

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

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1963-1964, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

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

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 $n \geq 0$, u_n entier.

On dira que cette suite admet la période $T \pmod m$ si

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

1° Considérons le "vecteur" $U_n = (u_n, \dots, u_{n+s-1}) \pmod m$, il ne peut prendre 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 :

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

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

1.3. - Nous désignerons par $T(m)$ le plus petit entier $T \geq 1$ 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 :

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

1.4. - Alors u_n admet la période $T \pmod m \iff T(m) \mid T$.

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

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

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

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

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

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

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

Donc si $n \geq n_0(m)$, $u_{n+kT(m)+r} = u_{n+kT(m)} \pmod{m}$, 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 $0 \leq r < T(m)$, 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 :

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

En effet, $\forall n \geq \max(n_0(a), n_0(b))$, $u_{n+T(a) \wedge T(b)} = u_n \begin{cases} \pmod{a} \\ \pmod{b} \end{cases} \Rightarrow \pmod{a \wedge b}$
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 ≥ 1 ,

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

Si $\rho_u(T) > 0$, la valuation p -adique étant discrète, $\exists n$ tel que $|u_{n+T} - u_n|_p = \rho_u(T)$, 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 $\rho_u(T) \leq p^{-\lambda}$
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 $i = 1, \dots, s$, alors $p^k \mid u_n$ pourvu que $\frac{n}{s} \geq k$. Nous supposons donc que $\exists i$ tel que $p \nmid b_i$, nous pouvons alors définir t tel que : $1 \leq t \leq s$ et, quel que soit $\sigma > t$, $|b_\sigma|_p < 1$, mais $|b_t|_p = 1$.

Nous supposons 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 \mathbb{Q} :

$$u_n = \begin{pmatrix} u_n & \dots & u_{n+s-1} \\ u_{n+s-1} & \dots & u_{n+2s-2} \end{pmatrix}$$

et les vecteurs :

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

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

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

on aura : $U_{n+1} = \mathcal{M}U_n$ et $u_{n+1} = \mathcal{M}u_n$.

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

Donc, les valeurs propres de \mathcal{M} sont les racines du polynôme $P(z) = z^s - b_1 z^{s-1} \dots b_s$, il en résulte que le maximum de leurs valeurs absolues est égal à $\max |b_i|^{1/i} = 1$ (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 \mathbb{Q}_p en gardant les hypothèses $\max_{i=1, \dots, s} |b_i| = 1$ et $\max_{i=0, \dots, s-1} |u_i| = 1$ 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 $\alpha = (a_{ij})$ ($i = 0, \dots, s-1$, $j = 0, \dots, s-1$), nous notons $|\alpha|_p = \max_{i,j} |a_{ij}|_p$. On a alors trivialement $|\alpha| = 0 \iff \alpha = 0$

$$\begin{cases} |c\alpha| = |c| |\alpha|, \quad \forall c \text{ scalaire,} \\ |\alpha + \beta| \leq \max(|\alpha|, |\beta|). \end{cases}$$

2.2. - Soit $\alpha = (a_{ij})$, $\beta = (b_{ij})$, $c = (c_{ij}) = \alpha\beta$.

$$c_{ij} = \sum_k a_{ik} b_{kj}, \quad \text{d'où } |c_{ij}| \leq \max_k |a_{ik}| |b_{kj}| \leq \max_k |a_{ik}| \max_k |b_{kj}| \leq |\alpha| |\beta|$$

donc $|\alpha\beta| \leq |\alpha| |\beta|$.

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

Supposons α inversible, c'est-à-dire $\det \alpha \neq 0$, alors $\alpha^{-1} = (a_{ij}^{-1})$ avec $a_{ij}^{-1} = \frac{A_{ji}}{\det \alpha}$, A_{ji} étant le mineur de a_{ji} dans α ; 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 α .

