DANIEL BARSKY

Nombres de Bell et analyse p-adique

Groupe de travail d'analyse ultramétrique, tome 3, nº 1 (1975-1976), exp. nº 11, p. 1-10
<http://www.numdam.org/item?id=GAU_1975-1976__3_1_A7_0>

NOMBRES DE BELL ET ANALYSE p-ADIQUE

par Daniel BARSKY

Résumé. - On montre que la fonction génératrice des nombres de Bell est, pour tout nombre premier p, un élément analytique, au sens de KRASNER, sur un quasi-connexe de $\underset{\sim}{C}_p$. Ce résultat est équivalent, d'après le théorème de Mittag-Loeffler p-adique, à des congruences entre nombres de Bell. On retrouve ainsi des résultats de CARLITZ, et on généralise des résultats de RADOUX. La méthode utilisée est une interprétation p-adique de la méthode de KUMMER, et elle se généralise aisément.

Introduction. - Le n-ième nombre de Bell, P_n, est le nombre de partitions d'un ensemble à n éléments ou, autrement dit, P_n est le nombre de relations d'équivalence distinctes sur un ensemble à n éléments. De la définition précédente, on déduit facilement que les nombres de Bell vérifient la relation de récurrence [7] :

$$P_{n+1} = \sum_{k=0}^{n} \binom{n}{k} P_k .$$

Les nombres de Bell ont donc pour fonction génératrice exponentielle [7] :

$$\tilde{F}(X) = \sum_{n\geq 0} P_n \frac{X^n}{n!} = \exp(e^X - 1) ,$$

on a posé $P_0 = 1$.

Nous allons montrer que la fonction génératrice des nombres de Bell,

$$F(X) = \sum_{n\geq 0} P_n X^n ,$$

est, pour tout nombre premier p, un élément analytique p-adique [1] sur le quasi connexe

$$\mathcal{C}_p = \underset{\sim}{C}_p - \bigcup_{i=1}^{p} B(\zeta_i , 1^-)$$

de $\underset{\sim}{C}_p$, où ζ_i est une racine du polynôme $X^p + X^{p-1} - 1$. Ceci nous permettra de préciser, grâce au théorème de Mittag-Loeffler p-adique [1] ou [14], des congruences démontrées par RADOUX [13], et de retrouver celles démontrées par CARLITZ [6] par une autre voie. On montrera que, si $k(p) = (p^p - 1)/(p - 1)$, on a, pour p premier impair,

$$P_{n+k(p)p^{h-1}} \equiv P_n \mod(p^h) , \qquad h \geq 1 ,$$

et pour $p = 2$,

$$P_{n+k(2)} \equiv P_n \mod(2) , \qquad P_{n+k(2)2^h} \equiv P_n \mod(2^h) , \qquad h \geq 1 .$$

Autrement dit, sur une classe modulo $k(p)$, la suite $n \to P_n$ est la restriction à $\underset{\sim}{N}$ d'une fonction lipschitzienne de $\underset{\sim}{Z}_p$ dans $\underset{\sim}{C}_p$. On verra s'introduire de façon très naturelle le polynôme $X^p + X^{p-1} - 1$ dont le rôle avait été remarqué par RADOUX [13]. On obtient ainsi une interpétation en termes de singularités d'éléments analytiques p-adiques de la méthode de KUMMER [10].

La méthode décrite ici se généralise aisément ; en particulier, elle s'applique aux nombres de Bernoulli [4] pour lesquels elle permet de retrouver la théorie de KUBOTA et LEOPOLDT [8] et les congruences classiques entre nombres de Bernoulli ; elle permet aussi de retrouver des résultats de KATZ [9] sur les nombres de Hurwitz [5].

Notations. - Soit p un nombre premier, $\underset{\sim}{N}$, $\underset{\sim}{Z}$, $\underset{\sim}{Z}_p$, $\underset{\sim}{Q}_p$, $\underset{\sim}{C}_p$ ont leur signification habituelle [1]. La valeur absolue sur $\underset{\sim}{Z}_p$, $\underset{\sim}{Q}_p$, $\underset{\sim}{C}_p$, notée $| \; |$, est normalisée par $|p| = p^{-1}$, $\mathcal{O}_p$ est l'anneau des entiers de $\underset{\sim}{C}_p$. Les lettres ε et ρ désignent des nombres réels positifs. Si $a \in \underset{\sim}{C}_p$, on note

