ANNALES MATHÉMATIQUES BLAISE PASCAL

ALAIN ROBERT

Le théorème des accroissements finis p-adique

Annales mathématiques Blaise Pascal, tome 2, n° 1 (1995), p. 245-258
<http://www.numdam.org/item?id=AMBP_1995__2_1_245_0>

Ann. Math. Blaise Pascal, Vol. 2, N° 1, 1995, pp.245-258

LE THEOREME DES ACCROISSEMENTS FINIS p-ADIQUE

Alain ROBERT, Université de Neuchâtel, Suisse

Résumé. La formule du calcul différentiel et intégral réel

$$|f(t+h) - f(t)| \leq |h| \cdot \|f'\|$$

est valable pour les fonctions $\mathcal{C}^1$. Malheureusement, on sait qu'il existe des fonctions p-adiques de dérivée identiquement nulle et qui ne sont localement constantes au voisinage d'aucun point (cette remarque avait déjà été faite par J. Dieudonné cf. [1]). Même pour les fonctions polynomiales p-adiques, le théorème n'est pas valable comme l'exemple suivant le montre. Prenons en effet $f(t) = t^p$, d'où $f'(t) = pt^{p-1}$ et avec la norme uniforme sur le disque unité p-adique $\|f'\| = |p| = 1/p < 1$ tandis que $f(1) - f(0) = 1$. En prenant encore $f(t) = t^{p^\nu}$, on voit qu'on peut même rendre $\|f'\|$ arbitrairement petite, tout en maintenant la différence $f(1) - f(0) = 1$ constante. On se propose de montrer qu'il y a une constante $r_p < 1$ universelle (indépendante de f) telle que le théorème des accroissements finis *reste valable pour* $|h| \leq r_p$.

1. NOTATIONS ET PREMIERE FORME DU THEOREME.

Considérons une extension complète K de $\mathbb{Q}_p$ et E un espace de Banach ultramétrique sur K. Pour toute suite $a = (a)_{n\geq 0}$ tendant vers zéro dans E, i.e. $a \in c_0(E)$, on peut considérer la série formelle restreinte $\sum_{n\geq 0} a_n T^n$. Grâce au fait que $\|a_n\| \to 0$, la série $\sum_{n\geq 0} a_n t^n$ va converger dans l'espace complet E pour $|t| \leq 1$, $(t \in K)$. Une telle suite définit une application

$$f : B_{\leq 1}(K) \longrightarrow E \ , \ t \mapsto f(t) = \sum_{n\geq 0} a_n t^n$$

par son développement en série. La *norme* de f est définie par

$$\|f\| = \sup_{n\geq 0} \|a_n\| = \max_{n\geq 0} \|a_n\|.$$

Lorsque $|t| \leq 1$, on a évidemment $\|f(t)\| \leq \|f\|$.

Proposition 1. *Lorsque le corps résiduel k de K est infini, on a*

$$\|f\| = \sup_{|t|\leq 1} \|f(t)\| = \max_{|t|=1} \|f(t)\|.$$

Preuve: Rappelons les notations: $k = \tilde{K} = R/P$ est le quotient de l'anneau $R = B_{\leq 1}(K)$ par son idéal maximal $P = B_{<1}(K)$. Posons $c = \|f\|$. Il est loisible de supposer $c > 0$. La boule $B_{\leq c}(E)$ est un R-module et son quotient

$$\tilde{E} = B_{\leq c}(E)/B_{<c}(E)$$

un espace vectoriel sur le corps résiduel k. La fonction f fournit un polynôme vectoriel $\tilde{f} = \sum \tilde{a}_n \cdot T^n$ ayant au moins un coefficient non nul puisque, par hypothèse, $\|f\| = c$. On peut choisir une forme linéaire φ sur $\tilde{E}$ telle que $\varphi(\tilde{a}_n) \neq 0$ pour un tel coefficient. Le polynôme scalaire

$$\varphi \circ \tilde{f} = \sum \alpha_n T^n = \sum \varphi(\tilde{a}_n) \cdot T^n \in k[T]$$

est non nul: il ne peut s'annuler en tous les points du corps infini k. On peut trouver $\tau \in k^\times$ tel que $\varphi \circ \tilde{f}(\tau) \neq 0$, et a fortiori

$$\|f(t)\| = c$$

pour tout $t \in R$, $\tau \equiv t \mod P$. Comme on a choisi $\tau \neq 0$, on a $|t| = 1$. ∎

