslant \frac{1}{\|\mathfrak{a}\|}$, donc $\|\mathfrak{a}\| \geqslant |\theta|$, donc finalement $\|\mathfrak{a}\| \geqslant \mu$.

0_n en déduit donc

$$\|\alpha\| = \mu = \max_{i=1,\dots,s} |a_i|^{1/i} ,$$

et par conséquent pour $n \geqslant 1$,

$$\|\alpha\|^n \leqslant |\alpha^n| \leqslant c\|\alpha\|^n .$$

4. Etude de $\mathfrak{M}^n \alpha$ où $\mathfrak{M}$ est la matrice associée à la relation de récurrence $u_{n+s} = b_1 u_{n+s-1} + \dots + b_s u_n$.

4.1. - Pour la matrice $\mathfrak{M} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & \diagdown & \diagdown \\ 0 & \diagdown & 1 \\ b_s & \dots & b_1 \end{pmatrix}$ on a évidemment $|\mathfrak{M}| = 1$, mais comme $\max |b_i|^{1/i} = 1$, on entire $\|\mathfrak{M}\| = |\mathfrak{M}| = 1$.

Si α est une matrice quelconque, on a alors $|\mathfrak{M}^{n+1} \alpha| \leqslant |\mathfrak{M}^n \alpha| \leqslant |\alpha|$.

En outre si $\det \alpha \neq 0$, on a : $|\mathfrak{M}^n \alpha| \geqslant \dfrac{|\mathfrak{M}^n|}{|\alpha|^{s-1}} |\det \alpha| = \dfrac{|\det \alpha|}{|\alpha|^{s-1}}$.

La suite décroissante $|\mathfrak{M}^n \alpha|$ sera bornée inférieurement par un nombre positif, donc la valeur absolue étant discrète, la suite $|\mathfrak{M}^n \alpha|$ sera constante à partir d'un certain rang. Nous allons maintenant préciser ce rang.

4.2. - Posons $\rho = \max_{\sigma>t} |b_\sigma|$, on a si $t < s$, $\rho < 1$.

Le polynôme caractéristique de $\mathfrak{M}$ étant le polynôme $(-1)^s P(z)$, il en résulte que :

$\mathfrak{M}^n \alpha$ satisfait à la relation de récurrence :

$$\mathfrak{M}^{n+s} \alpha = b_1 \mathfrak{M}^{n+s-1} \alpha + \dots + b_s \mathfrak{M}^n \alpha .$$

a. Supposons alors que $\exists\, n$ tel que : $|\mathfrak{M}^{n+i} \alpha| = |\mathfrak{M}^n \alpha|$ pour $i = 0 , \dots , r$, où $r = s - t$; alors on a :

$$\mathfrak{M}^{n+s} \alpha - b_1 \mathfrak{M}^{n+s-1} \alpha \dots - b_{t-1} \mathfrak{M}^{n+r+1} \alpha - b_t \mathfrak{M}^{n+r} \alpha - b_{t+1} \mathfrak{M}^{n+r-1} \alpha - b_s \mathfrak{M}^n \alpha = 0$$

si l'on avait $|\mathfrak{M}^{n+r+1} \alpha| < |\mathfrak{M}^{n+r} \alpha|$ on aurait, en vertu de la décroissance de $|\mathfrak{M}^n \alpha|$ et du fait que $|b_t| = 1$,

$$|\mathfrak{M}^{n+r} \alpha| \leqslant \max_{i=1,\dots,r} (|b_{t+i}| \, |\mathfrak{M}^{n+r-i} \alpha|) \leqslant \rho |\mathfrak{M}^n \alpha| ,$$

ce qui est impossible vu l'hypothèse faite, on a donc : $|\mathfrak{M}^{n+r+1} \alpha| = |\mathfrak{M}^n \alpha|$.