$$B(a , \rho^+) = \{X \in \underset{\sim}{C}_p \; ; \; |X - a| \leq \rho\}$$

(respectivement $B(a , \rho^-) = \{X \in \underset{\sim}{C}_p \; ; \; |X - a| < \rho\}$) la boule fermée (resp. ouverte) de centre a et de rayon ρ. Si $q = p^f$ ($f \in \underset{\sim}{N} - \{0\}$), on note $\underset{\sim}{F}_q$ le corps à q éléments, et $\overline{\underset{\sim}{F}}_p$ la clôture algébrique de $\underset{\sim}{F}_p$, donc de $\underset{\sim}{F}_q$. Si $a \in \mathcal{O}_p$, on note $\bar{a}$ l'image de a dans le corps résiduel de $\underset{\sim}{C}_p$ [1]. On note

$$\binom{x}{n} = \frac{x(x-1) \dots (x-n+1)}{n!} .$$

Rappelons que, si $B \subset \underset{\sim}{C}_p$, un élément analytique sur B est la limite uniforme sur B d'une suite de fractions rationnelles de $\underset{\sim}{C}_p(X)$ sans pôles dans B [1]. Si F est une fonction définie sur B, à valeurs dans $\underset{\sim}{C}_p$, on note

$$\|F\|_B = \sup_{X \in B} |F(X)| .$$

Enfin $H(B)$ (resp. $H_0(B)$) désigne l'espace de Banach des éléments analytiques sur B (resp. nuls à l'infini si B est non borné) muni de la norme $\| \; \|_B$ [1].

1. Transformation de Laplace formelle.

Nous allons définir une transformation sur $\underset{\sim}{C}_p[[X]]$ qui peut être considérée comme l'analogue formel de la transformation de Laplace classique. Rappelons que, si

$$f(X) = \sum_{n \geq 0} a_n X^n \quad \text{et} \quad g(X) = \sum_{n \geq 0} b_n X^n$$

appartiennent à $\underset{\sim}{C}_p[[X]]$, le produit de Hadamard $f \odot g$ de f et g défini par

$$f \odot g(X) = \sum_{n \geq 0} a_n b_n X^n .$$

Soit alors $g(X) = \sum_{n \geq 0} n! \, X^n$. On posera, si

$$F(X) = \sum_{n \geq 0} a_n \frac{X^n}{n!} \in \underset{\sim}{C}_p[[X]] ,$$

$$\mathfrak{L}F = g \odot F = \sum_{n \geq 0} a_n X^n .$$

On remarque $\mathcal{L}e^{kX} = (1 - kX)^{-1}$, $\mathcal{L}(XF) = X \frac{d}{dX}(X(\mathcal{L}F))$. L'application $\mathcal{L}$ est continue pour la topologie X-adique sur $\underset{\sim}{C}_p[[X]]$ et linéaire.

2. Fonction génératrice des nombres de Bell.

On a vu dans l'introduction que, si P_n est le n-ième nombre de Bell ($P_0 = 1$) , alors $\sum_{n\geq 0} P_n \frac{X^n}{n!} = \exp(e^X - 1)$. Or $\exp(e^X - 1) = \sum_{n\geq 0} (e^X - 1)^n/n!$, la série du second membre converge X-adiquement. Remarquons que

$$\mathcal{L}(\exp(e^X - 1)) = \sum_{n\geq 0} P_n X^n = F(X)$$

est la série génératrice des nombres de Bell. Donc

$$F(X) = \mathcal{L}\left(\sum_{n\geq 0} \frac{(e^X - 1)^n}{n!}\right) = \sum_{n\geq 0} \frac{\mathcal{L}(e^X - 1)^n}{n!}$$

car le second membre converge X-adiquement et, d'après une remarque précédente,

$$F(X) = \sum_{n\geq 0} \frac{1}{n!} \sum_{k=0}^{n} \frac{(-1)^{n-k}}{1 - kX} \binom{n}{k} ,$$

finalement il vient

$$F(X) = \sum_{n\geq 0} P_n X^n = \sum_{n\geq 0} \frac{X^n}{(1 - X) \dots (1 - nX)} .$$