Proposition 2. *Si $|s| \leq 1$ et $|t| \leq 1$. on a*

$$\|f(s) - f(t)\| \leq |s - t| \cdot \|f\|.$$

Preuve: Ecrivons simplement

$$\begin{aligned} f(s) - f(t) &= \sum_{n\geq 0} a_n s^n - \sum_{n\geq 0} a_n t^n = \sum_{n\geq 0} a_n (s^n - t^n) \\ &= (s-t) \sum_{n\geq 1} a_n (s^{n-1} + s^{n-2}t + \cdots + t^{n-1}). \end{aligned}$$

L'inégalité en résulte. car on a

$$|s^{n-1} + s^{n-2}t + \cdots + t^{n-1}| \leq \max_{i+j=n-1} |s^i t^j| \leq 1$$

sous l'hypothèse faite. ∎

Cette proposition montre par exemple que la boule unité de l'algèbre des séries formelles restreintes (aussi appelée *algèbre de Tate*) est uniformément équicontinue sur le disque unité fermé. On peut réécrire l'inégalité de la proposition 2 sous la forme équivalente

$$|f(t+h) - f(t)| \leq |h| \cdot \|f\|$$

si $|t| \leq 1$ et $|h| \leq 1$. Mais comme

$$\|f'\| = \sup_{n \geq 1} \|n a_n\| \leq \sup_{n \geq 0} \|a_n\| = \|f\|,$$

on voit bien que le théorème des accroissements finis ultramétrique visé est plus précis que l'équicontinuité qui vient d'être démontrée.

Théorème 1: *Lorsque* $f = \sum_{n \geq 0} a_n t^n$ *a des coefficients* a_n *dans un espace de Banach* E *ultramétrique sur un corps complet* K *avec* $\|a_n\| \to 0$, *on a*

$$\|f(t+h) - f(t)\| \leq |t| \cdot \|f'\|$$

si $|t| \leq 1$ *et* $|h| \leq r_p = |p|^{1/(p-1)}$.

Preuve: La formule de Taylor donne

$$f(t+h) - f(t) = \sum_{k \geq 1} h^k \cdot \frac{D^k f(t)}{k!} = h \cdot \sum_{k \geq 1} \frac{h^{k-1}}{k!} D^{k-1} f'(t)$$

avec $f' = \sum_{n \geq 1} n a_n t^{n-1}$. Il est clair que $\|D\| \leq 1$ d'où $\|D^{k-1} f'\| \leq \|f'\|$ et

$$\|D^{k-1} f'\| \leq \sup_{n \geq k} \|a_n\| \to 0 \quad (k \to \infty).$$

Le théorème sera démontré dès lors que l'on aura montré $|h^{k-1}/k!| \leq 1$. Cette condition pour $k = p$ requiert $|h|^{p-1} \leq |p|$, i.e. $|h| \leq r_p$. Lorsqu'elle est satisfaite, on aura

$$|h|^{k-1} \leq |p|^{(k-1)/(p-1)} \leq |k!|$$

car, en effet

$$ord_p(k!) = \frac{k - S_p(k)}{p-1} \leq \frac{k-1}{p-1}.$$

Alternativement, on peut observer que

$$D^k(x^m) = m(m-1)\cdots(m-k+1) \cdot x^{k-m}, \quad \frac{D^k(x^m)}{k!} = \binom{m}{k} \cdot x^{m-k}$$

d'où $\|\frac{D^k}{k!}\| \leq 1$ et $\|\frac{D^k(g)}{k!}\| \to 0$ lorsque les coefficients de g tendent vers 0. Puisque

$$f(t+h) - f(t) = h \cdot \sum_{k \geq 1} \frac{h^{k-1}}{k} \cdot \frac{D^{k-1} f'}{(k-1)!}(t)$$

il s'agit de montrer $|h^{k-1}/k| \leq 1$. Pour $k = p$, cette condition requiert bien $|h| \leq r_p = |p|^{1/(p-1)}$. Supposons-la satisfaite et prenons un entier $k \geq 1$ d'ordre p-adique ν. Alors

$$k = p^\nu m \geq p^\nu$$

et $\left|\frac{h^{k-1}}{k}\right| \leq \frac{r_p^{k-1}}{|p|^\nu} \leq r_p^{p^\nu - 1} \cdot |p|^{-\nu} = |p|^e$. L'exposant est positif

$$e = \frac{p^\nu - 1}{p-1} - \nu = (1 + p + \cdots + p^{\nu-1}) - \nu \geq 0$$

et la démonstration est achevée. ∎

Remarque: La limite de validité du théorème des accroissements finis peut être déduite de l'examen du seul exemple $f(t) = t^p$ car

$$|f(h) - f(0)| = |h^p|$$

doit être majoré par $|h| \cdot \|f'\| = |h| \cdot |p|$. Il en résulte déjà la condition $|h|^{(p-1)} \leq |p|$. D'autre part, on sait bien que le nombre $r_p = |p|^{1/(p-1)}$ est le rayon de convergence de l'exponentielle p-adique. Il est assez naturel que cette limitation apparaisse (même pour les polynômes) si on pense à la formule de Taylor

$$f(t+h) = \sum_{k \geq 0} h^k \cdot \frac{f^{(k)}(t)}{k!} = [\exp(hD) \cdot f](t)$$

