Congruences par l'analyse p-adique et le calcul symbolique

THÈSE

présentée à la Faculté des Sciences pour
obtenir le grade de docteur ès sciences

par
Alexandre Junod

sous la direction du
Professeur Alain Robert

Institut de Mathématiques, Université de Neuchâtel
Rue Emile-Argand 11, CH-2007 Neuchâtel (Suisse)

IMPRIMATUR POUR LA THESE

Congruences par l'analyse p-adique et le calcul symbolique

de M. Alexandre Junod

UNIVERSITE DE NEUCHATEL

FACULTE DES SCIENCES

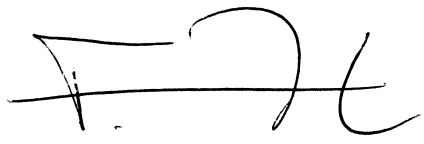
La Faculté des sciences de l'Université de Neuchâtel, sur le rapport des membres du jury

MM. A. Robert (directeur de thèse),
F. Sigrist, M. Zuber, C. Radoux (Mons B)
et D. Barsky (Paris)

autorise l'impression de la présente thèse.

Neuchâtel, le 12 juin 2003

Le doyen:



François Zwahlen

Congruences par l'analyse p-adique et le calcul symbolique

THÈSE

présentée à la Faculté des Sciences pour
obtenir le grade de docteur ès sciences

par
Alexandre Junod

sous la direction du
Professeur Alain Robert

Institut de Mathématiques, Université de Neuchâtel
Rue Emile-Argand 11, CH-2007 Neuchâtel (Suisse)

"Il n'est pas nécessaire qu'un problème de maths ait des applications pratiques pour qu'il soit intéressant et il peut être très agréable pour l'esprit d'essayer de résoudre des questions apparemment futiles."

Axel Thue

Introduction

Le présent travail est subdivisé en trois parties relativement indépendantes ayant pour point commun d'établir des congruences pour diverses suites classiques de nombres et de polynômes. Il reprend et complète les articles [15],[16] et [17]. Le premier chapitre utilise quelques méthodes d'*analyse p-adique*, notamment le *théorème des accroissements finis*, mais les techniques employées sont surtout issues du *calcul symbolique*, appelé parfois *calcul ombral*. Les origines de cette théorie sont assez floues. Utilisé sans grande rigueur depuis le début du XIXème siècle, le calcul symbolique a été développé par John Blissard vers 1860 mais il a fallu attendre près d'un siècle pour que E.T. Bell en donne des fondations rigoureuses (vers 1940) et pour que Gian-Carlo Rota [35][36] en fasse une théorie vraiment convaincante (vers 1970). L'idée de base consiste à relier une suite $\alpha = (\alpha_n)_{n\geqslant 0}$ (dans un anneau $\mathcal{A}$ commutatif unitaire intègre, éventuellement un anneau de polynômes) à la base canonique $(x^n)_{n\geqslant 0}$ de $\mathcal{A}[x]$ par une application linéaire $\Phi : x^n \longmapsto \alpha_n$, appelée *ombre de* α (le terme est dû à Sylvester). L'étude de la suite α se fait alors au travers de celle de son ombre. Certaines propriétés, comme les congruences, se transportent très bien par Φ. Par exemple, si $f(x) \equiv g(x) \mod m\mathcal{A}[x]$, alors $\Phi(f(x)) \equiv \Phi(g(x)) \mod m\mathcal{A}$. Ceci explique notre intérêt pour le calcul symbolique dans la théorie des congruences.