3. Etude de la fonction génératrice des nombres de Bell.

Soit p un nombre premier. Nous allons étudier les propriétés analytiques de F dans $\underset{\sim}{C}_p$. Il est clair, puisque $P_n \in \underset{\sim}{N}$, que la série $\sum_{n\geq 0} P_n X^n$ converge simplement sur la boule $B(0 , 1^-)$ de $\underset{\sim}{C}_p$ et qu'il en est de même de

$$\sum_{n\geq 0} X^n/((1 - X) \dots (1 - nX)),$$

car, si $|X| < 1$, $|X^n/((1 - X) \dots (1 - nX))| = |X^n|$. Or on a l'égalité suivante modulo $p^h \mathcal{O}_p[[X]]$:

$$\sum_{n\geq 0} \frac{X^n}{(1 - X)\dots(1 - nX)} = \sum_{n=0}^{p^h-1} \frac{X^n}{(1 - X)\dots(1 - nX)} \sum_{k\geq 0} \frac{X^{kp^h}}{((1 - X)\dots(1 - (p^h - 1)X))^k}$$

$$F(X) = \sum_{n=0}^{p^h-1} \frac{X^n}{(1 - X)\dots(1 - nX)} \left(1 - \frac{X^{p^h}}{(1 - X)\dots(1 - (p^h - 1)X)}\right)^{-1} \mod(p^h \mathcal{O}_p[[X]]) ,$$

et par conséquent on a

$$F(X) = \frac{\sum_{n=0}^{p^h-1} X^n(1 - (n + 1)X)\dots(1 - (p^h - 1)X)}{(1 - X)\dots(1 - (p^h - 1)X) - X^{p^h}} \text{ modulo } p^h \mathcal{O}_p[[X]] .$$

Appelons $F_{h,p}(X)$ le second membre de l'égalité précédente, $F_{h,p}$ est une fraction rationnelle de $\underset{\sim}{C}_p(X)$ sans pôles dans $B(0 , 1^-)$ comme le montre le polygône de Newton [1] du dénominateur, $D_{h,p}(X)$, de $F_{h,p}(X)$. On a donc

$$\|F - F_{h,p}\|_{B(0,1^-)} \leq p^{-h} .$$

PROPOSITION 1. - Pour tout nombre premier p, la fonction génératrice des nombres de Bell, $F(X) = \sum_{n\geq 0} P_n X^n$, est un élément analytique p-adique, au sens de KRASNER, sur $B(0, 1^-) \subset \underset{\sim}{C}_p$.

C'est immédiat d'après l'inégalité $\|F - F_{h,p}\|_{(B(0,1^-))} \leq p^{-h}$ et la définition d'un élément analytique [1].

COROLLAIRE. - La suite $(P_n)_{n\geq 0}$ est, pour tout nombre premier p, presque périodique au sens de ROBBA [14], c'est-à-dire que, pour tout $\varepsilon > 0$, il existe $n_0 \in \underset{\sim}{N}$ et $T \in \underset{\sim}{N} - \{0\}$ tels que, pour $n \geq n_0$, $|P_n - P_{n+T}| \leq \varepsilon$; autrement dit si $\varepsilon \leq p^{-h}$, $P_n \equiv P_{n+T} \mod(p^h)$.

Nous allons étudier maintenant un peu plus finement $F_{h,p}(X)$ et sa convergence vers $F(X)$, et nous en déduirons des congruences précises pour les P_n. Nous allons localiser les zéros de $D_{h,p}(X) = (1 - X)\dots(1 - (p^h - 1)X) - X^{p^h}$ dans $\underset{\sim}{C}_p$.

LEMME 1.

$$D_{h,p}(X) = (D_{1,p}(X))^{p^{h-1}} \mod(p\underset{\sim}{Z}[X]) \ \ \underline{\text{et}}\ \ D_{1,p}(X) = 1 - X^{p-1} - X^p \mod(p\underset{\sim}{Z}[X]) .$$

En effet,

$$\begin{aligned} D_{h,p}(X) &= ((1 - X)\dots(1 - (p - 1)X))^{p^{h-1}} - X^{p^h} \mod(p\underset{\sim}{Z}[X]) \\ &= ((1 - X)\dots(1 - (p - 1)X) - X^p)^{p^{h-1}} \mod(p\underset{\sim}{Z}[X]) \\ &= (D_{1,p}(X))^{p^{h-1}} \mod(p\underset{\sim}{Z}[X]) . \end{aligned}$$

