*Daniel BARSKY*
Université Paris VII, U.E.R. de Mathématiques
Tour 45-55, 5° étage
2, place Jussieu
75251 PARIS Cedex 05

# ANALYSE p-ADIQUE ET SUITES CLASSIQUES DE NOMBRES

## RESUME

Soit $(a_n)_{n\in\mathbb{N}}$ une suite de nombres rationnels (ou plus généralement de nombres algébriques sur $\mathbb{Q}$) et soit p un nombre premier. On montre que la propriété pour la suite $(a_n)_{n\in\mathbb{N}}$ d'être pour tout $h \in \mathbb{N}$ périodique modulo $p^h$ à partir d'un certain rang (ou de manière équivalente, que la suite $(a_n)_{n\in\mathbb{N}}$ satisfasse pour tout $h \in \mathbb{N}$ une récurrence linéaire modulo $p^h$ à partir d'un certain rang) est équivalente à des propriétés de prolongeabilité analytique p-adique de la série génératrice $Y = \sum_{n\geq 0} a_n X^n$ sur certains sous-ensembles de $\mathbb{C}_p$ (complété de la clôture algébrique de $\mathbb{Q}_p$). On indique comment la géométrie du domaine sur lequel Y est un élément analytique p-adique (i.e. sur lequel Y est prolongeable analytiquement p-adiquement) permet de prévoir a priori les congruences satisfaites par les $a_n$. On montre ensuite que, si la fonction génératrice exponentielle $\tilde{Y} = \sum_{n\geq 0} a_n \frac{X^n}{n!}$ satisfait certaines propriétés fonctionnelles, alors $Y = \sum_{n\geq 0} a_n X^n$ est un élément analytique p-adique sur un domaine de $\mathbb{C}_p$ contenant $D(0,1)^-$, le disque ouvert de centre 0 et de rayon 1 de $\mathbb{C}_p$; ceci est le cas par exemple si $\tilde{Y}$ satisfait une équation différentielle algébrique et si $a_n \in \mathbb{Z}$ ou si la série réciproque de $\tilde{Y}$ possède certaines propriétés.

On montre ensuite, sur des suites classiques de nombres, comment on peut obtenir des résultats effectifs. Pour cela, on est amené à introduire la transformation de Laplace formelle $\mathcal{L}$ qui à la série de Taylor $\tilde{Y} = \sum_{n\geq 0} a_n \frac{X^n}{n!}$ associe la série de Taylor $Y = \sum_{n\geq 0} a_n X^n$ et à indiquer quelques propriétés évidentes. Enfin, on indique pour terminer le lien qui existe entre les congruences de type Cartier satisfaites par une suite d'entiers $(e_n)_{n\geq 1}$ (i.e. pour tout $n \geq 1$, $e_{np^h} \equiv e_{np^{h-1}} \mod(p^h)$) et les congruences de type Kummer satisfaites par les coefficients $a_n$ de la série

$\tilde{Y} = \sum_{n>0} a_n \frac{X^n}{n!}$ réciproque de la série $X = \sum_{n\geq 1} \frac{e_n}{n} Y^n$.

## I.- ANALYSE p-ADIQUE

Soit p un nombre premier et soit $(a_n)_{n\in\mathbb{N}}$ une suite de nombres rationnels (resp. de nombres algébriques). On s'intéressse aux propriétés de congruences modulo $p^h$ ($h\in\mathbb{N}$) entre les $a_n$. Il est clair alors que l'analyse p-adique doit pouvoir apporter au moins un langage agréable pour traiter ce genre de questions.

Rappelons les généralités suivantes (cf. [1] ou [20]). Si $a/b = p^\alpha\, a'/b' \in \mathbb{Q}$ avec $(a',p) = (b',p) = 1$, on pose $|a/b| = p^{-\alpha}$. Avec cette définition $\mathbb{Q}$ est muni d'une valeur absolue ultramétrique, i.e. $|\frac{a}{b}+\frac{c}{d}| \leq \max(|\frac{a}{b}|, |\frac{c}{d}|)$. On peut compléter $\mathbb{Q}$ pour cette valeur absolue, on obtient ainsi $\mathbb{Q}_p$ le corps des nombres p-adiques. Dans toute la suite $|.|$ désignera une valeur absolue non archimédienne prolongeant la valeur absolue p-adique sur $\mathbb{Q}$. Le problème de départ se traduit donc aisément en terme de cette valeur absolue. On définit $\mathbb{Z}_p = \{x\in\mathbb{Q}_p\ ;\ |x|\leq 1\}$. Il est facile de voir que $\mathbb{Z}_p$ est un anneau, complété de $\mathbb{Z}$ pour la valeur absolue p-adique, et que $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^h\mathbb{Z}$ (cf. [1] ou [20]). On définit de la manière habituelle la notion de fonction continue sur $M\subset\mathbb{Q}_p$ à valeur dans $\mathbb{Q}_p$, on note $\mathcal{C}(M,\mathbb{Q}_p)$ l'ensemble de ces fonctions. On a le théorème important suivant :

THEOREME 1.- (Mahler [22]). *Soit $\mathcal{C}(\mathbb{Z}_p,\mathbb{Q}_p)$ l'espace des fonctions continues de $\mathbb{Z}_p$ dans $\mathbb{Q}_p$. Posons $\binom{x}{o} = 1$ et $\binom{x}{n} = \frac{x(x-1)\ldots(x-n+1)}{n!}$. Les deux propriétés suivantes sont équivalentes :*

*i)* $f\in\mathcal{C}(\mathbb{Z}_p,\mathbb{Q}_p)$

*ii) Il existe une unique suite $(\lambda_n(f))_{n\in\mathbb{N}}$ d'éléments de $\mathbb{Q}_p$ telle que $\lim_{n\to\infty} |\lambda_n(f)| = 0$ et, pour tout $x\in\mathbb{Z}_p$, $f(x) = \sum_{n\geq 0} \lambda_n(f)\binom{x}{n}$ la convergence étant uniforme sur $\mathbb{Z}_p$. En outre $\lambda_n(f) = \sum_{k=0}^{n} (-1)^{n-k}\binom{n}{k} f(k)$ et*

$$\|f\|_{\mathbb{Z}_p} = \mathrm{Sup}_{x\in\mathbb{Z}_p} |f(x)| = \mathrm{Sup}_{n\geq 0} |\lambda_n(f)|.$$

□ Nous donnons ici la preuve de Bojanic [7]. $\mathbb{Z}_p$ est compact, donc f est uniformément continue sur $\mathbb{Z}_p$. La seule chose à montrer est que $\lim_{n\to\infty} |\lambda_n(f)| = 0$ si $\lambda_n(f)$ est défini comme dans le théorème, car il est clair que, pour tout $m\in\mathbb{N}$,

$f(m) = \sum_{n\geq 0} \lambda_n(f)\binom{m}{n}$ et on conclura grâce à la densité de $\mathbb{N}$ dans $\mathbb{Z}_p$.

Pour h assez grand, on a $|\Delta^{p^h} f(x)| < 1$ car $|\binom{p^h}{k}| < 1$ si $k \neq 0$ ou $p^h$ et $|f(x+p^h) - f(x)| < 1$ où $\Delta^{p^h} f(x) = \sum_{k=0}^{p^h} (-1)^{p^h - k}\binom{p^h}{k} f(x+k)$. Donc pour tout $n \geq p^h$ on a $|\Delta^n f(0)| < 1$ car $\Delta^{m+n} f(x) = \Delta^m(\Delta^n f(x))$. Or si $n_1 = p^h$, $\Delta^{n_1} f(x) \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$. Donc il existe $n_2 = p^{h'}$ tel que : $|\Delta^{n_2}(\Delta^{n_1} f(x))| \leq \{|\Delta^{n_1}(f(x+n_2)) - \Delta^{n_1}(f(x))|,$ $p^{-1}|\Delta^{n_1} f(x)|\} \leq p^{-2}$. Et donc, si $n \geq n_1 + n_2$, $|\Delta^n f(x)| \leq p^{-2}$. On définit alors par récurrence $n_r$ tel que, si $n \geq n_1 + n_2 + \ldots + n_r$, $|\Delta^n f(x)| \leq p^{-r}$. On a donc montré que $\lim_{n\to\infty} |\Delta^n f(x)| = 0$ pour tout $x \in \mathbb{Z}_p$ et comme $\mathrm{Sup}_{x\in\mathbb{Z}_p} |\binom{x}{n}| = 1$, la série $\sum_{n\geq 0} \Delta^n f(0))\binom{x}{n}$ converge uniformément sur $\mathbb{Z}_p$ vers $f(x)$. Le reste du théorème est évident. □

Ce théorème peut se généraliser dans diverses directions, on peut remplacer $\mathbb{Z}_p$ par des ensembles plus généraux (cf. [2]), on peut remplacer les polynômes $\binom{x}{n}$ par d'autres fonctions (cf. [8] et [26]). Carlitz, par exemple [9 a],[9 b],[9 c], a démontré de nombreuses congruences du type $\sum_{k=0}^{n} (-1)^{n-k}\binom{n}{k} a_k \equiv 0 \bmod(p^{r(n)})$ pour $n \geq n_r$, où $a_k$ est une suite d'entiers définie arithmétiquement ou combinatoirement. Il exprimait en fait qu'il existait une fonction continue p-adique sous-jacente à la suite $a_n$. Nous reviendrons là-dessus ultérieurement.