1ère partie : *Polynômes d'Euler et de Bernoulli généralisés*

Tout a véritablement commencé en été 1999 lorsque Maxime Zuber énonca une conjecture dans une lettre adressée à Alain Robert. Sur la base de son travail de doctorat [40], il pressentait que les polynômes d'Euler généralisés $E_n^r(t)$, définis par la fonction génératrice

$$\sum_{n\geqslant 0} E_n^r(t)\frac{x^n}{n!} = \Big(\frac{2}{e^x+1}\Big)^r e^{xt},$$

vérifient des congruences *de type Honda* : $E_{np}^r(t) \equiv E_n^r(t^p) \mod np\mathbb{Z}_p[t]$ pour tous les entiers $n, r \geqslant 0$ et tout nombre premier p impair. Cette affirmation ayant été démontrée, un

deuxième défi fut lancé : trouver une congruence analogue pour les polynômes de Bernoulli généralisés $B_n^r(t)$ définis par la relation

$$\sum_{n\geqslant 0} B_n^r(t)\frac{x^n}{n!} = \Big(\frac{x}{e^x-1}\Big)^r e^{xt}.$$

Deux ans après ces premiers résultats, en les reprenant dans le but d'en faire un article, il apparaît que les congruences obtenues pour ces deux suites généralisées découlent directement des cas particuliers ($r = 1$) découverts par Zuber. L'argument consiste à montrer que pour un nombre premier p fixé, les suites $(a_n)_{n\geqslant 0}$ dans $\mathbb{Z}_p$ qui vérifient

$$a_{m+np} \equiv a_{m+n} \mod \frac{np}{2}\mathbb{Z}_p \text{ pour tous les entiers } m, n \geqslant 0$$

constituent un anneau pour l'addition usuelle et le produit de convolution binomial.

La version p-adique du théorème des accroissements finis, que l'on doit à Alain Robert [31], tient le rôle principal dans ce premier chapitre et permet au passage d'affiner élégamment plusieurs résultats connus sur les nombres de Bernoulli ordinaires.

2ème partie : *Nombres et polynômes de Bell*

La série $\kappa = \sum n!$ converge dans $\mathbb{Z}_p$ (puisque son terme général tend p-adiquement vers zéro) mais la valeur n'est à ce jour pas encore connue. Une conjecture dit qu'il s'agirait d'un nombre irrationnel, voire d'un nombre transcendant. Pour notre part, nous cherchons à montrer que κ est une unité p-adique (i.e. κ est multiplicativement inversible dans $\mathbb{Z}_p$) pour tout nombre premier $p \neq 2$. En d'autres termes, nous nous intéressons à la

Conjecture de Kurepa ("Left Factorial Hypothesis")
Aucun nombre premier impair p ne divise la somme $\kappa_p = 0! + 1! + \cdots + (p-1)!$.

Comme souvent en théorie des nombres, cet énoncé est d'une grande simplicité mais la démonstration ne semble pas facile pour autant puisqu'elle résiste depuis près de trente ans à plusieurs mathématiciens, des disciples de Kurepa issus des pays de l'Est pour la plupart. Peu connu en Europe occidentale, Đuro Kurepa (1907-1993) a eu en réalité une énorme influence sur le développement des mathématiques en Yougoslavie et a contribué dans divers domaines, notamment en théorie des ensembles, topologie générale, théorie des nombres et algèbre [19].

Cette deuxième partie fait suite aux travaux d'Anne Gertsch Hamadene [9] qui établit entre autre un lien entre κ_p et les nombres de Bell. Nous reprenons le cadre du calcul ombral dans lequel elle s'était placée afin d'étudier plus généralement les polynômes de Bell $B_n(x)$. Nous

montrons tout d'abord que ces polynômes engendrent de manière naturelle une famille de produits scalaires et construisons les systèmes de polynômes orthogonaux associés. Nous établissons ensuite

$$B_{m+np^\nu}(x) \equiv \sum_{k=0}^{n} \binom{n}{k} (x^p + x^{p^2} + \cdots + x^{p^\nu})^{n-k} B_{m+k}(x) \bmod \frac{np}{2}\mathbb{Z}_p[x]$$

pour tout nombre premier p et tous les entiers $m, n, \nu \geqslant 0$. Nous généralisons ainsi de nombreuses congruences bien connues pour les polynômes et nombres de Bell (Comtet-Zuber [8], Touchard, Radoux [21][22][23], Carlitz [3]) et déduisons des congruences pour les nombres de Stirling des deux espèces [13] ainsi que pour les polynômes de Bell à deux variables [20]. Nous donnons également une généralisation des congruences de Radoux [22], redécouvertes par Kahale [18], ainsi que de la "formule de trace" de Barsky-Benzaghou [4]. Les polynômes de Bell sont prolongés de manière naturelle à des indices négatifs. Nous obtenons en particulier $B_{-1}(x^{-1}) = x\sum_{k\geqslant 0} k!x^k$, ce qui établit un lien avec les ensembles