Il est clair que $D_{1,p}(X) = 1 - X^{p-1} - X^p \mod(p\underset{\sim}{Z}[X])$. Posons

$$D_p(X) = 1 - X^{p-1} - X^p .$$

Le polynôme $D_p(X)$ est irréductible sur $\underset{\sim}{F}_p$ car $|D_p(n)| = 1$ pour tout $n \in \underset{\sim}{N}$. Si η_i est une racine de $D_p(X)$ dans $\overline{\underset{\sim}{F}}_p$, l'extension $\underset{\sim}{F}_p[\eta_i]$ est galoisienne sur $\underset{\sim}{F}_p$ car les autres racines de $D_p(X)$ dans $\overline{\underset{\sim}{F}}_p$ sont $\eta_i + \overline{1}, \dots, \eta_i + \overline{p-1}$. Un générateur du groupe de Galois de $\underset{\sim}{F}_p[\eta_i]$ sur $\underset{\sim}{F}_p$ est le Frobénius

$$\sigma : t \to t^p .$$

Comme la norme de η_i sur $\underset{\sim}{F}_p$ est $\overline{1}$, on en déduit que, si

$$k(p) = 1 + p + \dots + p^{p-1} = (p^p - 1)/(p - 1) ,$$

on a $\eta_i^{k(p)} = 1$ (cf. aussi [13]). Donc, dans $\underset{\sim}{C}_p$, les racines $\xi_{i,1}$ $(1 \leq i \leq p)$ de $D_{1,p}(X)$ vérifient $|\xi_{i,p}^{k(p)} - 1| \leq p^{-1}$. Soit ζ_i le représentant de Teichmüller de $\xi_{i,1}$ (c'est-à-dire que ζ_i est une racine primitive de l'unité d'ordre premier à p contenue dans $\underset{\sim}{C}_p$, telle que $|\zeta_i - \xi_{i,1}| < 1$). On a

$$|\xi_{i,1} - \zeta_i| \leq p^{-1} ,$$

car l'extension $\underset{\sim}{Q}_p[\xi_{i,1}]$ est non ramifiée sur $\underset{\sim}{Q}_p$ [1]. Nous noterons

$\xi_{i,h}$ $(1 \leqslant i \leqslant p^h)$ les racines de $D_{h,p}(X)$ dans $\underset{\sim}{C}_p$. Le lemme de Hensel [1], appliqué à $D_{h,p}(X)$, montre que ses racines se groupent en p-classes contenant chacunes exactement p^{h-1} racines et deux racines d'une même classe vérifient $|\xi_{i,h} - \xi_{j,h}| < 1$, à chaque classe correspond une racine $\xi_{i,1}$ de $D_{1,p}(X)$ telle que $|\xi_{i,1} - \xi_{i',h}| < 1$ pour toute $\xi_{i',h}$ dans la classe. D'après le lemme 1 et la formule $ef = n$, reliant la ramification, le degré résiduel et le degré d'une extension finie de $\underset{\sim}{Q}_p$, on a $|\xi_{i,h} - \zeta_j| \leqslant p^{-r(h-1)}$, où ζ_j est le représentant de Teichmüller de $\xi_{i,h}$ et $r(h-1) = p^{-h+1}$. On posera désormais $\rho_h = p^{-r(h)}$.

PROPOSITION 2. - $F_{h,p}(X)$ <u>est un élément analytique nul à l'infini sur le quasi-connexe</u>

$$\mathbb{D}_{h,p} = \underset{\sim}{C}_p - \bigcup_{i=1}^{p} B(\zeta_i , \rho_{h-1}^{+}) , \text{ où } \rho_h = p^{-r(h)} , \quad r(h) = p^{-h} ,$$

<u>et</u> ζ_i <u>est le représentant de Teichmüller d'une racine de</u> $D_p(X) = 1 - X^{p-1} - X^p$.

<u>Pour tout nombre premier</u> p , $F(X)$ <u>est la restriction à</u> $B(0 , 1^-) \subset \underset{\sim}{C}_p$ <u>d'un élément analytique nul à l'infini sur le quasi-connexe</u> $\underset{\sim}{C}_p - \bigcup_{i=1}^{p} B(\zeta_i , 1^-)$.