Par récurrence on voit alors que si la suite $|\mathfrak{M}^n \alpha|$ est constante pour $n = n_0 , n_0 + 1 , \dots , n_0 + r$ elle est constante quel que soit $n \geqslant n_0$.

b. Si nous supposons au contraire que $|\pi^{n+1}\alpha| < |\pi^n\alpha|$, alors le même raisonnement montre que $|\pi^n\alpha| \leq \rho|\pi^{n-r}\alpha|$, il en résulte que, si n est tel que $\exists\ m > n$, $|\pi^m\alpha| < |\pi^n\alpha|$, il existe $n_1 \geq n - r$ tel que $|\pi^n\alpha| \leq \rho|\pi^{n_1}\alpha|$. On en déduit alors par récurrence que :

$$\underline{\text{ou bien}}\quad |\pi^m\alpha| \quad \underline{\text{est constante pour}}\quad m \geq n\ ,$$

$$\underline{\text{ou bien}}\quad |\pi^n\alpha| \leq \rho^{[n/r]}|\alpha|\ .$$

c. En particulier, <u>si</u> $\det\alpha \neq 0$, <u>la suite</u> $|\pi^n\alpha|$ <u>est constante dès que</u> $\rho^{[n/r]} \leq \dfrac{|\det\alpha|}{|\alpha|^s}$, et ce résultat vaut même si la valuation n'est pas discrète.

4.3. - Si $t = s$, on a alors $|b_s\pi^n\alpha| \leq \max\limits_{i=1,\dots,s} |\pi^{n+i}\alpha|$, et comme $|b_s| = 1$, on en déduit que dans ce cas : $|\pi^n\alpha| = |\alpha|$, $\forall\ n \geq 0$.

5. <u>Périodes de</u> π^n.

5.1. - Nous posons $\pi_{n,T} = \pi^{n+T} - \pi^n = \pi^n\pi_T$, avec $\pi_T = \pi^T - \mathfrak{d}$, et nous posons $\rho(T) = \lim\limits_{n\to\infty} |\pi_{n,T}|$, comme $|\pi_T| \leq 1$, on a $\rho(T) \leq 1$.

D'après le paragraphe précédent, si $\rho(T) > 0$, $\exists\ n_0(T)$ tel que

$$n \geq n_0(T) \implies |\pi_{n,T}| = \rho(T)\ ,$$

et l'on a la majoration :

$$0 \leq n_0(T) \leq \frac{r\ \mathrm{Log}\ \rho(T)}{\mathrm{Log}\ \rho}\ .$$

5.2. - <u>L'ensemble des</u> T, <u>tels que</u> $\rho(T) < 1$, <u>est constitué par les multiples d'un même nombre</u> τ. Nous posons $\tau = \min\limits_{\rho(T)<1} T$ (nous laissons pour l'instant à part la question d'existence).

Soit T tel que $\rho(T) < 1$, posons $T = q\tau + r$ $(0 \leq r < \tau)$

$$\pi_{n,T} = \pi^{n+q\tau+r} - \pi^n = \pi^{n+r}\sum_{i=0}^{q-1}(\pi^{(i+1)\tau} - \pi^{i\tau}) + \pi^{n+r} - \pi^n = \sum_{i=0}^{q-1}\pi_{n+r+i\tau,\tau} + \pi_{n,r}$$

alors dès que $n \geq \max(n_0(T)\ ,\ n_0(\tau))$, $|\pi_{n,T}| < 1$,

$$|\pi_{n+r+i\tau,\tau}| < 1 \implies |\pi_{n,r}| < 1 \implies \rho(r) < 1\ .$$

Mais d'après la définition de τ et de r ceci ne peut se produire que pour $r = 0$. La réciproque est évidente.