$$E(p) = \Big\{1 \leqslant a \leqslant p-1 \ : \ p \text{ ne divise pas } \kappa_p(a) = \sum_{k=0}^{p-1} k!a^k\Big\}$$

et la conjecture de Kurepa revient à dire que $1 \in E(p)$ pour tout p premier $\neq 2$. Afin d'éclaircir les travaux de Dragovitch [9], nous montrons finalement que pour toute unité p-adique $a \in \mathbb{Z}_p$, les séries

$$v_n(a) = \sum_{k\geqslant 0} k!a^k\big(k^n + a(-1)^n B_{n+1}(-a^{-1})\big) \quad (n \geqslant 0)$$

sont des sommes finies (dans $\mathbb{Z}_p$) et décrivent donc des entiers lorsque $a = \pm 1$.

3ème partie : *Déterminants de Hankel et polynômes orthogonaux*

Au cours de la deuxième partie, nous avons rencontré des matrices dites de Hankel, de la forme

$$H_n = \begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_n \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{n+1} \\ \vdots & \vdots & & \vdots \\ \alpha_n & \alpha_{n+1} & \cdots & \alpha_{2n} \end{pmatrix}$$

A partir des divers articles de Christian Radoux [27][28], nous étudions de manière plus détaillée de telles matrices et donnons une méthode pour évaluer leurs déterminants en admettant certaines conditions sur la fonction génératrice exponentielle (ou ordinaire) associée à la suite $(\alpha_n)_{n\geqslant 0}$. Plusieurs cas particuliers bien connus sont ainsi déduits dans un

contexte unifié (polynômes de Bell et d'Hermite, polynômes de dérangement et d'involution, nombres de Catalan, de Motzkin et d'Euler ...). Lorsque les matrices de Hankel associées à une même suite dans $\mathbb{R}$ ont des déterminants tous positifs, elles engendrent alors un produit scalaire et donnent donc lieu à un système de polynômes orthogonaux. Nous nous inspirons de ce fait pour définir des "produits scalaires généralisés" ainsi que des "systèmes de polynômes orthogonaux associés", et montrons comment ces polynômes peuvent servir à établir des congruences pour la suite des moments $(\alpha_n)_{n\geqslant 0}$. En guise d'illustration, nous retrouvons des congruences déjà établies dans les deux premiers chapitres pour les nombres d'Euler et les polynômes de Bell. La méthode proposée dans ce chapitre nous paraît très prometteuse pour établir de nouvelles congruences et traiter la conjecture de Kurepa par les nombres de Bell. Après avoir rappelé que les déterminants de Hankel permettent également de savoir si la fonction génératrice $\sum \alpha_n z^n$ décrit ou non une fonction rationnelle [2], nous faisons le lien entre les résultats obtenus et les "chaînes à accroissements pondérés" pour leur donner une signification combinatoire.

Remerciements

En premier lieu, je tiens à exprimer toute ma reconnaissance à mon directeur de thèse, Alain Robert, avec qui j'ai eu un énorme plaisir à travailler. Outre sa grande culture générale et mathématique, j'ai particulièrement apprécié son souci de pédagogie et son goût pour les raisonnements clairs et subtils qu'il aimait partager lors des pauses-café.

Je remercie vivement les Professeurs Daniel Barsky, Christian Radoux, François Sigrist et Maxime Zuber d'avoir accepté de composer mon jury et de l'intérêt qu'ils ont témoigné pour ce travail. Des remerciements plus particuliers sont adressés à Maxime Zuber, qui a motivé par quelques conjectures la première partie de cette thèse, ainsi qu'à Anne Gertsch Hamadene dont les travaux ont constitué la base de mes recherches pour la deuxième partie. Son soutien et ses encouragements constants m'ont été très précieux.