écrite à l'aide de l'opérateur de dérivation D. Nénamoins. l'exponentielle p-adique e^z ne converge que pour $|z| < r_p$ (inégalité stricte) alors que le théorème des accroissements finis est valable pour $|h| \leq r_p$, en particulier valable pour $|h| = |p|$ (même si $p = 2$).

Exemple: Considérons le polynôme

$$f(T) = (1+T)^{p^n} - 1 \in \mathbb{Z}_p[T].$$

Son terme constant est nul et on démontre sans peine par induction que

$$f(T) \in T(p,T)^n \subset (p,T)^{n+1} \subset \mathbb{Z}_p[T],$$

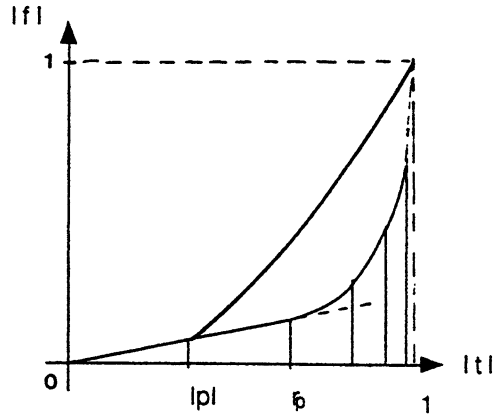
où (p,T) désigne l'idéal de l'anneau $\mathbb{Z}_p[T]$ engendré par p et T. Il en résulte immédiatement que pour tout $t \in \mathbb{C}_p$

$$|f(t)| \leq |t| \cdot \max(|p|^n, |t|^n)$$

et donc

$$|f(t)| \leq |t| \cdot |p|^n = |t| \cdot \|f'\| \text{ pour } |t| \leq |p|,$$
$$|f(t)| \leq |t|^{n+1} \text{ pour } |p| \leq |t| \leq 1.$$

Le théorème des accroissements finis montre que la première inégalité persiste dans la région $|p| \leq |t| \leq r_p$ qui représente une amélioration pour tout $p \geq 3$. La méthode du polygone de valuation permet d'évaluer exactement la valeur absolue $|f(t)|$. Celle-ci est en effet linéaire jusqu'au premier zéro de f qui intervient lorsque $1 + t$ est une racine de 1 d'ordre divisant p^n. Or les racines p-ièmes de 1 sont situées à distance r_p de 1. Ensuite le module de f dépasse l'estimation linéaire. La limitation donnée par le théorème des accroissements finis est donc la meilleure possible.



Application 1: Numérateurs des nombres de Bernoulli ([2], [3]).

Dénotons par $S_k(p)$ la somme des puissances k-ièmes des entiers $< p$

$$S_k(p) = \sum_{1 \leq j \leq p-1} j^k$$

p premier et k entier ≥ 1. Comme $\mu_{p-1} \subset \mathbb{Z}_p$, remplaçons dans la somme précédente chaque entier j par la racine de l'unité $\zeta_j \in \mu_{p-1}$ qui lui est congrue modulo p

$$j \equiv \zeta_j \mod p.$$

Donc

$$S_k(p) = \sum_{1 \leq j \leq p-1} \zeta_j^k = \sum_{\mu_{p-1}} \zeta^k \mod p$$

et cette dernière est nulle si k n'est pas multiple de $p - 1$. On a un peu mieux. En appliquant le théorème des accroissements finis à $f(x) = x^k$, donc $f'(x) = kx^{k-1}$ puis $\|f'\| = |k|$ $(k \geq 1)$, on en tire

$$\left|\zeta_j^k - i^k\right| \leq |p| \cdot \|f'\| = |pk|.$$

On peut écrire cette inégalité sous la forme

$$S_k(p) = \sum_{\mu_{p-1}} \zeta^k + pk \cdot u \quad (u \in \mathbb{Z}_p).$$

Ceci étant vu, rappelons quelques propriétés des nombres et polynômes de Bernoulli. On pose