On a donc

$$|A_{ji}| \leq |\alpha|^{s-1} \implies |\alpha^{-1}| \leq |\alpha|^{s-1} / |\det \alpha|,$$

mais alors

$$|\beta| = |\alpha^{-1} c| \leq |\alpha|^{s-1} |c| / |\det \alpha| \quad \text{soit } |c| \geq \frac{|\beta| |\det \alpha|}{|\alpha|^{s-1}}$$

(il est aisé de voir que l'on peut trouver α et β tel que l'on ait égalité).

On peut faire le même raisonnement en remplaçant α par β , et la majoration s'étend bien entendu au cas $\det \alpha = 0$, à condition que $\alpha \neq 0$. On a donc en supposant $\alpha \neq 0$, $\beta \neq 0$

$$\max \left(\frac{|\det \alpha|}{|\alpha|^s}, \frac{|\det \beta|}{|\beta|^s} \right) \leq \frac{|\alpha\beta|}{|\alpha| |\beta|} \leq 1.$$

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

3.1. - Soit α une matrice carrée. On a évidemment $|\alpha^n| \leq |\alpha|^n$, donc $\overline{\lim} |\alpha^n|^{1/n} \leq |\alpha|$. On posera

$$\|\alpha\| = \overline{\lim} |\alpha^n|^{1/n}, \text{ donc } \|\alpha\| \leq |\alpha|.$$

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

Supposons alors $\|\alpha\| \neq 0$, on ne peut avoir $|\alpha^v| = 0$ (sinon $\forall h \geq v$, $|\alpha^h| = 0$, d'où $\|\alpha\| = 0$). On peut écrire :

$$|\alpha^{m_k}| \leq |\alpha^v| |\alpha^n|^{u_k} \text{ d'où } |\alpha^{m_k}|^{1/m_k} \leq |\alpha^v|^{1/m_k} |\alpha^n|^{u_k/m_k}.$$

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

$$\|\alpha\| \leq |\alpha^n|^{1/n}.$$

Bien entendu cette égalité vaut aussi quand $\|\alpha\| = 0$.

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

On a donc : $(-1)^s \alpha^{n+s} + a_1 \alpha^{n+s-1} + \dots + a_s \alpha^n = 0$, α^n satisfait donc à une relation de récurrence linéaire à coefficients constants. Si $\theta_1, \dots, \theta_k$ sont les racines distinctes de $A(z)$ avec comme ordres de multiplicité h_1, \dots, h_k on peut écrire

$$\alpha^n = \sum_{i=1}^k \theta_i^n \rho_i(n),$$

où les $\rho_i(n)$ sont des matrices polynomiales :

$$\rho_i(n) = \sum_{j=0}^{h_i-1} n^j \rho_{i,j}.$$

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

$$|\alpha^n| \leq C\mu^n, \text{ d'où } \|\alpha\| \leq \mu.$$

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

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

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

O_n en déduit donc

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

et par conséquent pour $n \geq 1$,

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

4. Etude de $\pi^n \alpha$ où π 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 $\pi = \begin{pmatrix} 0 & 1 & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 & 1 \\ b_s & \dots & b_1 \end{pmatrix}$ on a évidemment $|\pi| = 1$, mais

comme $\max |b_i|^{1/i} = 1$, on entretient $\|\pi\| = |\pi| = 1$.

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

En outre si $\det \alpha \neq 0$, on a : $|\pi^n \alpha| \geq \frac{|\pi^n|}{|\alpha|^{s-1}} |\det \alpha| = \frac{|\det \alpha|}{|\alpha|^{s-1}}$.