Merci également à tous les collègues, professeurs et assistants, qui contribuent à une ambiance chaleureuse au sein de l'Institut de Maths et en font un lieu de travail très agréable.

Je remercie ma famille et plus particulièrement mes parents pour le soutien moral et financier qu'ils m'ont apporté durant mes études. Ce travail leur est entièrement dédié.

Pour conclure, merci à tous mes amis, musiciens ou autres, pour les moments de détente qui ne doivent pas être négligés dans la "vie psychologique" de tout chercheur ...

Neuchâtel, juin 2003 Alexandre Junod

Table des matières

Partie 1

Polynômes d'Euler et de Bernoulli généralisés

"Est rigoureuse toute démonstration, qui, chez tout lecteur suffisamment instruit et préparé, suscite un état d'évidence qui entraîne l'adhésion."

René Thom

1.1 Définitions et premières propriétés

On désigne par p un nombre premier quelconque et par $\mathbb{Z}_p$ l'anneau des entiers p-adiques, complété de $\mathbb{Z}$ pour la valeur absolue p-adique $|\cdot|$ normalisée par $|p| = p^{-1}$. Comme on n'aura affaire qu'à des entiers p-adiques rationnels, on pourra remplacer $\mathbb{Z}_p$ par l'anneau des nombres p-entiers formé des rationnels (irréductibles) dont le dénominateur n'est pas divisible par p. Cet anneau est dénoté par $\mathbb{Z}_{(p)} = \mathbb{Z}_p \cap \mathbb{Q}$.

Les *polynômes d'Euler* $E_n^r(t)$ d'ordre $r \in \mathbb{N}$ sont définis par la fonction génératrice

$$e_r(x,t) := \Big(\frac{2}{e^x+1}\Big)^r e^{xt} = \sum_{n\geqslant 0} E_n^r(t)\frac{x^n}{n!}$$

et les *polynômes de Bernoulli* $B_n^r(t)$ d'ordre r sont définis par

$$b_r(x,t) := \Big(\frac{x}{e^x-1}\Big)^r e^{xt} = \sum_{n\geqslant 0} B_n^r(t)\frac{x^n}{n!}\ .$$

On a $E_n^0(t) = B_n^0(t) = t^n$ et en prenant $r = 1$, on retrouve les polynômes d'Euler $E_n(t)$ et de Bernoulli $B_n(t)$ ordinaires. Les notations standards sont $E_n^{(r)}(t)$ et $B_n^{(r)}(t)$ mais nous laissons tomber le parenthésage de r (en prenant soin de ne pas considérer par exemple $E_n^r(t)$ comme une puissance de $E_n(t)$). Les premiers polynômes sont

$E_0^r(t) = 1$	$B_0^r(t) = 1$
$E_1^r(t) = t - \frac{r}{2}$	$B_1^r(t) = t - \frac{r}{2}$
$E_2^r(t) = t^2 - rt + \frac{r(r-1)}{4}$	$B_2^r(t) = t^2 - rt + \frac{r(3r-1)}{12}$
$E_3^r(t) = t^3 - \frac{3r}{2}t^2 + \frac{3r(r-1)}{4}t - \frac{(r-3)r^2}{8}$	$B_3^r(t) = t^3 - \frac{3r}{2}t^2 + \frac{r(3r-1)}{4}t - \frac{r^2(r-1)}{8}$

Signalons au passage que les polynômes de Bernoulli peuvent être exprimés récursivement par une *intégrale de Volkenborn* : pour tout nombre premier p, on a

$$B_n^{r+1}(t) = \int_{\mathbb{Z}_p} B_n^r(t+x)dx := \lim_{m\longrightarrow\infty} \frac{B_n^r(t) + B_n^r(t+1) + \cdots + B_n^r(t+p^m-1)}{p^m}.$$

En effet, la fonction génératrice des intégrales proposées est donnée formellement par

$$\int_{\mathbb{Z}_p} \Big(\sum B_n^r(t+x)\frac{z^n}{n!}\Big)dx = \Big(\frac{z}{e^z-1}\Big)^r e^{zt}\int_{\mathbb{Z}_p} e^{zx}dx = \Big(\frac{z}{e^z-1}\Big)^{r+1} e^{zt}$$

et coïncide avec celle de la suite $B_n^{r+1}(t)$. On pourra se référer à [31] ou [37] pour de plus amples informations sur les intégrales de Volkenborn et sur les nombres de Bernoulli ordinaires $B_n = B_n^1(0)$ avec cette optique.