La première partie de la proposition est évidente puisque $F_{h,p}(X)$ est une fraction rationnelle sans pôles dans $\mathbb{D}_{h,p}$, et le degré du numérateur est inférieur à celui du dénominateur. On a, pour $h \geqslant 2$, $\|F_{h,p} - F_{h-1,p}\|_{B(0,1^-)} \leqslant p^{-h+1}$. Comme, pour tout $X \in B(0 , 1^-)$, $|D_{h,p}(X)| = |D_{h-1,p}(X)| = 1$, on en déduit que, si $N_{h,p}(X)$ est le numérateur de $F_{h,p}(X)$,

$$\|N_{h,p} D_{h-1,p} - N_{h-1,p} D_{h,p}\|_{B(0,1^-)} \leqslant p^{-h+1}$$

et donc, d'après les inégalités de Cauchy [1],

$$N_{h-1,p}(X) D_{h,p}(X) - N_{h,p}(X) D_{h-1,p}(X) \in p^{h-1} \underset{\sim}{Z}[X] .$$

Il est immédiat, alors, que la suite $h \to F_{h,p}(X)$ est une suite de Cauchy, uniformément pour $X \in \underset{\sim}{C}_p - \bigcup_{i=1}^{p} B(\zeta_i , 1^-)$. Donc $F(X)$ peut être prolongée de manière unique [14] en un élément analytique nul à l'infini, sur le quasi-connexe $\underset{\sim}{C}_p - \bigcup_{i=1}^{p} B(\zeta_i , 1^-)$, que l'on notera encore $F(X)$.

COROLLAIRE. - <u>Pour tout nombre premier</u> p <u>et pour tout entier</u> h , <u>il existe</u> $n(h) \in \underset{\sim}{N}$ <u>tel que</u>, <u>pour tout</u> $n \in \underset{\sim}{N}$,

$$P_n \equiv P_{n+k(p)p^{n(h)}} \bmod(p^h) , \text{ où } k(p) = (p^p - 1)(p - 1)^{-1} .$$

C'est une conséquence immédiate du fait que $F(X)$ est un élément analytique sur $\underset{\sim}{C}_p - \bigcup_{i=1}^{p} B(\zeta_i , 1^-)$, nul à l'infini.

4. <u>Congruences entre nombres de Bell.</u>

Nous allons rendre effective l'expression de $n(h)$ en fonction de h .

Soit p un nombre premier fixé pour tout le paragraphe, on posera donc

$F_h(X) = F_{h,p}(X)$, $\mathcal{D}_h = \mathcal{D}_{h,p}$; $k(p) = \frac{p^p - 1}{p - 1}$, $r(h) = p^{-h}$, $\rho_h = p^{-r(h)}$.

LEMME 2. - Si $F_1(X) = \sum_{n\geq 0} P_{n,1} X^n$, on a

$$P_{n+k(p)p^{j-1},1} \equiv P_{n,1} \mod(p^j) , \qquad j \in \mathbb{N} - \{0\} .$$

En effet, F_1 est un élément analytique nul à l'infini sur $\mathcal{D}_1$. On peut donc poser, d'après le théorème de Mittag-Loeffler p-adique ([1] ou [14]),

$$F_1 = \sum_{i=1}^{p} F_{i,1} \text{ , où } F_{i,1} \in H_0(\mathbb{C}_p - B(\zeta_i , \rho_0^+)) .$$

En fait, $F_{i,1}(X) = \lambda_{i,1}(1 - \xi_{i,1}^{-1} X)^{-1}$, avec $|\lambda_{i,1}| \leq 1$, d'après Mittag-Loeffler. Donc si $F_{i,1}(X) = \sum_{n\geq 0} P_{n,i,1} X^n$, on a $P_{n,i,1} = \lambda_{i,1} \xi_{i,1}^{-n}$ et, par conséquent,

$$P_{n+k(p)p^{j-1},i,1} - P_{n,i,1} = \lambda_{i,1}(\xi_{i,1}^{-n-k(p)p^{j-1}} - \xi_{i,1}^{-n}) .$$

On en déduit que

$$|P_{n+k(p)p^{j-1},i,1} - P_{n,i,1}| \leq |\lambda_{i,1}| |\xi_{i,1}^{-n-p^{j-1}k(p)} - \xi_{i,1}^{-n}| \leq p^{-j} .$$

Donc comme $P_{n,1} = \sum_{i=1}^{p} P_{n,i,1}$,

$$|P_{n+k(p)p^{j-1},1} - P_{n,1}| \leq p^{-j} .$$

Ce résultat est équivalent à l'énoncé du lemme puisque $P_{n,1} \in \mathbb{Z}$.