$$\frac{t\exp(xt)}{\exp(t)-1} = \sum_{k\geq 0} B_k(x)\frac{t^k}{k!}, \quad \frac{t}{\exp(t)-1} = \sum_{k\geq 0} b_k \frac{t^k}{k!}$$

d'où $b_k = B_k(0)$, $b_0 = 1$, $b_1 = -1/2$, $b_2 = 1/6, \ldots$ $b_{2k+1} = 0$ pour $k \geq 1$ et inversément

$$B_k(x) = (b+x)^k = \sum_{0\leq i\leq k} \binom{k}{i} b_{k-i}x^i.$$

On utilise ces polynômes de Bernoulli pour estimer les sommes de puissances

$$S_k(n) = \sum_{0\leq \ell<n} \ell^k = 0^k + 1^k + \cdots (n-1)^k$$

(avec $0^k = 0$ si $k \geq 1$, tandis que $0^k = 1$ si $k = 0$). Pour calculer ces sommes, on peut former la fonction génératrice

$$\sum_{k\geq 0} S_k(n)\frac{t^k}{k!} = \sum_{k\geq 0}\sum_{0\leq \ell<n} \frac{\ell^k t^k}{k!} = \sum_{0\leq \ell<n} e^{\ell t} = \frac{e^{nt}-1}{e^t-1}$$

et en revenant aux polynômes de Bernoulli

$$\sum_{k\geq 0} S_k(n)\frac{t^k}{k!} = \frac{1}{t}\sum_{k\geq 0}(B_k(n)-b_k)\frac{t^k}{k!}$$

d'où

$$S_k(n) = \frac{B_{k+1}(n)-b_{k+1}}{k+1}.$$

On a ainsi

$$S_0(n) = n, \; S_1(n) = \frac{n(n-1)}{2}\ldots.$$

et plus généralement

$$\begin{aligned} S_k(n) &= \frac{1}{k+1}\sum_{1\leq i\leq k+1}\binom{k+1}{i} n^i b_{k+1-i} \\ &= \sum_{1\leq i\leq k+1}\frac{1}{i}\binom{k}{i-1} n^i b_{k+1-i} \\ &= nb_k + \sum_{2\leq i\leq k+1}\frac{1}{i}\binom{k}{i-1} n^i b_{k+1-i}. \end{aligned}$$

Nous utiliserons l'expression précédente pour n premier, disons $n = p > 2$

$$\begin{aligned} S_k(p) &= pb_k + \sum_{2\leq i\leq k+1}\frac{1}{i}\binom{k}{i} p^i b_{k+1-i} \\ &= pb_k + pk\cdot\sum_{2\leq i\leq k+1}\frac{1}{i(i-1)}\binom{k-1}{i-2} p^{i-2}\cdot pb_{k+1-i}. \end{aligned}$$

Cette identité montre (par induction) que $pb_k \in \mathbb{Z}_p$ et que

$$S_k(p) = pb_k + pk \cdot v$$

avec $v \in \mathbb{Z}_p$. En comparant les deux dernières expressions pour la somme $S_k(p)$

$$S_k(p) = \begin{cases} \sum_{\mu_{p-1}} \zeta^k + pk \cdot u \\ pb_k + pk \cdot v \end{cases}$$

on obtient

$$pb_k = \sum_{\mu_{p-1}} \zeta^k + pk \cdot w \quad (w = u - v \in \mathbb{Z}_p).$$

Lorsque k n'est pas multiple de $p-1$, on a ainsi $b_k = k \cdot w$ ($w \in \mathbb{Z}_p$) et cela montre que si k est multiple d'une puissance p^ν de p, alors le numérateur de b_k est aussi divisible par p^ν. C'est un théorème de Kummer (qui a été redécouvert plusieurs fois!). On a démontré

Théorème 2: *Les nombres de Bernoulli ont les propriétés suivantes*

1/ $pb_k \in \mathbb{Z}_p$ *pour tout nombre premier* p, $b_k \in \mathbb{Z}_p$ *si* $p-1$ *ne divise pas* k;

2/ *(Kummer)* $ord_p(b_k) \geq ord_p(k)$ *si* $p-1$ *ne divise pas* k;

3/ *(von Staudt)* $pb_k \equiv -1 \mod p\mathbb{Z}_p$ *si* $p-1$ *divise* k.

Corollaire: *(von Staudt) On a*

$$b_k = -\sum_{p-1|k} \frac{1}{p} + m_k \quad avec \quad m_k \in \mathbb{Z}$$

(En effet, $b_k + \sum_{p-1|k} \frac{1}{p}$ est un nombre rationnel qui est entier p-adique pour tout nombre premier p: son dénominateur est 1.)