Les relations $\frac{\partial}{\partial t}e_r(x,t) = xe_r(x,t)$ et $\frac{\partial}{\partial t}b_r(x,t) = xb_r(x,t)$ montrent déjà que

$$\big\{\ E_0^r(t)' = 0\ ,\ E_n^r(t)' = nE_{n-1}^r(t)\ \big\} \quad \text{resp.} \quad \big\{\ B_0^r(t)' = 0\ ,\ B_n^r(t)' = nB_{n-1}^r(t)\ \big\}.$$

Autrement dit, les polynômes $(E_n^r(t))_{n\geqslant 0}$ et $(B_n^r(t))_{n\geqslant 0}$ forment des *familles d'Appell* et leurs séries de Taylor en un point a sont données par

$$E_n^r(t) = \sum_{k=0}^{n}\binom{n}{k}E_k^r(a)(t-a)^{n-k} \quad \text{resp.} \quad B_n^r(t) = \sum_{k=0}^{n}\binom{n}{k}B_k^r(a)(t-a)^{n-k}.$$

De manière plus générale, en identifiant les termes de même degré dans les égalités

$$e_{r+s}(x,a+b) = e_r(x,a)e_s(x,b) \quad \text{resp.} \quad b_{r+s}(x,a+b) = b_r(x,a)b_s(x,b),$$

nous obtenons

$$E_n^{r+s}(a+b) = \sum_{k=0}^{n}\binom{n}{k}E_k^r(a)E_{n-k}^s(b) \quad \text{resp.} \quad B_n^{r+s}(a+b) = \sum_{k=0}^{n}\binom{n}{k}B_k^r(a)B_{n-k}^s(b)$$

et le choix $s=0$, $b=t-a$ confirme les développements de Taylor. De la relation

$$b_r\Big(2x, \frac{a+b}{2}\Big) = \Big(\frac{2x}{e^{2x}-1}\Big)^r e^{x(a+b)} = \Big(\frac{x}{e^x-1}\Big)^r e^{ax}\Big(\frac{2}{e^x+1}\Big)^r e^{bx} = b_r(x,a)e_r(x,b)$$

découle une formule qui relie les deux familles de polynômes :

$$B_n^r\Big(\frac{a+b}{2}\Big) = \frac{1}{2^n}\sum_{k=0}^{n}\binom{n}{k}B_k^r(a)E_{n-k}^r(b)$$

(on remarquera que le choix $a=b=t$ est particulièrement intéressant). Les identités

$$e_r(-x,t) = \Big(\frac{2}{e^{-x}+1}\Big)^r e^{-xt} = \Big(\frac{2e^x}{e^x+1}\Big)^r e^{-xt} = \Big(\frac{2}{e^x+1}\Big)^r e^{x(r-t)} = e_r(x,r-t)$$

$$b_r(-x,t) = \Big(\frac{-x}{e^{-x}-1}\Big)^r e^{-xt} = \Big(\frac{xe^x}{e^x-1}\Big)^r e^{-xt} = \Big(\frac{x}{e^x-1}\Big)^r e^{x(r-t)} = b_r(x,r-t)$$

donnent lieu aux relations

$$(-1)^n E_n^r(t) = E_n^r(r-t) \quad \text{resp.} \quad (-1)^n B_n^r(t) = B_n^r(r-t).$$