5.3. - Soit T tel que $\rho(T) < 1$, alors si $p \nmid q$, $\rho(qT) = \rho(T)$. On a

$$\pi_{n,qT} = (\mathfrak{M}^{n+qT} - \mathfrak{M}^n = \mathfrak{M}^n(\mathfrak{M}^{qT} - \mathbb{S}) = \mathfrak{M}^n((\mathbb{S} + \pi_T)^q - \mathbb{S}) = \mathfrak{M}^n(\sum_{i=1}^{q} C_q^i \pi_T^i)$$

d'où

$$\pi_{n,qT} = q\pi_{n,T} + \sum_{i=2}^{q} C_q^i \mathfrak{M}^n \pi_T^i ,$$

$\mathfrak{M}$ et π_T sont commutables, on a donc, si n est assez grand et $i \geqslant 2$:

$$\mathfrak{M}^n \pi_T^i = \mathfrak{M}^{n-2[n/2]}(\mathfrak{M}^{[n/2]} \pi_T)^2 \pi_T^{i-2} , \text{ d'où } |\mathfrak{M}^n \pi_T^i| \leqslant \rho(T)^2 ,$$

donc $|\pi_{n,qT} - q\pi_{n,T}| \leqslant \rho(T)^2$, on en déduit bien le résultat.

5.4. - Si $p > 2$ et $\rho(T) < 1$, on a : $\rho(pT) = \frac{1}{p}\rho(T)$. On a en effet

$$\pi_{n,pT} = p\pi_{n,T} + \sum_{i=2}^{p-1} C_p^i \mathfrak{M}^n \pi_T^i + \mathfrak{M}^n \pi_T^p ,$$

alors dès que n assez grand si $i = 2, \ldots, p-1$, $|\mathfrak{M}^n \pi_T^i| \leqslant (\rho(T))^2$ et $|C_p^i| \leqslant \frac{1}{p}$; de même dès que n assez grand :

$$\mathfrak{M}^n \pi_T^p = \mathfrak{M}^{n-p[n/p]}(\mathfrak{M}^{[n/p]} \pi_T)^p , \text{ donc } |\mathfrak{M}^n \pi_T^i| \leqslant (\rho(T))^p .$$

C'est ici qu'intervient l'hypothèse valuation discrète, en effet $\rho(T) < 1 \implies \rho(T) \leqslant 1/p$, donc $\rho(T)^p \leqslant \rho(T)^2 \times (\frac{1}{p})^{p-2}$, comme $p > 2$, $\rho(T)^p \leqslant \frac{1}{p}\rho(T)^2$ d'où

$$|\pi_{n,pT} - p\pi_{n,T}| \leqslant \frac{1}{p}\rho(T)^2 \text{ et } |p\pi_{n,T}| = \frac{1}{p}\rho(T) ,$$

ce qui montre bien le résultat.

5.5. - Bien entendu les résultats de 5.3 et 5.4, établis dans le cas $\rho(T) \neq 0$, s'étendent au cas $\rho(T) = 0$. D'autre part soit $\overline{\mathfrak{M}}$ la matrice associée à $\mathfrak{M}$ dans le corps des restes. Celui-ci étant fini $\overline{\mathfrak{M}}^n$ ne peut prendre qu'un nombre fini de valeurs, donc (principe des tiroirs) il existe n et T tels que $\overline{\mathfrak{M}}^{n+T} = \overline{\mathfrak{M}}^n$. Il en résulte $|\mathfrak{M}^{n+T} - \mathfrak{M}^n| < 1$, donc $\rho(T) < 1$, ce qui prouve l'existence de τ. On peut alors résumer les résultats précédents par :

$$\exists\ \tau \geqslant 1 \text{ tel que : } \begin{cases} \rho(T) = 1 \text{ si } \tau \nmid T , \\ \rho(T) = |\frac{T}{\tau}|_p \rho(\tau) \text{ si } \tau \mid T . \end{cases}$$

6. Etude des fonctions $\rho_u(T)$ et $n_u(T)$.

6.1. - Nous supposons que la suite u_n ne vérifie pas de relation de récurrence d'ordre inférieur, c'est-à-dire que $\det \mathcal{U}_0 \neq 0$. Si nous posons alors

$$\gamma_{n,T} = \mathcal{U}_{n+T} - \mathcal{U}_n = \pi_{b,T}\, \mathcal{U}_0 \ ,$$

d'où $|\gamma_{n,T}| \leqslant |\gamma_{n,T}|$, donc : $|\gamma_{n,T}| = |U_{n+T} - U_n|$. On a $\rho_u(T) = \lim |\gamma_{n,T}|$, donc on a la majoration $\rho(T)\,|\det \mathcal{U}_0| \leqslant \rho_u(T) \leqslant \rho(T)$ (on a supposé $\overline{\lim}_{n\to\infty} |\mathcal{U}_0| = 1$).