Application 2: Congruences de coefficients binomiaux.

Posons $(1+x)^p = 1 + p \cdot g(x) + x^p$ puis $f(T) = (1 + T \cdot g(x) + x^p)^n$ de sorte que

$$f(p) = (1 + p \cdot g(x) + x^p)^n = (1+x)^{pn}, \quad f(0) = (1+x^p)^n.$$

Alors le théorème des accroissements finis appliqué à la fonction vectorielle f (dont les coefficients sont dans l'espace de dimension finie $E \subset \mathbb{Q}_p[x]$ formé des polynômes de degrés $\leq pn$) va permettre d'évaluer

$$f(p) - f(0) = (1+x)^{pn} - (1+x^p)^n = \sum \binom{np}{j} x^j - \binom{n}{k} x^k.$$

Comme $\|f'\| \leq |n|$, $|f(p) - f(0)| \leq |pn|$ et on déduit

$$\binom{np}{kp} \equiv \binom{n}{k} \mod npZ_p, \text{ et } \binom{np}{k} \equiv 0 \mod npZ_p \text{ si } p \text{ ne divise pas } k$$

(cette méthode est donnée dans [5]). La deuxième congruence est triviale car

$$\binom{np}{k} = \frac{np}{k}\binom{np-1}{k-1} \in npZ_p$$

(car $k \in Z_p^\times$ par hypothèse).

Application 3: Théorème du point fixe p- adique.

Soit K une extension finie du corps Q_p et $f \in K\{T\}$ une série formelle restreinte avec $\|f\| \leq 1$. Alors f définit une application continue de la boule unité $B = B_{\leq 1}(K)$ dans elle-même. Lorsque

$$\|f'\| < 1 \text{ et } \inf \|f(x) - x\| \leq r_p = |p|^{1/(p-1)}$$

f possède un point fixe.

Preuve: Par continuité de f sur la boule compacte B, on peut trouver $x_0 \in B$ avec $|f(x_0) - x_0| \leq r_p$. Posons alors $x_{n+1} = f(x_n)$ pour $n \geq 0$. On voit, par induction, en utilisant le théorème des accroissements finis

$$|x_{n+1} - x_n| = |f(x_n) - f(x_{n-1})| \leq |x_n - x_{n-1}| \cdot \|f'\| < |x_n - x_{n-1}| \leq r_p.$$

Comme le corps K est localement compact, sa valuation est discrète et la suite strictement décroissante $|x_{n+1} - x_n|$ tend vers zéro: c'est une suite de Cauchy. Sa limite est un point fixe de f. ∎

Pour voir que les hypothèses sont nécessaires, on peut considérer l'exemple de $f(T) = T^p + 1 \in Q_p[T]$, d'où $f'(T) = pT^{p-1}$, $\|f'\| = 1/p \leq r_p < 1$. On a

$$f(x) - x = x^p - x + 1 \equiv 1 \mod p$$

pour tout $x \in Z_p$. Cette fonction f n'a pas de point fixe dans la boule unité $B = Z_p$ de Q_p. Dans une extension convenable (de degré p) de Q_p, on pourra néanmoins trouver une racine de $x^p - x + 1 = 0$!).

2. LE THEOREME DES ACCROISSEMENTS FINIS D'ORDRE 2

Théorème 3: *Avec les mêmes notations que précédemment, si $|t| \leq 1$, on a*

$$\|f(t+h) - f(t) - f'(t)h\| \leq \left|\frac{t^2}{2}\right| \cdot \|f''\|$$

dès que $|h| \leq |p|^{1/(p-2)}$ pour $p \geq 3$, et dès que $|h| \leq |\sqrt{2}|$ pour $p = 2$.

Preuve: On écrit encore la formule de Taylor de f au point t

$$\begin{aligned} f(t+h) - f(t) - f'(t)h &= \sum_{k\geq 2} h^k \cdot \frac{D^k f(t)}{k!} \\ &= h^2 \cdot \sum_{k\geq 2} \frac{h^{k-2}}{k!} \cdot D^{k-2} f''(t) \\ &= h^2 \cdot \sum_{k\geq 2} \frac{h^{k-2}}{k(k-1)} \cdot \frac{D^{k-2} f''}{(k-2)!}(t). \end{aligned}$$

Comme précédemment

$$\left\| \frac{D^{k-2} f''}{(k-2)!} \right\| \leq \|f''\| \ \ (k \geq 2) \ \text{ et } \ \left\| \frac{D^{k-2} f''}{(k-2)!} \right\| \to 0.$$