Elles montrent en particulier que $E_n^r(r/2)$ et $B_n^r(r/2)$ sont nuls pour tout indice n impair. Nous pouvons encore remarquer que les formules

$$e_r(x,t+1) + e_r(x,t) = \Big(\frac{2}{e^x+1}\Big)^r e^{xt}(e^x+1) = 2\Big(\frac{2}{e^x+1}\Big)^{r-1} e^{xt} = 2e_{r-1}(x,t)$$

$$b_r(x,t+1) - b_r(x,t) = \Big(\frac{x}{e^x-1}\Big)^r e^{xt}(e^x-1) = x\Big(\frac{x}{e^x-1}\Big)^{r-1} e^{xt} = xb_{r-1}(x,t)$$

fournissent respectivement

$$E_n^r(t+1)+E_n^r(t)=2E_n^{r-1}(t) \quad \text{et} \quad B_n^r(t+1)-B_n^r(t)=nB_{n-1}^{r-1}(t)=B_n^{r-1}(t)'.$$

Par sommes téléscopiques, on en déduit

$$\frac{(-1)^N E_k^r(N)-E_k^r(0)}{2}=\sum_{l=0}^{N-1}\frac{(-1)^{l+1}}{2}(E_k^r(l+1)+E_k^r(l))=\sum_{l=0}^{N-1}(-1)^{l+1}E_k^{r-1}(l),$$

$$\frac{B_{k+1}^r(N)-B_{k+1}^r(0)}{k+1}=\sum_{l=0}^{N-1}\frac{B_{k+1}^r(l+1)-B_{k+1}^r(l)}{k+1}=\sum_{l=0}^{N-1}B_k^{r-1}(l).$$

Mentionnons finalement une dernière propriété plus particulière que nous invoquerons à plusieurs reprises par la suite. Il s'agit de l'*identité de Raabe* (pour les nombres de Bernoulli ordinaires)

$$B_n(a)=a^{n-1}\sum_{k=0}^{a-1}B_n\Big(1+\frac{k}{a}\Big),$$

que l'on démontre simplement en comparant les fonctions génératrices.

1.2 Théorème des accroissements finis

Le théorème p-adique des accroissements finis découvert par A. Robert [31] occupe une place primordiale dans ce premier chapitre. Nous en rappelons l'énoncé pour les polynômes.

Théorème (TAF). *On considère un espace de Banach ultramétrique $(\mathbb{E},|\cdot|)$ sur un corps complet $\mathbb{K}$, un polynôme $f(t)\in\mathbb{E}[t]$ à coefficients dans $\mathbb{E}$ et deux éléments $h,a\in\mathbb{E}$ avec $|a|\leqslant 1$. On munit $\mathbb{E}[t]$ de la norme de Gauss $\|\sum a_k t^k\|_{\mathbb{E}[t]}=\max\{|a_k|:k\geqslant 0\}$.*

1. *si $|h|\leqslant|p|^{1/(p-1)}$, alors $|f(a+h)-f(a)|\leqslant|h|\cdot\|f'\|_{\mathbb{E}[t]}$,*
2. *si p est impair et $|h|\leqslant|p|^{1/(p-2)}$, alors $|f(a+h)-f(a)-hf'(a)|\leqslant|\frac{h^2}{2}|\cdot\|f''\|_{\mathbb{E}[t]}$, la même conclusion étant valable dans le cas $p=2$ dès que $|h|\leqslant|2|^{1/2}$.*

De manière plus générale, le théorème est valable pour le sous-anneau de $\mathbb{E}[[t]]$ regroupant les séries formelles dont les coefficients tendent (pour la norme $|\cdot|$) vers 0 : cet ensemble est le complété de $\mathbb{E}[t]$ pour la norme de Gauss.