On peut plus généralement, définir des fonctions dérivables, localement analytiques de $\mathbb{Z}_p$ dans $\mathbb{Q}_p$, toutes ces fonctions sont caractérisées aisément en terme de leurs coefficients d'interpolation $\lambda_n$. Par exemple :

THEOREME 2.- (Amice [2]). *Soit $f \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$, f est localement analytique sur $\mathbb{Z}_p$ (i.e. en tout point a de $\mathbb{Z}_p$ il existe un disque $D(a,\rho_a)^+ = \{x \in \mathbb{Z}_p ; |x-a| \leq \rho_a\}$ tel que f soit représentable sur $D(a,\rho_a)^+$ par une série de Taylor en $x-a$) si et seulement si $f(x) = \sum_{n\geq 0} \lambda_n(f)\binom{x}{n}$ et $\limsup. |\lambda_n(f)|^{1/n} < 1$.*

On définit à partir de $\mathbb{Q}_p$ la clôture algébrique de $\mathbb{Q}_p$ que l'on note $\overline{\mathbb{Q}}_p$, sur laquelle la valeur absolue p-adique s'étend de manière unique si l'on impose $|p| = p^{-1}$ ([1],[20]). Mais $\overline{\mathbb{Q}}_p$ n'est pas complet pour cette valeur absolue. On complète donc $\overline{\mathbb{Q}}_p$ et l'on obtient un corps complet et algébriquement clos $\mathbb{C}_p$. Ce corps $\mathbb{C}_p$ est le bon corps pour manipuler les séries de Taylor car le principe du maximum y est valide ainsi que le théorème de Liouville (cf. [1]). On suppose que l'on a choisi

une fois pour toutes un plongement de $\overline{\mathbb{Q}}$ dans $\mathbb{C}_p$. On note encore $|.|$ la valeur absolue sur $\mathbb{C}_p$ qui prolonge donc la valeur absolue p-adique de $\mathbb{Q}_p$.

Nous allons donner maintenant un critère dû à Y. Amice [3] qui montre que certaines propriétés de congruences de la suite $(a_n)_{n\in\mathbb{N}}$ se reflètent sur des propriétés de prolongeabilité analytique p-adique de sa fonction génératrice $Y = \sum_{n\geq 0} a_n X^n$. Auparavant nous allons donner quelques définitions.

DEFINITION 1.- ([1],[24]). *Soit $\mathcal{D} \subset \mathbb{C}_p$. On dit que F est un élément analytique (p-adique) sur $\mathcal{D}$ si et seulement si F est limite uniforme sur $\mathcal{D}$ d'une suite de fractions rationnelles $F_n(X) \in \mathbb{C}_p(X)$ sans pôle dans $\mathcal{D}$. Si $\mathcal{D}$ n'est pas borné, on dit que F est un élément analytique sur $\mathcal{D}$ nul à l'infini si F est un élément analytique sur $\mathcal{D}$ et si $\lim_{\substack{|X|\to\infty \\ X\in\mathcal{D}}} |F(X)| = 0$. On note $\mathcal{H}(\mathcal{D})$, resp. $\mathcal{H}_o(\mathcal{D})$, l'espace des éléments analytiques sur $\mathcal{D}$, resp. nuls à l'infini.*

On note $D(a,r)^+ = \{x \in \mathbb{C}_p ; |x-a| \leq r\}$ et $D(a,r)^- = \{x \in C_p ; |x-a| < r\}$ pour $a \in \mathbb{C}_p$ et $r \in \mathbb{R}_+$.

DEFINITION 2.- ([24]). *Soit $\mathcal{D} \subset \mathbb{C}_p$, on dit que $\mathcal{D}$ est un quasi-connexe si, pour tout $x \in \mathcal{D}$ et pour tout $y \in \mathcal{D}$ il existe $0 < r_1 < r_2 < \ldots < r_n < |x-y|$ tels que si $x \notin \mathcal{D}$ et $|z-x| < |x-y|$ alors il existe $1 \leq i \leq n$ tel que $|z-x| = r_i$.*

Dans les exemples on considèrera souvent des quasi-connexes de la forme

$$\mathcal{D} = D(a,r)^+ - \bigcup_{i=1}^{n} D(a_i,r_i)^- \text{ où } a_i \in D(a,r)^+ \text{ et } r_i \leq r.$$

DEFINITION 3.- ([1] ou [24]). *Soit $F(X) = \sum_{n\geq 0} a_n X^n$ une série de Taylor de $\mathbb{C}_p[[X]]$ convergeant sur $D(0,1)^-$ et soit $\mathcal{D} \supset D(0,1)^-$ un quasi-connexe. On dit que F est prolongeable en un élément analytique (p-adique) sur $\mathcal{D}$ s'il existe un élément analytique sur $\mathcal{D}$, noté encore F, dont la restriction à $D(0,1)^-$ coïncide avec F.*

L'intérêt de cette définition est qu'il y a unicité du prolongement analytique à $\mathcal{D}$ ([24]).

THEOREME 3.- (Amice [3]). *Soit $(a_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathbb{C}_p$. Les conditions suivantes sont équivalentes :*

*i) il existe une fonction $f \in \mathcal{C}(\mathbb{Z}_p,\mathbb{C}_p)$ telle que $f(n) = a_n$ pour tout $n \in \mathbb{N}$ ;*

*ii) la série de Taylor* $F(X) = \sum_{n\geq 0} a_n X^n$ *est prolongeable en un élément analytique sur* $\mathbb{C}_p - D(1,1)^-$, *nul à l'infini.*

□ Si $F \in \mathscr{H}_o(C_p - D(1,1)^-)$ alors F est limite uniforme sur $\mathbb{C}_p - D(1,1)^-$ d'une suite de fractions rationnelles $F_n$ ayant toutes leurs pôles dans $D(1,1)^-$. On peut donc écrire $F_n(X) = \sum_{k\geq 0} \lambda_{k,n} \frac{X^k}{(1-X)^{k+1}}$ avec $\lim_{k\to\infty} |\lambda_{k,n}| = 0$, et comme $|F_{n+1}(X) - F_n(X)| \leq \varepsilon(n)$ si $X \in \mathbb{C}_p - D(1,1)^-$, on a $\mathrm{Sup}_{k\in\mathbb{N}} |\lambda_{k,n+1} - \lambda_{k,n}| \leq \varepsilon(n)$. Il est alors immédiat que la suite $n \to \lambda_{k,n}$ converge vers une limite $\lambda_k$ et en outre $\lim_{k\to\infty} |\lambda_k| = 0$. On en déduit que $F(X) = \sum_{k\geq 0} \lambda_k \frac{X^k}{(1-X)^{k+1}}$ sur $\mathbb{C}_p - D(1,1)^-$. De là on tire que, si $|X| < 1$, $F(X) = \sum_{m\geq 0} X^m \sum_{k\geq 0} \lambda_k \binom{m}{n}$. Or comme $\lim_{k\to\infty} |\lambda_k| = 0$, il existe une unique fonction continue de $\mathbb{Z}_p$ dans $\mathbb{C}_p$, f, telle que $f(x) = \sum_{k\geq 0} \lambda_k \binom{x}{k}$ et donc $F(X) = \sum_{m\geq 0} f(m) X^m$ si $|X| < 1$. La réciproque est immédiate. □

Or, dire que $f \in \mathscr{C}(\mathbb{Z}_p, \mathbb{C}_p)$ revient à dire que les valeurs f(n), pour $n \in \mathbb{N}$, satisfont certaines congruences. Ce théorème se généralise de la manière suivante.