• **1.** Pour $p \neq 2$, il reste à vérifier

$$\left| \frac{h^{k-2}}{k(k-1)} \right| \leq 1 \ \ (k \geq 2).$$

Pour $k = p$, ceci requiert $|h^{p-2}| \leq |p|$, condition indiquée dans l'énoncé. Lorsqu'elle est satisfaite, si $\nu = ord_p k \geq 1$. on a $k \geq p^\nu$ et $|k-1| = 1$ d'où

$$\left| \frac{h^{k-2}}{k(k-1)} \right| \leq \frac{|h|^{p^\nu - 2}}{|p|^\nu} \leq |p|^e$$

avec un exposant e valant

$$e = \frac{p^\nu - 2}{p-2} - \nu \geq \frac{p^\nu - 1}{p-1} - \nu \geq 0.$$

(L'homographie $\frac{p^\nu - x}{p-x}$ est croissante jusqu'en $x = p$ -asymptote verticale- car elle vaut $p^{\nu-1} \geq 1$ en $x = 0$, et est donc au-dessus de son asymptote horizontale jusqu'en $x = p$.) Dans le cas $\nu = ord_p(k-1) \geq 1$, on a $k \geq p^\nu + 1$ et les estimations précédentes sont a fortiori satisfaites. Finalement, $ord_p(k-1) = ord_p(k) = 0$ implique

$$|k(k-1)| = 1$$

et la démonstration est terminée.

• **2.** Dans le cas $p = 2$, on met $h^2/2$ en évidence et il reste à montrer

$$\left| \frac{h^{k-2}}{k(k-1)/2} \right| \leq 1$$

si $|h| \leq |\sqrt{2}|$. Le terme $k = 4$ requiert $|h^2/2| \leq 1$ qui fournit le domaine $|h| \leq |\sqrt{2}|$. Supposons ainsi $|h| \leq |\sqrt{2}|$. Si $\nu = ord_2(k) \geq 1$,

$$k \geq 2^\nu \ \text{ et } \ |k(k-1)/2| = |2|^{\nu-1},$$

d'où

$$\left|\frac{h^{k-2}}{k(k-1)/2}\right| \leq \frac{|h|^{2^\nu-2}}{|2|^{\nu-1}} \leq |2|^{2^{\nu-1}-1-(\nu-1)} = |2|^e.$$

Comme nous supposons $\nu \geq 1$, l'exposant $e = 2^{\nu-1} - \nu \geq 0$ est positif. On peut traiter de façon similaire le cas où $\nu = ord_2(k-1) \geq 1$.

Remarque: La condition sur la valeur absolue de l'accroissement est moins restrictive pour $p = 2$ mais l'inégalité est aussi moins forte dans ce cas puisque le dénominateur 2 se fait sentir dans $|h^2/2|$ (alors qu'il passe inaperçu si $p \geq 3$).

Application 4. *Soit K une extension finie de $\mathbb{Q}_p$, $R = B_{\leq 1}$ son anneau d'entiers d'idéal maximal P. Pour $n \in \mathbb{N}$ (ou même $n \in \mathbb{Z}_p$), on a* ([4], p.33-34)

$$(1+x)^n \equiv 1 + nx \mod pnxR$$

dès que $x \in 2pR$.

On prendra ici $f(T) = (1+T)^n$, d'où $f''(T) = n(n-1)(1+T)^{n-2}$ et

$$\|f''\| = |n(n-1)| \text{ si } n \geq 2.$$

Pour $|x| \leq |p|^{1/(p-2)}$ (resp. $\leq |\sqrt{2}|$ si $p = 2$) on ainsi

$$|(1+x)^n - 1 - nx| \leq \left|\frac{x^2}{2}\right| \cdot \|f''\| \leq |nx| \cdot \left|\frac{x}{2}\right|.$$

En particulier, lorsque $x \in 2pR$, $|x/2| \leq |p|$ et l'inégalité précédente fournit le résultat souhaité.

Application 5. Numérateurs des nombres harmoniques, théorème de Wolstenholme.