6.2. - Plus précisément on peut refaire les raisonnements du paragraphe précédent. On a

$$\gamma_{n,qT+r} = \sum_{r=0}^{q-1} \gamma_{n+iT,T} + \gamma_{n,r} \ ,$$

donc les T <u>tels que</u> $\rho_u(T) \leqslant x$ <u>sont les multiples du plus petit d'entre eux.</u>

6.3. - D'autre part dans l'hypothèse où $\rho(T) \neq 0$,

$$\gamma_{n+T,T} - \gamma_{n,T} = (\pi^{m+T} - \pi^m)\, \gamma_{n-m,T} \ ,$$

donc dès que n assez grand :

$$|\gamma_{n+T,T} - \gamma_{n,T}| \leqslant \rho(T)\ \rho_u(T) \ .$$

En particulier si $\rho(T) < 1$, comme

$$\gamma_{n,qT} = \sum_{i=0}^{q-1} \gamma_{n+iT,T} \ ,$$

on a par récurrence $|\gamma_{n,qT} - q\gamma_{n,T}| \leqslant \rho(T)\ \rho_u(T) < \rho_u(T)$, donc si $|q| = 1$, $|\gamma_{n,qT}| = \rho_u(T)$, c'est-à-dire $\rho_u(qT) = \rho_u(T)$.

6.4. - On a d'autre part

$$\begin{aligned}\gamma_{n,pT} &= \pi^n(\pi^{pT} - \mathcal{I})\ \mathcal{U}_0 \\ &= p\gamma_{n,T} + p\Big(\sum_{i=2}^{p-1} C_p^i/p\ \pi_T^{i-2}\Big)\, \pi^{n-m}\pi_T\, \pi^m \pi_T\, \mathcal{U}_0 + \pi^{n-m}\pi^{p-1}\pi^m \pi \mathcal{U}_0 \ ,\end{aligned}$$

donc si $\rho(T) < 1$ et toujours dans l'hypothèse $p > 2$, on a dès que n assez grand

$$|\gamma_{n,pT} - p\gamma_{n,T}| \leqslant \frac{1}{p}\,\rho_u(T)\ \rho(T) < \frac{1}{p}\,\rho_u(T) \ ,$$

c'est-à-dire $\rho_u(pT) = \frac{1}{p}\,\rho_u(T)$.

6.5. - Les résultats précédents montrent alors que :

si $\tau \not| T$, $\quad \rho_u(T) \geq |\det u_0|$,

si $\tau \mid T$, $\quad \rho_u(T) = |\frac{T}{\tau}|\, \rho_u(\tau)$ avec $\rho(\tau)\,|\det u_0| \leq \rho_u(\tau) \leq \rho(\tau)$,

quand $\rho_u(T) \neq 0$, on a $0 \leq n_u(T) \leq \dfrac{r \operatorname{Log} \rho_u(T)}{\operatorname{Log} \rho}$ (si $t < s$)

et $n_u(T) = 0$ si $t = s$.

Le cas où $p = 2$ serait un peu plus compliqué, la récurrence telle que dans 5.4 ou 6.4 ne pouvant se faire que si $\rho(T) < 1/p$.

6.6. - On peut voir aisément que τ ne dépend que du polynôme $\overline{P}$ associé à P dans le corps des restes (et même seulement de $\overline{Q}$, si $\overline{P} = \overline{Q} \times z^r$) et que l'on a

$$\begin{cases} \tau_{\overline{P \wedge Q}} = \tau_{\overline{P}} \wedge \tau_{\overline{Q}} , \\ \tau_{\overline{P^2}} = p\tau_{\overline{P}} . \end{cases}$$

Par ailleurs $\rho(\tau) = 0$ si et seulement si les racines de $P(z)$ de module 1 sont simples et racines de l'unité.