LEMME 3. - Si $F_h(X) = \sum_{n\geq 0} P_{n,h} X^n$, on a, pour $j \geq 0$ et $h \geq 2$,

$$P_{n+k(p)p^{j-1},h} \equiv P_{n,h} \mod(p^j) \text{ si } p > 2 ,$$

$$P_{n+k(2)2^j,h} \equiv P_{n,h} \mod(2^j) .$$

On raisonne par récurrence sur h pour j fixé. Le lemme est vrai pour $h = 1$ (lemme 2), supposons-le vrai pour $2 , 3 , \ldots , h - 1$. On a

$$F_h(X) = F_h(X) - F_{h-1}(X) + F_{h-1}(X)) \text{ et } \|F_h - F_{h-1}\|_{\mathcal{D}_h} \leq p^{-h+2+p^{-1}} ,$$

car

$$|D_h(X) D_{h-1}(X)| \geq p^{-1-p^{-1}} \quad (D_h(X) = D_{h,p}(X)) \quad \text{sur } B(\zeta_i , 1^-) - B(\zeta_i , \rho_{h-1}^+)$$

et

$$|F_h(X) - F_{h-1}(X)| \leq p^{-h+1} \quad \text{sur } \mathbb{C}_p - \cup_{i=1}^{p} B(\zeta_i , 1^-) .$$

Posons $G_h(X) = F_h(X) - F_{h-1}(X)$, $G_h \in H_0(\mathcal{D}_h)$. On peut donc, d'après le théorème de Mittag-Loeffler, décomposer G_h en ses parties singulières relatives aux trous de $\mathbb{D}_h$,

$$\mathbb{G}_h(X) = \sum_{i=1}^p G_{i,h}(X) \quad \text{où} \quad G_{i,h} \in H_0(\underset{\sim}{C}_p - B(\zeta_i , \rho_{h-1}^+)) .$$

Posons

$$G_{i,h}(X) = \sum_{k\geq 1} \lambda_{i,h,k}(1 - X\zeta_i^{-1})^{-k} \quad \text{pour} \quad X \in \underset{\sim}{C}_p - B(\zeta_i , \rho_{h-1}^+)$$

et

$$G_{i,h}(X) = \sum_{n\geq 0} g_{i,h,n} X^n \quad \text{pour} \quad X \in B(0 , 1^-) .$$

On a $g_{i,h,n} = \sum_{k\geq 1} \lambda_{i,h,k} \zeta_i^{-k-n} \binom{n+k-1}{k-1}$. Le théorème de Mittag-Loeffler montre que $\sup_i \|G_{i,h}\|_{\underset{\sim}{C}_p - B(\zeta_i , \rho_{h-1}^+)} = \|\mathbb{G}_h\|_{\mathbb{D}_h}$ d'où l'on déduit que

$$|\lambda_{i,h,k}| \leq p^{-h+2+p^{-1}-kr(h-1)} .$$

On a donc d'après l'inégalité ultramétrique

$$|g_{i,h,n+k(p)p^{j-1}} - g_{i,h,n}|$$

$$\leq \sup_{k\geq 1}\{ |\lambda_{i,h,k}| \, |\zeta_i^{-k-n-k(p)^{j-1}} \binom{n+k(p)p^{j-1}+k-1}{k-1} - \zeta_i^{-k-n} \binom{n+k-1}{k-1}|\}$$

$$\leq \sup_{k\geq 1} \sup\{ |\lambda_{i,h,k}| \, |\zeta_i^{-k-n-k(p)p^{j-1}} - \zeta_i^{-k-n}| \, |\binom{n+k(p)p^{j-1}+k-1}{k-1}| ,$$

$$|\lambda_{i,h,k}| \, |\zeta_i^{-k-n}| \, |\binom{n+k(p)p^{j-1}+k-1}{k-1} - \binom{n+k-1}{k-1}|\} .$$

or ζ_i est une racine $k(p)$-ième de l'unité, puisque $|\xi_{i,1}^{k(p)} - 1| \leq p^{-1}$, et que ζ_i est le représentant de Teichmüller de $\xi_{i,1}$. Enfin,

$$|\binom{n+k(p)p^{j-1}+k-1}{k-1} - \binom{n+k-1}{k-1}| \leq \inf(1 , p^{-j+1+\ell(k-1)}) , \quad \text{où} \quad \ell(k-1) = [\frac{\log(k-1)}{\log(p)}]$$