Les *nombres harmoniques* $h_n \in \mathbb{Q}$ sont définis par

$$h_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}.$$

On a par exemple

$$h_2 = \frac{3}{2},\ h_3 = \frac{11}{6},\ h_4 = \frac{25}{12},\ h_6 = \frac{49}{20},\ h_{10} = \frac{11^2 \cdot 61}{2520}, \ldots$$

De façon générale, pour tout nombre premier p, le dénominateur de h_{p-1} est premier à p. Modulo p, on a

$$h_{p-1} \equiv \sum_{0 \neq \zeta \in \mathbb{F}_p^\times} \frac{1}{\zeta} = 0 \text{ si } p > 2.$$

Donc le numérateur de h_{p-1} est divisible par p pour $p \geq 3$. Le théorème de Wolstenholme précise la situation lorsque $p \geq 5$. Il affirme que

pour tout nombre premier p supérieur à 3, le numérateur de h_{p-1} est divisible par p^2.

Preuve: (M. Zuber). Introduisons le polynôme

$$f(T) = (T-1)(T-2)\cdots(T-p+1)$$

de degré $p-1$ pair. On constate que $f(p-T) = f(T)$ d'où

$$f(p) = f(0), \quad -f'(p-T) = f'(T), \quad f''(p-T) = f''(T), \ldots$$

(Explicitement $f(0) = (-1)(-2)\cdots(-p+1) = (-1)^{p-1}(p-1)! = (p-1)! = f(p)$ car p est impair.) La dérivée de f vaut

$$f'(T) = \sum_{1 \leq i \leq p-1} (T-1)\cdots(T-\hat{i})\cdots(T-p+1)$$

(où le circonflexe indique un terme à omettre du produit), d'où

$$f'(0) = -f'(p).$$

La dérivée logarithme $f'/f = \sum_{1 \leq i \leq p-1} \frac{1}{T-i}$ permet de calculer h_{p-1}

$$h_{p-1} = -\frac{f'}{f}(0) = \frac{f'}{f}(p).$$

Le théorème de Wolstenholme revient à dire $h_{p-1} \in p^2\mathbb{Z}_p$, i.e. $|h_{p-1}| \leq |p|^2$. Mais puisque $f(0)$ est premier à $p \neq 2$

$$|h_{p-1}| = \left|\frac{f'(0)}{f(0)}\right| = |f'(0)| = |2f'(0)| = |f'(p) - f'(0)|.$$

Le théorème des accroissements finis (d'ordre 2) permet d'estimer

$$|f'(p) - f'(0) - pf''(0)| \leq |p|^2 \cdot \|f'''\| \leq |p|^2$$

(car $f \in \mathbb{Z}[T]$ implique $\|f^{(k)}\| \leq 1$ pour toutes les dérivées de f). Or on sait que $f(T) \equiv T^{p-1} - 1 \mod p$, d'où $f'(T) \equiv (p-1)T^{p-2}$, $f''(T) \equiv (p-1)(p-2)T^{p-3}$ et finalement $f''(0) \equiv 0 \mod p$ dès que $p > 3$. Dans ce cas, on a

$$f'(p) - f'(0) \equiv f'(p) - f'(0) - pf''(0) \equiv 0 \mod p^2\mathbb{Z}_p.$$

■

3. LE THEOREME DE ROLLE p-ADIQUE.

Il s'agit du théorème analogue au théorème classique (réel) qui fournit l'existence d'une valeur intermédiaire $t \leq \tau \leq t+h$ pour laquelle

$$f(t+h) = f(t) + h \cdot f'(\tau)$$

(rappelons le fait que cette forme n'est valable que pour les fonctions f d'une variable *à valeurs scalaires*). Si $f \in \mathbb{C}_p[[x]]$ est une série formelle, nous dénoterons par $r_f \in [0, \infty]$ son rayon de convergence. On sait que

$$r_f = \sup\{r \geq 0 : a_n r^n \to 0\} = \frac{1}{\limsup |a_n|^{1/n}}.$$

Théorème 4. a) *Soit $f \in \mathbb{C}_p[[x]]$ avec $r_f > 1$ (donc $f \in \mathbb{C}_p\{x\}$); supposons que f a deux zéros $a \neq b$ dans $B_{\leq 1}$ suffisamment proches*

$$|a-b| \leq r_p = |p|^{1/(p-1)}.$$

Alors f s'annule dans $B_{\leq 1}$.

b) *Soit $f \in \mathbb{C}_p\{x\}$ avec $r_f > 1$: supposons que f a deux zéros $a \neq b$ dans $B_{\leq 1}$ suffisamment proches*

$$|a-b| < r_p = |p|^{1/(p-1)}.$$

Alors f s'annule dans $B_{<1}$.