THEOREME 4.- (Robba [24]). *Une condition nécessaire et suffisante pour que* $F(X) = \sum_{n\geq 0} a_n X^n \in \mathbb{C}_p[[X]]$ *soit un élément analytique sur* $D(0,1)^-$ *est que la suite* $(a_n)_{n\in\mathbb{N}}$ *soit* (p)*-presque périodique (ou bien ultimement périodique modulo* $p^h$ *pour tout* $h \geq 0$), *c'est dire que :*

$$\forall\, \varepsilon > 0,\ \exists\, n_o \in \mathbb{N} \text{ et } T \in \mathbb{N} \quad \textit{tels que} \quad \forall\, n \geq n_o,\ |a_n - a_{n+T}| \leq \varepsilon.$$

□ Une fraction rationnelle sans pôles dans $D(0,1)^-$ vérifie le théorème précédent par application du critère d'Amice après décomposition en éléments simples. En effet $P_n(X) = \sum_{i,k} \frac{\lambda_{i,k,n}}{(1-e_{i,n}X)^k} \in \mathbb{C}_p(X)$ avec $|e_{i,n}| \leq 1$, si $|e_{i,n}| = 1$ alors pour tout $h \in \mathbb{N}$, il existe r et $r' \in \mathbb{N}$ tels que $|e_{i,n}^{(p^r-1)p^{r'}} - 1| \leq p^{-h}$ ; donc si $P_n(X) = \sum_{m\geq 0} a_{m,n} X^m$ pour $|X| < 1$, la suite $(a_{m,n})_{m\in\mathbb{N}}$ est clairement presque périodique, on conclut par passage à la limite pour les éléments analytiques sur $D(0,1)^-$. Si, maintenant, on suppose que la suite $(a_n)_{n\in\mathbb{N}}$ est presque périodique, on a :

$$F(X) = a_o + a_1 X + \ldots + a_{n_o-1} X^{n_o-1} + X^{n_o} \frac{a_{n_o} + a_{n_o+1} X + \ldots + a_{n_o+T-1} X^{T-1}}{1 - X^T} + \varepsilon G(X)$$

où $\sup_{X \in D(0,1)^-} |G(X)| \leq 1$ et où $n_o, T, \varepsilon$ sont comme dans l'énoncé du théorème. □

On voit donc que montrer qu'une suite est (p)-presque-périodique équivaut à montrer que sa fonction génératrice est un élément analytique p-adique sur $D(0,1)^-$. En fait, en regardant les endroits où la série génératrice $F(X) = \sum_{n \geq 0} a_n X^n$ est prolongeable analytiquement, on peut préciser la liaison qui existe entre $\varepsilon, n_o$ et T. Ceci repose sur le théorème de Mittag-Leffler p-adique ([24]), que nous allons donner sans démonstration après la définition suivante :

*DEFINITION 4.- (Robba [24]). Soit $\mathcal{D}$ un quasi-connexe de $\mathbb{C}_p$. Un disque ouvert $T = \{x \in \mathbb{C}_p ; |x - a| < r_T\}$ est un trou de $\mathcal{D}$ si $T \subset \mathbb{C}_p - \mathcal{D}$ et si T est maximal pour la relation d'inclusion. On note $\mathcal{C}$ la famille de trous (ouverts) de $\mathcal{D}$. Si $\mathcal{D}$ est borné, on admet comme trou le "disque ouvert" de centre l'infini $\mathbb{C}_p - D(a,R)^+$ où $a \in \mathcal{D}$ et $R = \mathrm{Inf}\{r ; \mathcal{D} \subset D(a,r)^+\}$.*

EXEMPLE.- Si $\mathcal{D} = D(0,1)^-$ les trous de $\mathcal{D}$ sont le disque ouvert de centre l'infini et de "rayon 1", $\mathbb{C}_p - D(0,1)^+$, et tous les disques $D(\alpha,1)^-$ où les $\alpha$ forment un système complet de représentants de $\mathcal{O}_p / \underline{m}_p$ où $\mathcal{O}_p$ est l'anneau des entiers de $\mathbb{C}_p$ (i.e. $\mathcal{O}_p = D(0,1)^+$) et où $\underline{m}_p$ est l'idéal maximal de $\mathcal{O}_p$ (i.e. $\underline{m}_p = D(0,1)^-$) ; par exemple on peut choisir les $\alpha$ comme étant toutes les racines primitives de l'unité d'ordre premier à p.

*THEOREME 5.- (de Mittag-Leffler p-adique ; Robba [24]). Soit F un élément analytique sur le quasi-connexe $\mathcal{D}$, soit $\mathcal{C}$ la famille des trous de $\mathcal{D}$. Il existe pour chaque $T \in \mathcal{C}$ un unique élément analytique $F_T$ sur $\mathbb{C}_p - T$, nul à l'infini, tel que $F - F_T$ se prolonge analytiquement dans T. En outre, on a $F = \sum_{T \in \mathcal{C}} F_T$ la somme convergeant uniformément sur $\mathcal{D}$ suivant le filtre des complémentaires des parties finies et $\|F\|_{\mathcal{D}} = \sup_{X \in \mathcal{D}} |F(X)| = \sup_{T \in \mathcal{C}} \|F\|_{\mathbb{C}_p - T} = \sup_{T \in \mathcal{C}} \sup_{X \in \mathbb{C}_p - T} |F(X)|$.*

Comme application immédiate on a le résultat suivant qui montre le lien entre la géométrie du quasi-connexe sur lequel F se prolonge et la presque périodicité de la suite $a_n$.

*COROLLAIRE 1.- Une condition nécessaire et suffisante pour que* $F(X) = \sum_{n\geq 0} a_n X^n$ *soit un élément analytique sur* $\mathbb{C}_p - \bigcup_{i=1}^{p-1} D(i^{-1},1)^-$ *nul à l'infini, est que les suites* $m \to a_{i+m(p-1)}$ *soient pour* $1 \leq i \leq p-1$ *la restriction à* $\mathbb{N}$ *d'une fonction continue de* $\mathbb{Z}_p$ *dans* $\mathbb{C}_p$.

□ D'après le théorème de Mittag-Leffler on a $F = F_1 + \ldots + F_{p-1}$ où $F_i \in \mathcal{H}_o(\mathbb{C}_p - D(i^{-1},1)^-)$, et $F_i(X) = \sum_{k\geq 0} \lambda_{i,k} \frac{(Xi^{-1})^k}{(1-Xi^{-1})^{k+1}}$ avec $\lim_{k\to\infty} |\lambda_{i,k}| = 0$, le résultat est alors immédiat grâce au critère d'Amice et au petit théorème de Fermat. □

On voit donc que la théorie des éléments analytiques fournit un cadre et un langage agréable pour le traitement des suites d'entiers p-presque périodiques.

## II.-SUITES CLASSIQUES DE NOMBRES

On peut remarquer que la plupart des fonctions génératrices exponentielles (resp. génératrices ordinaires) des suites classiques de nombres satisfont une équation différentielle algébrique (voir les exemples ci-après). Ce type de propriété impose a priori des limitations assez sévères sur les dénominateurs des nombres en cause. En effet, soit $F(X) = \sum_{n\geq 0} a_n X^n \in \overline{\mathbb{Q}}[[X]]$ où $\overline{\mathbb{Q}}$ est la clôture algébrique de $\mathbb{Q}$. On a alors le théorème suivant :

*THEOREME 6.- (Sibuya-Sperber [25 a]). Si* $F \in \mathbb{Q}[[X]]$ *satisfait une équation différentielle algébrique (non triviale), alors* F *possède un disque de convergence non trivial pour toute valeur absolue non archimédienne* $\nu$ *de* $\mathbb{Q}$.

La signification de ce théorème est la suivante. Si $F \in \mathbb{Q}[[X]]$ et si $\nu$ est la valeur absolue p-adique sur $\mathbb{Q}$, alors le dénominateur de $a_n$ (écrit sous forme irréductible) contient p avec au plus la puissance rn où $r \in \mathbb{R}_+$ et est indépendant de n.

Ce théorème généralise les résultats classiques de Eisenstein et Hurwitz que je rappelle ci-après.

*THEOREME 7.- (Eisenstein [13]). Si une série* $F(X) = \sum_{n\geq 0} c_n X^n$ *de* $\overline{\mathbb{Q}}[[X]]$ *représente une fonction algébrique, alors il existe un* $\ell_o \in \mathbb{N}$ *tel que* $\ell_o^n c_n \in I$ *où* I *est l'anneau des entiers de* $\overline{\mathbb{Q}}$. *En outre, il existe* $c > 0$ *tel que, ou bien* $c_n = 0$, *ou bien*

$|c_n|_\infty \geq c^n > 0$ *où* $|\ |_\infty$ *est une valeur absolue archimédienne sur* $\overline{\mathbb{Q}}$.

THEOREME 8.- (*Hurwitz [17 a]*). *Si* $F(X) = \sum_{n\geq 0} c_n X^n \in \mathbb{Q}[[X]]$, *satisfait une équation différentielle algébrique, il existe* $h(s) \in \mathbb{Z}[s]$ *et* $n_o \in \mathbb{N}$ *tels que, si un nombre premier* p *divise le dénominateur de* $c_n$ *pour* $n \geq n_o$ *alors* p *divise* $h(n_o)h(n_o+1)\ldots h(n)$.

Après ces généralités, nous allons donner un résultat plus précis dû à Fujiwara et dont le domaine d'application coïncide assez bien avec les suites de nombres provenant de l'analyse combinatoire ou de l'artihmétique et, en particulier, des suites de nombres provenant de dénombrement sur le groupe symétrique ou de nombres provenant de valeurs en certains points de série de Dirichlet ayant une signification arithmétique.