(c'est-à-dire que $\ell(k-1)$ est le plus grand entier inférieur ou égal à $\frac{\log(k-1)}{\log(p)}$) (cf. [2]). Deux cas sont à envisager :

$$k - 1 < p^j \quad \text{et} \quad k - 1 \geq p^j .$$

Si $k - 1 \geq p^j$, alors

$$|\lambda_{i,h,k}| \leq p^{-h+2+p^{-1}-(p^j+1)r(h-1)} ,$$

or $h - 2 - (1/p) + ((p^j + 1)/p^{h-1}) > j - 1$ pour tout entier j, donc

$$|\lambda_{i,h,k}| < p^{-j+1} \quad \text{si} \quad k - 1 \geq p^j .$$

Si $k - 1 < p^j$, alors

$$|\lambda_{i,h,k}| \, |\binom{n+k(p)p^{j-1}+k-1}{k-1} - \binom{n+k-1}{k-1}| \leq p^{-s(k)} ,$$

où $s(k) = h-2-p^{-1}+kp^{-h+1}+j-1-\ell(k-1) \geqslant h-3-p^{-1}+kp^{-h+1}+j-\frac{\log(k-1)}{\log(p)}$.

Le minimum du dernier membre est atteint pour $k-1 = p^{h-1}/\log(p)$. Pour cette valeur de k, et compte tenu de la définition de $\ell(k-1)$, le premier membre vaut

$$s\left(\frac{p^{h-1}}{\log(p)}+1\right) = h-2+p^{-1}+(1/\log(p))+p^{-h+1}+j-1-h+2$$

$$= j-1-p^{-1}+(1/\log(p))+p^{-h+1} > j-1 \quad \text{si} \quad p>2,$$

si $p = 2$, alors

$$s\left(\frac{2^{h-1}}{\log(2)}+1\right) = h-2-2^{-1}+(\log(2))^{-1}+2^{-h+1}+j-1-h+1 > j-2 \quad (\text{si } h \geqslant 2).$$

Comme $\ell(k-1)$ garde la même valeur pour $p^r \leqslant k < p^{r+1}$, on en déduit que le minimum de $s(k)$ est atteint pour $k-1 = p^{h-2}$ si $p>2$ (resp. pour $k-1 = 2^{h-1}$ si $p=2$). Donc $s(k) > j-1$ si $p>2$ (resp. $s(k) > j-2$ si $p=2$). On a donc montré que

$$|g_{i,h,n+k(p)p^{j-1}} - g_{i,h,n}| < p^{-j+1} \quad \text{si} \quad p>2,$$

respectivement

$$|g_{i,h,n+k(2)2^{j-1}} - g_{i,h,n}| < 2^{-j+2} \quad (h \geqslant 2).$$

De ces inégalités, on tire, comme $P_{n,h} = P_{n,h-1} + \sum_{i=1}^{p} g_{i,h,n}$,

$$|P_{n+k(p)p^{j-1},h} - P_{n,h}| < p^{-j+1} \quad \text{si} \quad p>2,$$

respectivement

$$|P_{n+k(2)2^{j-1},h} - P_{n,h}| < 2^{-j+2} \quad (h \geqslant 2).$$

Or $P_{n,h} \in \underset{\sim}{Z}$, les inégalités précédentes entraînent alors

$$|P_{n+k(p)p^{j-1},h} - P_{n,h}| \leqslant p^{-j} \quad \text{si} \quad p>2,$$

respectivement

$$|P_{n+k(2)2^{j},h} - P_{n,h}| \leqslant 2^{-j} \quad (h \geqslant 2).$$

Le lemme 3 est démontré.

THÉORÈME. - Les nombres de Bell vérifient les congruences suivantes. On pose $k(p) = (p^p - 1)/(p-1)$ pour tout nombre premier p. Si p est un nombre premier impair,

$$P_{n+k(p)p^{h-1}} \equiv P_n \mod(p^h) \qquad (h \geqslant 1),$$

respectivement

$$P_{n+k(2)} \equiv P_n \mod(2) \quad \text{et} \quad P_{n+k(2)2^h} \equiv P_n \mod(2^h) \qquad (h \geqslant 2).$$

Pour montrer des congruences $\bmod(p^h)$ sur les P_n, il suffit de montrer les mêmes congruences sur les $P_{n,h}$, car $\|F - F_{h,p}\|_{B(0,1^-)} \leq p^{-h}$, ce qui entraîne, d'après les inégalités de Cauchy, pour tout $n \in \mathbb{N}$, $P_{n,h} \equiv P_n \bmod(p^h)$. Il suffit alors d'appliquer les lemmes 2 et 3.