La suite décroissante $|\pi^n \alpha|$ sera bornée inférieurement par un nombre positif, donc la valeur absolue étant discrète, la suite $|\pi^n \alpha|$ 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 π étant le polynôme $(-1)^s P(z)$, il en résulte que :

$\pi^n \alpha$ satisfait à la relation de récurrence :

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

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

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

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

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

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

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

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 $|\pi^{n_1} \alpha| \leq \rho |\pi^{n_1} \alpha|$. On en déduit alors par récurrence que :

$$\begin{aligned} &\text{ou bien } |\pi^m \alpha| \text{ est constante pour } m \geq n, \\ &\text{ou bien } |\pi^n \alpha| \leq \rho^{\lfloor n/r \rfloor} |\alpha|. \end{aligned}$$

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

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

5. Périodes de π^n .

5.1. - Nous posons $\pi_{n,T} = \pi^{n+T} - \pi^n = \pi^n \pi_T$, avec $\pi_T = \pi^T - \mathfrak{I}$, et nous posons $\rho(T) = \lim_{n \rightarrow \infty} |\pi_{n,T}|$, 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 :

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

5.2. - L'ensemble des T , tels que $\rho(T) < 1$, est constitué par les multiples d'un même nombre τ . Nous posons $\tau = \min_{\rho(T) < 1} T$ (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

$$\pi_{n,qT} = (\pi^{n+qT} - \pi^n = \pi^n(\pi^{qT} - s) = \pi^n((s + \pi_T)^q - s) = \pi^n \left(\sum_{i=1}^q C_q^i \pi_T^i \right)$$

d'où

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

π et π_T sont commutables, on a donc, si n est assez grand et $i \geq 2$:

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

donc $|\pi_{n,qT} - q\pi_{n,T}| \leq \rho(T)^2$, 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

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

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

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

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

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

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 $\overline{\pi}$ la matrice associée à π dans le corps des restes. Celui-ci étant fini $\overline{\pi}^n$ ne peut prendre qu'un nombre fini de valeurs, donc (principe des tiroirs) il existe n et T tels que $\overline{\pi}^{n+T} = \overline{\pi}^n$. Il en résulte $|\pi^{n+T} - \pi^n| < 1$, donc $\rho(T) < 1$, ce qui prouve l'existence de τ . On peut alors résumer les résultats précédents par :

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

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 $\det u_0 \neq 0$. Si nous posons alors

$$y_{n,T} = u_{n+T} - u_n = \pi_{b,T} u_0 ,$$

d'où $|y_{n,T}| \leq |y_{n,T}|$, donc : $|y_{n,T}| = |u_{n+T} - u_n|$. On a $\rho_u(T) = \lim_{n \rightarrow \infty} |y_{n,T}|$, donc on a la majoration $\rho(T) |\det u_0| \leq \rho_u(T) \leq \rho(T)$ (on a supposé $|\det u_0| = 1$) .

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

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

donc les T tels que $\rho_u(T) \leq x$ sont les multiples du plus petit d'entre eux.

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

$$y_{n+T,T} - y_{n,T} = |\pi^{m+T} - \pi^m| y_{n-m,T} ,$$

donc dès que n assez grand :

$$|y_{n+T,T} - y_{n,T}| \leq \rho(T) \rho_u(T) .$$

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

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

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

6.4. - On a d'autre part

$$\begin{aligned} y_{n,pT} &= \pi^n (\pi^{pT} - \mathfrak{J}) u_0 \\ &= p y_{n,T} + p \left(\sum_{i=2}^{p-1} C_{p/p}^i \pi_T^{i-2} \right) \pi^{n-m} \pi_T^m \pi_T^m u_0 + \pi^{n-m} \pi^{p-1} \pi^m \pi u_0 , \end{aligned}$$

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

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

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

6.5. - Les résultats précédents montrent alors que :

$$\text{si } \tau \nmid T, \quad \rho_u(T) \geq |\det u_0|,$$

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

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

$$\text{et } n_u(T) = 0 \quad \text{si } t = s.$$

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 \bar{P} associé à P dans le corps des restes (et même seulement de \bar{Q} , si $\bar{P} = \bar{Q} \times z^r$) et que l'on a

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

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