THEOREME 9.- (*Fujiwara [15]*). *Soit* $F(x,y,y',\ldots,y^{(n)})$ *un polynôme à coefficients entiers rationnels et soit* $y = f(x) = \sum_{n\geq 0} a_n \frac{x}{n!}$ *avec* $a_n \in \mathbb{Z}$. *Si* y *vérifie l'équation différentielle* $F(x,y,y',\ldots,y^{(n)}) = 0$ *et si* $\frac{\partial F}{\partial y^{(n)}}(x,f(x),f'(x),\ldots,f^{(n)}(x))\Big|_{x=0} = a$ *avec* $(a,p) = 1$, *alors la série de Taylor* $g(x) = \sum_{n\geq 0} a_n x^n$ *est un élément analytique p-adique sur* $D(0,1)^- \subset \mathbb{C}_p$ ; *autrement dit, la suite* $(a_n)_{n\in\mathbb{N}}$ *est p-presque périodique.*

□ On a $y^{(k)} = f^{(k)}(x) = \sum_{n\geq k} a_n \frac{x^{n-k}}{(n-k)!}$. De $F(x,y,\ldots,y^{(n)}) = 0$ on tire

$\frac{\partial F}{\partial y^{(n)}} \cdot y^{(n+1)} + \frac{\partial F}{\partial y^{(n-1)}} \cdot y^{(n)} + \ldots + \frac{\partial F}{\partial y} \cdot y' + \frac{\partial F}{\partial x} = 0$ ce que l'on peut écrire

$P(x,y,y',\ldots,y^{(n)})y^{(n+1)} = Q_o(x,y,y',\ldots,y^{(n)})$. De là on tire

$P \cdot y^{(n+2)} = \frac{d}{dx}(Q_o) - y^{(n+1)} \frac{dP}{dx} = Q_1(x,y,y',\ldots,y^{(n+1)})$, $P \cdot y^{(n+3)} = \frac{d}{dx}(Q_1) - y^{(n+2)} \frac{dP}{dx}$

et donc $P^2 \cdot y^{(n+2)} = Q_2(x,y,\ldots,y^{(n+1)})$ et par récurrence $P^k \cdot y^{(n+k+1)} = Q_k(x,y,\ldots y^{(n+1)})$.

On remarque que si $f(x) = a_o + a_1 \frac{x}{1!} + \ldots + a_n \frac{x^n}{n!} + \ldots$ avec $a_n \in \mathbb{Z}$ alors

$(f(x) - a_o)^m = f(x)^m - mf(x)^{m-1}a_o + \ldots + (-1)^m a_o^m \equiv 0$ modulo m!, où la congruence est à prendre au sens suivant : si $f(x) = \sum_{n\geq 0} a_n \frac{x^n}{n!}$ et $h(x) = \sum_{n\geq 0} b_n \frac{x^n}{n!}$ avec $a_n$ et $b_n \in \mathbb{Z}$,

alors $f \equiv h \bmod(m)$ équivaut par définition à $a_n \equiv b_n \bmod(m)$ pour tout $n \geq 0$. Il faut donc montrer que si $a_o = 0$ alors $f^m(x) \equiv 0 \bmod(m!)$. On montre ceci par récurrence, c'est vrai pour $m = 1$, supposons que ce soit vrai pour $m - 1$ ; alors on remarque que $\frac{d}{dx} f^m(x) = mf'(x)f^{m-1}(x)$ et on conclut en utilisant l'hypothèse de récurrence et le fait que les séries exponentielles forment une algèbre. Donc $Q_k(x,y,y',\ldots,y^{(n+1)}) \equiv R_k(x,y,y',\ldots,y^{(n+1)}) \bmod(m)$ où $R_k \in \mathbb{Z}[x,y,y',\ldots,y^{(n+1)}]$ est de degré $m - 2$ au plus en chacune des variables et ses coefficients sont modulo m. On appelle un tel polynôme un polynôme réduit. Le nombre de polynômes réduits distincts est fini et au plus $N - 1$. Donc pour tout k, on a :

$$P^N \cdot y^{(n+k+1)} = Q_k(x,y,\ldots,y^{(n+1)})P^{N-k} \equiv \overline{R}_k(x,y,\ldots,y^{(n+1)}) \bmod(m)$$

où $\overline{R}_k$ est un polynôme réduit. Il existe donc un i tel que $1 \leq i \leq N - 1$ et $\overline{R}_i(x,y,\ldots,y^{(n+1)}) = \overline{R}_N(x,y,\ldots,y^{(n+1)})$ et donc $P^N \cdot y^{(n+N+1)} \equiv P^N \cdot y^{(n+i+1)} \bmod(m)$ et comme on a supposé que $P(x,y,y',\ldots,y^{(n+1)})_{|x=0} = a$ avec $(a,p) = 1$ on en déduit que $y^{(n+N+1)} \equiv y^{(n+i+1)} \bmod(p^h)$ si l'on a choisi $m = p^h$. Il est alors immédiat que la suite $a_n$ est p-presque périodique. □

On voit apparaître dans ce théorème le fait qui apparaîtra constamment dans les exemples ci-après, du passage entre une série génératrice exponentielle ayant de bonne propriétés fonctionnelles et la série génératrice ordinaire ayant de bonnes propriétés de prolongeabilité analytique p-adique. On est donc amené à introduire la transformation de Laplace formelle.

*DEFINITION 5.*- ([6]). *Soit* $\widetilde{F}(X) = \sum_{n\geq 0} a_n \frac{X^n}{n!} \in K[[X]]$ *où* K *est un surcorps de* $\mathbb{Q}$. *On pose* $\mathcal{L}(\widetilde{F}(X)) = F(X) = \sum_{n\geq 0} a_n X^n$. *On appelle l'application* $\mathcal{L}$, *la transformation de Laplace formelle.*

*LEMME 1.*- ([4 d]). *La transformation de Laplace formelle possède les propriétés suivantes :*

*i)* $\mathcal{L}$ *est continue pour la topologie* X*-adique,*

ii) $\mathcal{L}(e^{aX}) = \frac{1}{1 - aX}$

iii) *si* $\mathcal{L}(\widetilde{F}(X)) = F(X)$ *alors* $\mathcal{L}(e^{aX}\widetilde{F}(X)) = \frac{1}{1 - aX} F(\frac{X}{1 - aX})$

*iiii)* $\mathcal{L}\left(\frac{d}{dx} X \frac{d}{dX}\right)(F(X)) = \frac{d}{dX}(F(X))$.

□ Toutes ces propriétés sont évidentes, nous allons seulement démontrer iii).

On pose $\widetilde{F}(X) = \sum_{n\geq 0} b_n \frac{X^n}{n!}$, il vient :

$$e^{aX}\widetilde{F}(X) = \sum_{n\geq 0} \left( \sum_{k=0}^{n} a^k b_{n-k} \binom{n}{k} \right) \frac{X^n}{n!} \quad \text{et par conséquent :}$$

$$\mathcal{L}(e^{aX}\widetilde{F}(X) = \sum_{n\geq 0} \left( \sum_{k=0}^{n} a^k b_{n-k} \binom{n}{k} \right) X^n = \sum_{n\geq 0} b_n \sum_{k\geq 0} X^{n+k}\, a^k \binom{n+k}{k} =$$

$$\sum_{n\geq 0} b_n \frac{X^n}{(1-aX)^{n+1}} \cdot \quad \square$$

LEMME 2.- *Soit* $\widetilde{F}(X) = \sum_{n\geq 0} a_n \frac{X^n}{n!} \in K[[X]]$, *on peut écrire de manière unique* $\widetilde{F}(X) = \sum_{n\geq 0} b_n (e^X - 1)^n$ *avec* $b_n \in K$.

□ C'est clair car $T = e^X - 1$ est une uniformisante locale de $K[[X]]$. □

On a le théorème suivant qui est la clef des applications .

THEOREME 10.- *Soit* $\widetilde{F}(X) = \sum_{n\geq 0} a_n \frac{X^n}{n!} \in \mathbb{C}_p[[X]]$. *Soit* $\widetilde{F}(X) = \sum_{n\geq 0} b_n (e^X - 1)^n = \sum_{n\geq 0} b_n T^n = \widetilde{G}(T)$ *où l'on a posé* $T = e^X - 1$. *On pose* $G(T) = \mathcal{L}(\widetilde{G}(T)) = \sum_{n\geq 0} (n!) b_n T^n$ . *Les deux propositions suivantes sont équivalentes :*

*i)* $F(X)$ *est un élément analytique p-adique sur* $D(0,1)^-$ ;

*ii)* $G(T)$ *est un élément analytique p-adique sur* $D(0,1)^-$.

Montrons tout d'abord i) $\Rightarrow$ ii).