6. Généralisation.

On peut généraliser un peu la proposition 1 en remarquant que, si p est un nombre premier,

$$F(X) = \sum_{n\geq 0} \frac{a_n X^n}{(1 - X) \ldots (1 - nX)}$$

est un élément analytique sur $B(0, 1^-) \subset \mathbb{C}_p$ toutes les fois que

$$G(T) = \sum_{n\geq 0} a_n T^n$$

en est un sur $B(0, 1^-) \subset \mathbb{C}_p$. La connaissance des singularités de G entraîne des informations sur celles de F et donc des congruences entre les coefficients de Taylor de F.

En particulier, cette méthode s'applique aux nombres de Bernoulli relatifs à un caractère, et permet de retrouver de manière simple les congruences classiques entre nombres de Bernoulli ainsi que la théorie de KUBOTA et LEOPOLDT (cf. [4]). Elle s'applique aussi aux nombres de Hurwitz (cf. [5]) et permet de retrouver des résultats de KATZ [9].

Remarque. — On peut avoir une connaissance précise sur la localisation des pôles de $F_{h,p}$. En particulier, on peut tracer le polygône de Newton de $D_{h,p}(X + \xi_{i,h})$ pour tout i et tout h. On peut, de plus, placer les racines de $D_{h,p}$ par rapport à celles de $D_{h-1,p}$. On peut montrer que, pour $1 \leq i \leq p^{h-2}$, il existe j tel que $1 \leq j \leq p^{h-1}$ et $|\xi_{i,h-1} - \xi_{j,h}| < p^{(p-1)^{-1}}$. Mais on n'obtient pas de congruences plus précises pour les P_n.

BIBLIOGRAPHIE

[1] AMICE (Y.). - Les nombres p-adiques. - Paris, Presses Universitaires de France, 1975 (Collection SUP, "le Mathématicien", 14).

[2] BARSKY (D.). - Fonctions k-lipschitziennes sur un anneau local et polynômes à valeurs entières, Bull. Soc. math. France, t. 101, 1973, p. 397-411.

[3] BARSKY (D.). - Analyse p-adique et nombre de Bell, C. R. Acad. Sc. Paris (à paraître).

[4] BARSKY (D.). - Fonction génératrice et congruences, Séminaire Delange-Pisot-Poitou : Théorie des nombres, 17e année, 1975/76, n° 21, 16 p.

[5] BARSKY (D.). - Congruences de coefficients de séries de Taylor, Groupe d'étude d'Analyse ultramétrique (Amice-Robba), 3e année, 1975/76, n° 17.

[6] CARLITZ (L.). - Congruences for generalized Bell and Stirling numbers, Duke math. J., t. 22, 1955, p. 193-205.

[7] COMTET (L.). - Analyse combinatoire, Vol 1 et 2. - Paris, Presses Universi-

taires de France, 1970 (Collection SUP, "le Mathématicien", 4 et 5).

[8] IWASAWA (K.). - Lectures on p-adic L-functions. - Princeton, Princeton University Press, 1972 (Annals of mathematical Studies, 74).

[9] KATZ (N. M.). - The congruences of Clausen-von Staudt and Kummer for Bernoulli-Hurwitz numbers, Math. Annalen, t. 216, 1975, p. 1-4.

[10] KUMMER (E. F.). - Über eine allgemeine Eigenschaft der rationalen Entwickelungscoëfficienten einer bestimmten Gattung analytischer Functionen, J. für die reine und ang. Math., t. 41, 1851, p. 368-372.

[11] LANG (S.). - Algebra. - Reading, Addison-Wesley, 1965.

[12] RADOUX (C.). - Nouvelles propriétés arithmétiques des nombres de Bell, Séminaire Delange-Pisot-Poitou : Théorie des nombres, 16e année, 1974/75, n° 22, 12 p.

[13] RADOUX (C.) - Nombres de Bell, modulo p premier et extensions de degré p de $\underset{\sim}{F}_p$, C. R. Acad. Sc. Paris, t. 281, 1975, Série A, p. 879-882.

[14] ROBBA (P.). - Fonctions analytiques sur les corps values ultramétriques complets, Astérisque n° 10, 1973, p. 108-218.

(Texte reçu le 1er juillet 1976)

Daniel BARSKY
Département de Mathématiques
Université de Paris-7
Tour 45-55, 5e étage
2 place Jussieu
75221 PARIS CEDEX 05