Preuve: Développant f en série de puissances centrée au voisinage de b, on voit qu'il suffit de considérer le cas où f s'annule en 0 et en a avec

$$|a| \leq r_p \quad (\text{resp. } < r_p).$$

Posons $f(x) = \sum_{n \geq 1} a_n x^n$ et supposons $a_1 \neq 0$ (sinon f' s'annule en 0 et le théorème est démontré). On peut aussi supposer que $|a| = r$ est le plus petit rayon critique > 0. Il y a donc un entier $n > 1$ avec

$$|a_1| r = |a_n| r^n,$$

d'où

$$\left|\frac{a_1}{a_n}\right| = r^{n-1} \leq r_p^{n-1} \quad (\text{resp. } < r_p^{n-1}).$$

Mais si $\nu = ord_p n$. disons $n = p^\nu$. on a

$$\frac{n-1}{p-1} = \frac{p^\nu m - 1}{p-1} \geq \frac{p^\nu - 1}{p-1} = p^{\nu-1} + \cdots + p + 1 \geq \nu$$

(avec des égalités si $m = 1$ et $\nu = 1$). Revenant à ce que nous avons trouvé, on en déduit

$$\left|\frac{a_1}{a_n}\right| \leq r_p^{n-1} = |p|^{\frac{n-1}{p-1}} \leq |p|^{\nu} = |n|$$

puis

$$|a_1| \leq |na_n| \text{ (resp. } < |na_n|).$$

Ceci montre que la série de puissances de f' admet $r = 1$ (resp. un rayon < 1) comme rayon critique. Il en résulte que f' doit s'annuler dans $B_{\leq 1}$ (resp. $B_{<1}$) et le théorème est complètement démontré.

■

On en déduit la version du développement limité avec point intermédiaire.

Corollaire 1. *Si $f \in \mathbb{C}_p[[x]]$ possède un rayon de convergence $r_f > 1$, alors pour tout couple de points a, b de $B_{\leq 1}$ satisfaisant $|a - b| \leq r_p$, il existe un point ξ de la boule unité B avec*

$$f(b) - f(a) = (b - a) \cdot f'(\xi).$$

Corollaire 2. *Si $f \in \mathbb{C}_p\{x\}$ et $|a - b| < r_p$, il existe $\xi \in B_{<1}$ avec*

$$f(b) - f(a) = (b - a) \cdot f'(\xi).$$

Preuve: Comme dans le cas classique, on considérera la fonction

$$\varphi(x) = \begin{vmatrix} f(a) & f(x) & f(b) \\ a & x & b \\ 1 & 1 & 1 \end{vmatrix}$$

qui s'annule en $x = a$ et $x = b$ et dont la dérivée

$$\varphi'(x) = \begin{vmatrix} f(a) & f'(x) & f(b) \\ a & 1 & b \\ 1 & 0 & 1 \end{vmatrix}$$

doit s'annuler dans la boule correspondant à la situation ...

Exemple: Prenons $f = x^p - px$ et choisissons une racine $(p-1)$-ième de p dans $\mathbb{C}_p$. Alors f s'annule en

$$x = 0 \text{ et } x \in \mu_{p-1} \cdot p^{1/(p-1)}.$$

Deux racines distinctes de f sont donc à distance r_p. Les zéros de f' sont les zéros de $f'/p = x^{p-1} - 1$, donc les éléments de μ_{p-1}. Ces zéros sont sur la sphère unité. Plus généralement, si $f = x^{p^\nu} - p^\nu x$, les zéros de f' sont encore les racines de 1 d'ordre divisant $p^\nu - 1$ (donc situés sur la sphère unité), tandis que les zéros de f sont les éléments

$$0 \text{ et } \zeta \cdot p^{\nu/(p^\nu - 1)} \text{ (où } \zeta \in \mu_{p^\nu - 1}).$$

REFERENCES:

[1] Dieudonné J. : Sur les fonctions analytiques p-adiques,
Bulletin des Sc. Math. 2e série t. 58 (mai-Juin 1944) p. 79-95
[Chois d'oeuvres mathématiques, Hermann 1981, vol. 1, p. 177-192].

[2] Girstmair K. : A Theorem on the Numerators of the Bernoulli Numbers, *The American Math. Monthly vol. 97, nb. 2, 1990 pp. 136-138.*

[3] Robert A. : A Note on the Numerators of the Bernoulli Numbers,
Expositiones Math. 9 (1991), pp. 189-191.

[4] Weil A. : Basic Number Theory. *Springer Verlag (1967).*

[5] Zuber M. : Propriétés p-adiques de polynômes classiques,
Thèse 1992. Inst. de Mathématiques. CH-2007 Neuchâtel.

Alain Robert
Institut de Mathématiques
Emile-Argand 11
CH-2007 NEUCHATEL
(Suisse)