Soit $F_n$ une fraction rationnelle de $\mathbb{C}_p(X)$ approchant F uniformément sur $D(0,1)^-$. On décompose $F_n$ en élément simple et on est donc amené à étudier $f_k(X) = \frac{1}{(1-aX)^k}$ avec $|a| \leq 1$, et $h_k(X) = X^k$, $k \in \mathbb{N}$. On a $f_1(X) = \frac{1}{1-aX}$ et $f_k(X) = \frac{1}{k!} f_k(X) = \frac{1}{k!} a^{-k+1} \frac{d^{k-1}}{dX^{k-1}}(f_1(X))$. Or $\widetilde{f}_1(X) = e^{aX} = (e^X - 1 + 1)^a$ donc $\widetilde{f}_1(X) = \sum_{n\geq 0} \binom{a}{n} (e^X - 1)^n$

et donc $\widetilde{g}_1(T) = \sum_{n\geq 0} \binom{a}{n} T^n$, $g_1(T) = \sum_{n\geq 0} a(a-1)\ldots(a-n+1)T^n$ avec $|a| \leq 1$.

Or $a-k-p^h \equiv a-k \bmod(p^h \mathcal{O}_p)$ où $\mathcal{O}_p$ est l'anneau des entiers de $\mathbb{C}_p$, et donc, si $n = rp^h + q$ avec $0 \le q \le p^h - 1$, on a :

$$a(a-1)\dots(a-n+1) \equiv a(a-1)\dots(a-q+1)\{a(a-1)\dots(a-p^h+1)\}^r \bmod(p^h),$$

et donc $g_1(T) \equiv \sum_{n=0}^{p^h-1} a(a-1)\dots(a-n+1)T^n \sum_{r\ge 0} (a(a-1)\dots(a-p^h+1))^r T^{rp^h}$

$$\equiv \sum_{n=0}^{p^h-1} a(a-1)\dots(a-n+1)T^n \frac{1}{1-a(a-1)\dots(a-p^h+1)T^{p^h}}$$

modulo $p^h \mathcal{O}_p[[T]]$. Raisonnons par récurrence sur k, on a montré que $g_1(T) \in \mathcal{H}_o(D(0,1)^-)$, supposons que l'on ait montré que $g_{k-1} \in \mathcal{H}_o(D(0,1)^-)$ ; on a

$$\tilde{f}_k(X) = \frac{1}{ka}\frac{d}{dX}X\frac{d}{dX}(\tilde{f}_{k-1}(X)) = \frac{1}{ka}\frac{d}{dX}X\frac{d}{dX}\sum_{n\ge 0} b_n(k-1)(e^X-1)^n =$$

$$= \frac{1}{ka}\frac{d}{dX}X\sum_{n\ge 0}(b_{n+1}(k-1)\cdot(n+1)+n\cdot b_n(k-1))(e^X-1)^n =$$

$$= \frac{1}{ka}\sum_{n\ge 0}\{(n+1)b_{n+1}(k-1)+nb_n(k-1)\}(e^X-1)^n +$$

$$+\frac{1}{ka}X\sum_{n\ge 0}\{(n+2)(n+1)b_{n+2}(k-1)+((n+1)^2+n(n+1))b_{n+1}(k-1)+$$

$$+n^2 b_n(k-1)\}(e^X-1)^n.$$

On pose $A_n = \frac{1}{ka}((n+1)b_{n+1}(k-1)+nb_n(k-1))$ et

$B_n = \frac{1}{ka}((n+2)(n+1)b_{n+2}(k-1)+((n+1)^2+n(n+1)b_{n+1}(k-1)+n^2 b_n(k-1))$.

Il est clair que $\tilde{g}_k(T) = \sum_{n\ge 0} A_n T^n + \mathrm{Log}(1+T)\sum_{n\ge 0} B_n T^n$ et donc

$$g_k(T) = \sum_{n\ge 0}(n!)A_n T^n + \sum_{n\ge 0} T^n \sum_{n=0}^{n=1}(k!)((n-k-1)!)\binom{n}{k}B_k.$$

Il est clair que la suite $n \to (n!)A_n$ est p-presque périodique, que la suite $k \to (k!)B_k$ l'est aussi et donc que la suite $n \to C_n = \sum_{k=0}^{n-1}(k!)((n-k-1)!)\binom{n}{k}B_k$ l'est aussi car la suite $k \to k!$ tend vers zéro p-adiquement, et la suite $n \to \binom{n}{k}$ est p-presque périodique. On a donc montré que $g_k \in \mathcal{H}(D(0,1)^-)$ pour tout $k \in \mathbb{N}$. Il reste donc à étudier le cas de $X^n$. Or on a $X = \mathrm{Log}(e^X - 1 + 1) = \sum_{n\ge 0}\frac{(-1)^n}{n}(e^X-1)^n$ et la suite $n \to (-1)^n(n-1)!$ est presque périodique. Par récurrence on montre alors aisément que si $X^k = \sum_{n\ge 0} c_n(e^X-1)^n$ alors

la suite $n \to (n!)c_n$ est presque-périodique. On conclut alors que les fractions rationnelles satisfont ii). Les éléments analytiques vérifient ii) car $F \equiv F_n \bmod(p^h \mathcal{O}_p[[X]])$ entraîne $G(T) \equiv G_n(T) \bmod p^h \mathcal{O}_p[[T]])$.

Montrons maintenant que ii) $\Rightarrow$ i). On a $\tilde{F}(X) = \sum_{n\geq 0} b_n (e^X - 1)^n$ et donc $F(X) = \sum_{n\geq 0} \frac{(n!)X^n}{(1-X)(1-2X)\ldots(1-nX)} b_n$. Comme la suite $n \to (n!)b_n$ est p-presque périodique :

$$\forall\, h,\ \exists\, N \text{ et } \exists\, M \text{ tels que } \forall\, n \geq N,\quad |n!b_n - (n+M)!b_{n+M}| \leq p^{-h}.$$

On a $F(X) \equiv F_h \bmod(p^h \mathcal{O}_p[[X]])$ où

$$F_h(X) = \sum_{n=0}^{N-1} b_n \frac{n!X^n}{(1-X)\ldots(1-nX)} +$$

$$+ \sum_{n=N}^{N+Mp^h-1} b_n \frac{n!X^n}{(1-X)\ldots(1-nX)} \sum_{r\geq 0} \frac{X^{rMp^h}}{((1-X)\ldots(1-(Mp^h-1)X))^r}$$

$$F_h(X) = \sum_{n=0}^{N-1} b_n \frac{n!X^n}{(1-X)\ldots(1-nX)} +$$

$$+ \sum_{n=N}^{N+Mp^h-1} b_n \frac{n!X^n}{(1-X)\ldots(1-nX)} \cdot \frac{(1-X)\ldots(1-(Mp^h-1)X)}{(1-X)\ldots(1-(Mp^h-1)X) - X^{Mp^h}}$$

et donc $F_h(X)$ est une fraction rationnelle sans pôle dans $D(0,1)^-$, d'où le théorème. □

REMARQUE.- Un cas particulièrement agréable est celui où la suite $n \to n!b_n$ a pour limite p-adique zéro. Ce cas est fréquent pour les nombres définis combinatoirement ou arithmétiquement (cf. ci-après).

Nous allons montrer sur quelques exemples comment utiliser les techniques indiquées ci-dessus.

*PROPOSITION 1.*- ([16]). *Soit $g_n$ les nobmres définis par $\sum_{n\geq 0} g_n \frac{X^n}{n!} = \frac{1}{2-e^X}$. On a $g_{n+(p-1)p^h} \equiv g_n \bmod(p^h)$ pour $n \geq h$. Autrement dit, $\sum_{n\geq 0} g_n X^n$ est un élément analytique p-adique sur $D(0,1)^+ - \bigcup_{i=1}^{p-1} D(i,1)^-$.*

Ces nombres ont une interprétation combinatoire. On a

$\tilde{F}(X) = \dfrac{1}{1 + (1 - e^X)} = \sum_{n\geq 0} (e^X - 1)^n$, ici $b_n = 1$. Donc

$F(X) = \sum_{n\geq 0} \dfrac{n!X^n}{(1-X)\ldots(1-nX)} = \sum_{n\geq 0} \sum_{k=0} (-1)^{n-k}\binom{n}{k} \dfrac{1}{(1-kX)}$. De là on déduit par exemple que : $F(X) \equiv F_n(X) = \sum_{k=0}^{n-1} \dfrac{k!X^k}{(1-X)\ldots(1-kX)} \bmod(n!\mathbb{Z}[[X]])$ et donc

$g_r \equiv \sum_{m=0}^{n-1} \sum_{k=0}^{m} (-1)^{m-k}\binom{m}{k} k^r \bmod(n!)$, le petit théorème de Fermat donne alors les congruences annoncées. D'autre part, on a

$(1-X)\ldots(1-(n-1)X) \sum_{n\geq 0} g_n X^n \equiv \sum_{m=0}^{n-1} m!X^m(1-(m+1)X)\ldots(1-(n-1)X)$ d'où des relations de récurrence mod(n!) entre les $g_n$. □

REMARQUE 1.- Les relations de récurrence mod(n!) s'interprètent dans ce cadre par le fait que la série génératrice des $g_n$ est une limite uniforme de fractions rationnelles que l'on connaît explicitement.

REMARQUE 2.- On constate que $Y = F(X) = (2 - e^x)^{-1}$ vérifie l'équation différentielle algébrique $Y' = 2Y^2 - Y$.

*PROPOSITION 2.- ([21],[18]). Soit $0 \leq i < p-1$ et soit $B_n$ le n-ième nombre de Bernoulli. La suite $m \to (1 - p^{i+m(p-1)-1})B_{i+m(p-1)}$ est la restriction à $\mathbb{N}$ d'une fonction continue de $\mathbb{Z}_p$ dans $\mathbb{C}_p$ (et même localement analytique).*

□ On définit $\sum_{n\geq 0} B_n \dfrac{x^n}{n!} = \dfrac{x}{e^x - 1} = \sum_{i=0}^{p-1} - \dfrac{xe^{ix}}{e^{px} - 1}$ et donc

$\sum_{n\geq 0} (1 - p^{n-1})B_n \dfrac{x^n}{n!} = \sum_{i=1}^{p-1} - \dfrac{xe^{ix}}{e^{px} - 1} = \sum_{i=1}^{p-1} - p^{-1} \dfrac{e^{ix}\mathrm{Log}(1 + e^{px} - 1)}{e^{px} - 1}$ et donc

$\sum_{n\geq 0} (1 - p^{n-1})B_n x^n = \sum_{i=1}^{p-1} \sum_{n\geq 0} \dfrac{(-1)^{n+1}}{n+1} \dfrac{p^{n-1}n!x^n}{(1-ix)\ldots(1-(i+np)x)} = F(X)$, il est alors facile de voir que $F \in \mathcal{H}_o(\mathbb{C}_p - \bigcup_{i=1}^{p-1} D(i,1)^-)$ et le corollaire 1 donne le résultat. (cf.[4b]).

□

*PROPOSITION 3.* ([5 d]). *Soit $A_n(t)$ le n-ième polynôme Eulérien défini par*

$\sum_{n\geq 0} A_n(t)\,\frac{x^n}{n!} = \frac{1-t}{-t+e^{x(t-1)}}$. *Soit* $A_n^*(t)$ *les fractions rationnelles définies par*

$A_n(t) = \frac{tA_n(t)}{(t-1)^{n+1}} - p^n\,\frac{t^pA_n(t^p)}{(t^p-1)^{n+1}}$. *Alors pour* $n \equiv i \bmod(p-1)$ *la suite* $n \to A_n^*(t)$ *est la restriction à* $\mathbb{N}$ *d'une fonction continue p-adique de* $\mathbb{Z}_p$ *à valeurs dans* $\mathbb{Q}(t)\otimes\mathbb{Q}_p$.

□ On a en effet par un calcul facile (cf.[5 d]) :

$$\sum_{n\geq 0} A_n^*(t)\,\frac{v^n}{n!} = \sum_{i=1}^{p-1}\ \sum_{n\geq 0} e^{iv}\,\frac{t^{p-i}}{t^p-1}\left(\frac{e^{pv}-1}{t^p-1}\right)^n.$$

La suite du calcul est facile et se mène comme pour les nombres de Bernoulli. □

*PROPOSITION 4.* ([16]). *Soit* $\tilde{F}(X) = \sum_{n\geq 0} t_n\,\frac{x^n}{n!} = \exp(x+\frac{x^2}{2})$. *Alors*

$F(x) = \sum_{n\geq 0} t_n x^n = \sum_{n\geq 0} \frac{2n!}{2^n n!}\,\frac{x^{2n}}{(1-x)^{2n+1}}$ *et donc la suite* $(t_n)_{n\geq 0}$ *est la restriction, si* $p \neq 2$, *d'une fonction continue p-adique de* $\mathbb{Z}_p$ *dans* $\mathbb{Q}_p$ *(et même localement analytique cf. théorème 2). (Si* $p = 2$ *on peut donner des congruences modulo* $2^h$ *entre les* $t_n$ *cf.[4 d]).*

Les nombres $t_n$ ont une interprétation combinatoire. On a $\tilde{F}(x) = e^x\tilde{G}(x)$ où $\tilde{G}(x) = e^{x^2/2}$. Or $\mathcal{L}\,\tilde{G}(x) = \sum_{n\geq 0} 2^{-n}(2n!)\,\frac{x^{2n}}{n!}$ et donc d'après le lemme 1 :

$F(x) = \mathcal{L}(\tilde{F}(x)) = \sum_{n\geq 0} \frac{2n!}{2^n n!}\,\frac{x^{2n}}{(1-x)^{2n+1}}$ d'où le résultat grâce au critère d'Amice. On remarquera que $Y = \exp(x + x^2/2)$ satisfait l'équation différentielle algébrique $Y^2 = Y''Y' - (Y')^2$. □

*PROPOSITION 5.-* ([4 a],[9 c],[14],[16],[23]). *Les nombres de Bell* $(P_n)_{n\geq 0}$ *définis par* $\sum_{n\geq 0} P_n\,\frac{x^n}{n!} = e^{e^x-1} = \tilde{F}(x)$ *vérifient les congruences suivantes : on pose* $k(p) = \frac{p^p-1}{p-1}$ *alors* $P_n \equiv P_{n+k(p)p^{h-1}} \bmod(p^h)$ *si* $p \neq 2$ $(h \geq 1)$, $P_n \equiv P_{n+k(2)} \bmod(2)$ *et* $P_n \equiv P_{n+k(2)2^h} \bmod(2^h)$, $h \geq 2$. *En outre* $F(x) = \sum_{n\geq 0} P_n x^n$ *est un élément analytique sur le quasi-connexe* $\mathcal{D}_p = \mathbb{C}_p - \bigcup_{i=1}^{p} D(\zeta_i,1)^-$ *où* $\zeta_i$ *sont les racines de l'équation* $1 - X^{p-1} - X^p = 0$.

On a $\tilde{F}(x) = e^{e^x - 1} = \sum_{n \geq 0} \frac{e^x - 1}{n!}$ donc $F(x) = \sum_{n \geq 0} \frac{x^n}{(1-x)\ldots(1-nX)}$. A partir de là on montre comme au théorème 10 que $F(x) \equiv F_h(x) \bmod(p^h \mathbb{Z}[[x]])$ où

$$F_h(x) = \frac{\sum_{n=0}^{p^h-1} x^n(1-(n+1)x)\ldots(1-(p^h-1)x)}{(1-x)\ldots(1-(p^h-1)x) - x^{p^h}}$$

. Une étude précise des $F_h$ et le théorème de Mittag Leffler p-adique donnent le résultat. Remarquons que $Y = e^{e^x - 1}$ satisfait l'équation différentielle algébrique $Y' = Y''Y - Y^2$. □

*PROPOSITION 6.*- ([16]). *Soit* $F(x) = \sum_{n \geq 0} d_n \frac{x^n}{n!} = \frac{e^{-x}}{1-x}$ . *La suite* $n \to (-1)^n d_n$ *est, pour tout nombre premier p, la restriction à* $\mathbb{N}$ *d'une fonction continue de* $\mathbb{Z}_p$ *dans* $\mathbb{C}_p$. *(et même localement abalytique de* $\mathbb{Z}_p$ *dans* $\mathbb{C}_p$).

□ Les nombres $d_n$ ont une interprétation combinatoire. On a $\mathcal{L}(\frac{1}{1-x}) = \sum_{n \geq 0} n! x^n$ et donc d'après le lemme 1 on a : $\mathcal{L}(\frac{e^{-x}}{1-x}) = \frac{1}{1+x} \sum_{n \geq 0} n! \frac{x^n}{(1+x)^n}$. Et par conséquent : $\sum_{n \geq 0} (-1)^n d_n x^n = \sum_{n \geq 0} (-1)^n n! \frac{x^n}{(1-x)^{n+1}}$. Le critère d'Amice donne le résultat. On peut remarquer que $Y = F(x)$ vérifie l'équation différentielle algébrique $Y = -(1-x)Y - (1-x)Y'$. □

On pourrait multiplier les exemples cf. [4],[5],[9],[14],[16],[23] ainsi que de nombreux articles non cités ici.

On a le résultat suivant dû à Carlitz ([9 b]) (cf. aussi [5 e][5 f] pour une autre démonstration).

*THEOREME 11.*- ([9 b],[5 f]). *Soit* $X = \sum_{n \geq 1} e_n \frac{Y^n}{n} \in \mathbb{C}_p[[X]]$ *avec* $e_1 = 1$ *et* $|e_n| \leq 1$, *soit* $Y = \sum_{n \geq 1} a_n \frac{X^n}{n!}$ *la série réciproque de X. Soit* $c \in \mathbb{C}_p$ *tel que* $|c^{p-1} - e_p| \leq p^{-1}$, *alors on a* $Y = \sum_{n \geq 1} b_n (e^{cX} - 1)^n$ *où* $b_n = b_n(c)$, *avec*

*i)* $b_1 = c^{-1}$

*ii)* $|b_n| \leq |c|^{-n}$ *si* $1 \leq n \leq 2p-1$

*iii)* $|b_n| \leq |c|^{-n} . r_p^{n-1}$ *si* $n \geq 2p$ *où* $r_p = p^{1/(2p-2)}$ *si* $p \neq 2$ *et* 3, $r_3 = 3^{2/7}$, $r_2 = 2^{3/4}$.

□ La démonstration est basée sur le théorème d'inversion de Lagrange des séries formelles. On peut remarquer que ce théorème est, a priori, en dehors du champ d'application du théorème de Fujiwara. □

*COROLLAIRE 2.- Avec les notations et les hypothèses du théorème 11, la série* $F(X) = \sum_{n\geq 1} a_n X^n$ *est un élément analytique sur* $D(0,1)^-$. *Si l'on suppose que* $|e_p| = 1$ *et donc que* $|c| = 1$, *alors* F *est un élément analytique* p*-adique sur* $D(0,1)^+ - \bigcup_{i=1}^{p-1} D(i^{-1}c^{-1},1)^-$.

□ On a $F(X) = \sum_{n\geq 1} \frac{n!c^n X^n}{(1-cX)\ldots(1-ncX)} b_n$, et d'après le théorème 11, $\lim_{n\to\infty} |n!b_n| = 0$, le corollaire est immédiat. □

Parmi les applications de ce théorème on peut citer les nombres de Schröder ([5f]) et les coefficients des fonctions elliptiques de Weierstrass ([9a],[5 e], [19 a],[19 b]).

En fait, on peut remarquer que, si l'on a certaines congruences de type "Cartier" entre les $e_n$, alors on a de meilleures estimations pour $|b_n|$ et donc de meilleures congruences pour la suite $(a_n)_{n>0}$. Plus précisément, nous allons montrer que si les $e_n \in \mathbb{Z}$ et s'il existe $\omega \in \mathbb{Z}_p$ tel que, pour tout $n > 0$, $e_{np^h} \equiv \omega e_{np^{h-1}} \bmod (p^h\mathbb{Z}_p)$ alors $\sup_{n\in\mathbb{N}} (|b_n|) = 1$ si $|e_p| = 1$. Pour montrer ceci, nous aurons besoin du résultat suivant dû à Dwork.

*THEOREME 12.- ([12],[20]). Soit* K *l'extension maximale non ramifiée de* $\mathbb{Q}_p$ *et soit* $\sigma$ *le Frobenius sur* K *(i.e.* $\sigma$ *est l'unique automorphisme du groupe de Galois de* K *sur* $\mathbb{Q}_p$, *tel que, si* $x \in K$ *et* $|x| = 1$ *alors* $|\sigma(x) - x^p| < 1$). *Soit* $F(X) \in 1 + XK[[X]]$ . *Soit* $A_p = \{x \in K ; |x| \leq 1\}$ *l'anneau des entiers de* K. *Alors* $F(X) \in 1 + XA_p[[X]]$ *si et seulement si* $\frac{(F(X))^p}{F^\sigma(X^p)} \in 1 + pX\, A_p[[X]]$ *où* $F^\sigma(X) = \sum_{n\geq 0} \sigma(a_n)X^n$ *si* $F(X) = \sum_{n\geq 0} a_n X^n$.

□ On peut écrire formellement $F(X) = \prod_{n>0} (1 + b_n X^n)$ avec $b_n \in K$. Supposons que $F(X) \in 1 + X.A_p[[X]]$, alors il est clair que $b_n \in A_p$, et donc

$$\frac{(F(X))^p}{F^\sigma(X^p)} = \prod_{n\geq 1} \frac{(1+b_nX^n)^p}{1+\sigma(b_n)X^{np}} \equiv \prod_{n\geq 1} \frac{1+b_n^pX^{np}}{1+\sigma(b_n)X^{np}} \bmod pA_p[[X]].\text{Or } \frac{1+b_n^pX^{n}p}{1+\sigma(b_n)X^{np}} \in 1+pX$$

par définition de $\sigma$ et donc $\frac{(F(X))^p}{F^\sigma(X^p)} \in 1 + pX\, A_p[[X]]$ Réciproquement, si la dernière

relation est vraie, alors $\frac{(1+b_1X)^p}{1+\sigma(b_1)X^p} = 1 + p\alpha_1 X + X^2\,K[[X]]$, avec $|\alpha_1| \le 1$, et donc $pb_1 = p\alpha_1$ ce qui implique $|b_1| \le 1$. Par récurrence, on montre que $\frac{(1+b_kX^k)^p}{1+\sigma(b_k)X^{kp}} = 1 + p\alpha_kX^k + X^{k+1}\,K[[X]]$, avec $|\alpha_k| \le 1$, et donc $|b_k| \le 1$. □

*THEOREME 15.- Soit* $Y = \sum_{n\ge1} a_n \frac{X^n}{n!}$ *et* $X = \sum_{n\ge1} e_n \frac{Y^n}{n}$ *deux séries réciproques de* $\mathbb{Q}_p[[X]]$, *telles que* $e_1 = 1$ *et* $e_n \in \mathbb{Z}_p$ *pour tout entier* $n \ge 1$. *Les deux propositions suivantes sont équivalentes :*

*i) On a* $|e_p| = 1$ *et il existe* $\omega \in \mathbb{Z}_p$ *tel que, pour tout* $n \ge 1$ *et tout* $h \ge 1$, $e_{np^h} \equiv \omega e_{np^{h-1}} \bmod(p^h\mathbb{Z}_p)$,

*ii) il existe un nombre c de l'extension maximale non ramifiée K de* $\mathbb{Q}_p$, *tel que* $|c| = 1$ *et* $Y = \sum_{n\ge1} b_n(e^{cX}-1)^n$ *avec* $\sup_{n\ge1}|b_n| = 1$, *et on peut choisir* $\omega = \sigma(c)/c$.

□ Démontrons i) ⟹ ii). Nous allons commencer par montrer que, s'il existe $\omega \in \mathbb{Z}_p$ tel que $e_{np^h} \equiv \omega e_{np^{h-1}} \bmod(p^h\mathbb{Z}_p)$, on a en posant $\omega = \sigma(c)/c$,

$e^{cX} = 1 + \sum_{n\ge1} d_n Y^n$ avec $|d_n| \le 1$, $d_1 = c$ (et donc $|d_1| = 1$, car $e_p \equiv \omega \bmod(p)$).

Pour montrer ceci on va utiliser le théorème 12.

$\frac{(\exp(c\sum_{n\ge1} e_n \frac{Y^n}{n}))^p}{\exp(\sigma(c)\sum_{n\ge1}\sigma(e_n\frac{Y^{np}}{\sigma(n)}))} = \exp\{(\sum_{n\ge1} pce_n\frac{Y^n}{n}) - (\sum_{n\ge1}\sigma(c)e_n\frac{Y^{np}}{n})\}$ ; posons $F(Y) = e^{cX} = \exp(c\sum_{n\ge1} e_n\frac{Y^n}{n})$. On a :

$\frac{(F(Y))^p}{F^\sigma(Y^p)} = \exp\{\sum_{\substack{n\ge1\\(n,p)=1}} pce_n\frac{Y^n}{n} + \sum_{n\ge1}\frac{ce_{np}-\sigma(c)e_n}{n}Y^{np}\}$, or $|\frac{e_{np}-e_n}{n}| \le p^{-1}$ pour tout $n \ge 1$.

Par conséquent : $\frac{(F(Y))^p}{F^\sigma(Y^p)} = \exp\{\sum_{\substack{n\ge1\\(n,p)=1}} pce_n\frac{Y^n}{n} + \sum_{n\ge1} p\alpha_nY^{np}\}$, avec $|\alpha_n| \le 1$.

On a donc montré que $\frac{(F(Y))^p}{F^\sigma(Y^p)} \in 1 + pX\,A_p[[X]]$ où $A_p$ est l'anneau des entiers de K. D'après le théorème 12 ceci implique que $|d_n| \le 1$ pour $n \ge 1$ et comme $d_1 = c$, $\omega \equiv e_p \bmod(p)$, on a

aussi $|d_1| = 1$. On tire immédiatement de là que :

$$(*) \qquad Y = \sum_{n\geq 1} b_n (e^{cX} - 1)^n, \text{ avec } |b_1| = 1 \text{ et } |b_n| \leq 1 \text{ pour } n \geq 1.$$

Réciproquement, supposons que les relations (*) soient vraies, alors $e^{cX} = 1 + \sum_{n\geq 1} d_n Y^n$ avec $|d_n| \leq 1$ pour $n \geq 1$, et $d_1 = c$, donc $X = c^{-1}\mathrm{Log}(1 + \sum_{n\geq 1} d_n Y^n) =$

$= \sum_{n\geq 1} e_n \frac{Y^n}{n}$ avec $e_n \in \mathbb{Q}_p$ car $a_n \in \mathbb{Q}_p$. Or il est bien clair que

$\exp(c \sum_{n\geq 1} e_n \frac{Y^n}{n}) \in 1 + X\, A_p[[X]]$. De là on tire d'abord en dérivant logarithmitiquement que : $c \sum_{n\geq 1} e_n Y^n \in A_p[[X]]$ et donc que $e_n \in \mathbb{Z}_p$, et d'après le théorème 12

$\dfrac{\exp(pc \sum_{n\geq 1} e_n \frac{Y^n}{n})}{\exp(\sigma(c) \sum_{n\geq 1} e_n \frac{Y^{np}}{n})} \in 1 + pX\, A_p[[X]]$ ce qui implique que $\dfrac{ce_{np} - \sigma(c)e_n}{n} \in pA_p$ et donc

$e_{np} - \dfrac{\sigma(c)}{c} e_n \in pnA_p$. D'où le théorème en posant $\omega = \sigma(c)/c$. □

Ce théorème est utile pour les congruences entre coefficients de fonctions elliptiques ([9 a],[19 a],[19 b]). Actuellement il est utilisé dans le sens i) $\Longrightarrow$ ii) mais on pourrait probablement l'utiliser dans le sens ii) $\Longrightarrow$ i) grâce aux travaux de Carlitz.

REMARQUE 1.- Posons $c^{-n} a_n^* = \lim_{h\to\infty} c^{-n-(p-1)p^h} a_{n+(p-1)p^h}$, la limite étant au sens p-adique. Sous les hypothèses du théorème, la limite existe. Ce théorème traduit alors l'équivalence entre les congruences "à la Cartier" pour les $e_n$ et le fait que la suite $n \to c^{-n} a_n^*$ est, pour $n \equiv i \bmod(p-1)$, la restriction à $\mathbb{N}$ d'une fonction de l'algèbre d'Iwasawa [6]. C'est-à-dire que la suite $n \to c^{-i-(p-1)n} a^*_{i+(p-1)n}$ est la restriction à $\mathbb{N}$ de la limite uniforme sur $\mathbb{Z}_p$ d'une suite de polynômes exponentiels $\sum_{\text{fini}} \lambda_u u^s$ où $u \in 1 + p\mathbb{Z}_p$, $\lambda_u \in \mathbb{C}_p$, $|\lambda_u| \leq 1$, $s \in \mathbb{Z}_p$.

REMARQUE 2.- Dans les propositions 1, 2, 3, 4, 6 on peut facilement améliorer le résultat en remarquant que la fonction génératrice ordinaire est un élément analytique sur un ensemble plus grand que celui indiqué dans le texte.

## BIBLIOGRAPHIE

[1] AMICE Y. : "Nombres p-adiques" P.U.F. collection Sup., le Mathématicien, Paris, 1975.

[2] AMICE Y. : "Interpolation p-adique", Bull. Soc. Math. France t. 92, 1964, pp. 117-180.

[3] AMICE Y. & FRESNEL J. : "Fonctions zéta p-adiques des corps de nombres abéliens réels", Acta Arith., Warszawa t. 20, 1970, pp. 353-384.

[4] BARSKY D. : a) "Analyse p-adique et nombres de Bell", C.R. Acad. Sc. Paris, t. 282, 1976, série A, pp. 1257-1259.

b) "Analyse p-adique et nombres de Bernoulli", C.R. Acad. Sc. Paris, t. 283, 1976, série A, pp. 1069-1072.

c) "Analyse p-adique et nombres de Bernoulli-Hurwitz", C.R. Acad. Sc. Paris, t. 284, 1977, série A, pp. 137-140.

d) "On Morita's p-adic Γ function", Math. Proc. Camb. Phil. Soc. vol. 89, 1981, pp. 23-27.

[5] BARSKY D. : a) "Analyse p-adique et nombres de Bell", Groupe d'étude d'analyse ultramétrique, Amice-Robba, 3° année, 1975/76, exposé N°8.

b) "Fonctions génératrices et congruences", Séminaire Delange-Pisot-Poitou, 17° année, 1975/76, exposé N°21.

c) "Congruences de coefficients de série de Taylor", Groupe d'étude d'analyse ultramétrique, Amice-Robba, 3° année, 1975/76, exposé exposé N° 17.

d) "Polynômes Eulériens mod $p^h$", Groupe d'étude d'analyse ultramétrique, Amice-Robba, 4° année, 1976/77, exposé N°11.

e) "Différentielles et congruences", Groupe d'étude d'analyse ultramétrique, Amice-Robba, 4° année, 1976/77, exposé N° 12.

f) "Congruences pour les nombres de Schröder", Groupe d'étude d'analyse ultramétrique, Amice-Christol-Robba, 6° année, 1978/79, exposés N° 2 & 4.

g) "Congruences pour les nombres de Genocchi de 2° espèce", Groupe d'étude d'analyse-ultramétrique, Amice-Christol-Robba, 8° année, 1980/81, exposé N°34.

[6] BARSKY D. : "Transformation de Cauchy p-adique et algèbre d'Iwasawa", Math. Ann. t. 232, 1978, pp. 255-266.

[7] BOJANIC R. : "A simple proof of Mahler's Theorem on approximation of continuous function of a p-adic variable by polynomials",Journal of Number theory,vol. 6, 1974, pp. 412-415.

[8] CAENEPEEL S. : "p-adic interpolation of continuous functions", Preprint 1981.

[9] CARLITZ L. : a) "Congruences for the coefficient of the Jacobi elliptic function", Duke Math. J., t. 16, 1949, pp. 297-302.

b) "Congruences for the coefficient of hyperelliptic and related functions", Duke Math. J. t. 19, 1952, pp. 329-337.

c) "Congruences for generalized Bell and Stirling numbers", Duke Math. J. t. 22, 1955, pp. 193-205.

[10] CASSOU-NOGUES P. : "Application arithmétique de l'étude aux entiers négatifs des séries de Dirichlet associées à un polynôme", Preprint 1980.

[11] COMTET L. : "Analyse combinatoire", tomes I et II, P.U.F., collection Sup., le Mathématicien, Paris 1970.

[12] DWORK B. : "A deformation theory for the zeta function of a hypersurface", Proc. of the Int. Congress of Math., Stockholm, 1962, pp. 247-259.

[13] EISENSTEIN G. : "Uber eine allgemeine Eigenschaft der Reihen Entwicklungen aller algebraischen Funktionen", Preuss. Akad. der Wissenschaften Berlin, 1852, S. 441-443.

[14] FLAJOLET Ph. : "On congruences and continued fractions for some classical combinatorial quantities", Preprint 1981.

[15] FUJIWARA M. : "Uber die Periodizität der Entwicklungs Koeffizienten einer analytischen Funktion nach dem Modul m", Tohoku Math. J. t. 2, 1912, pp. 57-73.

[16] GESSEL I. : "Congruences for Bell and tangent numbers", I.B.M. Thomas J. Watson Research Center, R.C. 7280, 1978 (# 31371).

[17] HURWITZ A. : a) "Sur le développement des fonctions satisfaisant à une équation différentielle algébrique", Ann. Ec. Norm. Sup., série 3, t. 6, 1889, pp. 327-332.

b) "Uber die Entwicklungskoeffizienten der lemniscatischen Funktionen", Math. Ann. Bd. 51, 1899, pp. 196-226.

[18] IWASAWA K. : "Lectures on p-adic L function", Annals of Math. Studies N° 74, 1972, Princeton University Press.

[19] KATZ N. : a) "The Eisenstein measures and p-adic interpolation", Amer. J. of Math., t. 99, 1977, pp. 238-311.

b) "p-adic interpolation of real analytic Eisenstein series", Ann. of Math. t. 104, 1976, pp. 459-571.

[20] KOBLITZ N. : "p-adic numbers, p-adic analysis and zeta function", Springer Verlag, G.T.M., N° 58, 1977.

[21] KUBOTA T. & LEOPOLDT H.W. : "Eine p-adische Theorie der Zetawerte I", Journ. für die reine und ang. Math. Bd. 241-215, 1964, pp. 328-339.

[22] MAHLER K. : a) "An interpolation serie for continuous functions of a p-adic variable", Jour. für die reine und ang. Math. Bd. 199, 1958, pp. 23-34.

b) "Introduction to p-adic numbers and their functions", Cambridge University Press, 1973.

[23] RADOUX Ch. : "Arithmétique des nombres de Bell et analyse p-adique", Bull. Soc. Math. Belg., t. 29, 1977, pp. 13-28.

[24] ROBBA Ph. : "Fonctions analytiques sur les corps valués ultramétriques complets" Astérisque N° 10, 1973, pp. 109-220.

[25] SIBUYA Y. & SPERBER S. : a) "Arithmétic properties of power series solutions of algebraic differential equations", Annals. of Math., t. 113, 1981, pp. 111-157.

b) "Some new results on power-series solutions of algebraic differential equations", In Singular perturbations and asymptotics, Academic Press, 1980, pp. 379-403.

[26] Van der PUT M. : "Algèbres de fonctions continues p-adiques I & II", Proc. Kon. Ned. Akad. v. Wetensch. serie A, t. 71, 1968, pp. 401-420.