En guise de premier exemple, fixons-nous un entier p-adique $a\in\mathbb{Z}_p$ et considérons le polynôme

$$f(t)=(r(x)t+x^p+a^p)^n \quad \text{avec} \quad r(x)=\frac{(x+a)^p-x^p-a^p}{p} \quad \text{et } n\geqslant 1.$$

Comme $r(x) \in \mathbb{Z}[x] \subset \mathbb{Q}_p[x]$, les coefficients de $f(t)$ se trouvent dans le $\mathbb{Q}_p$-espace de Banach $\mathbb{E} = \{g(x) \in \mathbb{Q}_p[x] \ : \ \deg g \leqslant np\} \subset \mathbb{Q}_p[x]$. Le TAF du premier ordre dit alors que

$$|f(p) - f(0)| \leqslant |p| \cdot \|f'\| = |p| \cdot \|nr(x)(r(x)t + x^p + a^p)^{n-1}\| \leqslant |np|.$$

Cela signifie que $f(p) - f(0) = (x+a)^{np} - (x^p + a)^n$ se trouve dans $np\mathbb{Z}_p[x]$, ce qui pour $a = 1$ revient à dire (en identifiant les coefficients) que

$$\binom{np}{kp} \equiv \binom{n}{k} \bmod np\mathbb{Z}_p \ \text{ et } \ \binom{np}{k} \equiv 0 \bmod np\mathbb{Z}_p \ \text{ si } p \nmid k.$$

Alors que la deuxième congruence est évidente, la première sera d'une très grande utilité pour la suite. On peut évidemment affiner ces résultats avec le TAF d'ordre 2 : en prenant $a = 1$, on obtient

$$(1+x)^{np} - (1+x^p)^n \equiv np(1+x^p)^{n-1} r(x) \bmod \frac{n(n-1)p^2}{2}\mathbb{Z}_p[x]$$

et en identifiant les coefficients devant x^{kp}, on trouve alors $\binom{np}{kp} \equiv \binom{n}{k} \bmod \frac{n(n-1)p^2}{2}\mathbb{Z}_p$. G.S. Kazandzidis améliore encore cette congruence pour p impair en montrant qu'elle est valable modulo $\frac{n^2(n-1)p^3}{3}\binom{n-2}{k-1}\mathbb{Z}_p$ (voir [31] ou [32] pour une preuve).

Nous avons déjà remarqué que les polynômes d'Euler et de Bernoulli généralisés formaient des suites d'Appell. Le résultat suivant, que l'on doit à M. Zuber [40], est donc le bienvenu pour établir des congruences.

Théorème 1. *Pour une famille de polynômes d'Appell $(A_n(t))_{n\geqslant 0}$ dans $\mathbb{Z}_p[t]$, les assertions suivantes sont équivalentes :*

1) $A_{np}(t) \equiv A_n(t^p) \bmod np\mathbb{Z}_p[t]$ pour tout $n \geqslant 0$,

2) il existe $a \in \mathbb{Z}_p$ pour lequel $A_{np}(a) \equiv A_n(a^p) \bmod np\mathbb{Z}_p$ pour tout $n \geqslant 0$,

3) il existe $a \in \mathbb{Z}_p$ pour lequel $A_{np}(a) \equiv A_n(a) \bmod np\mathbb{Z}_p$ pour tout $n \geqslant 0$.

PREUVE. La démonstration originale de [40] est élémentaire mais nous en présentons ici une simplification qui évite d'introduire "l'identité de Spitzer" et "le théorème de Barsky". L'implication 1) $\Longrightarrow$ 2) est évidente et 2) $\Longrightarrow$ 3) se démontre avec le TAF en utilisant la propriété d'Appell : $|A_n(a^p) - A_n(a)| \leqslant |a^p - a| \cdot \|nA_{n-1}\| \leqslant |np|$ pour tout $n \geqslant 1$. On démontre 3) $\Longrightarrow$ 1) à l'aide du développement de Taylor au point a : on a

$$A_{np}(t) = \sum_{0\leqslant k\leqslant np}^{p\nmid k} \binom{np}{k} A_k(a)(t-a)^{np-k} + \sum_{k=0}^{n} \binom{np}{kp} A_{kp}(a)(t-a)^{np-kp}$$

et par l'exemple qui suit l'énoncé du TAF, on peut écrire

$$A_{np}(t) \equiv \sum_{k=0}^{n} \binom{n}{k} A_{kp}(a)(t-a)^{np-kp} \bmod np\mathbb{Z}_p[t].$$

Ce même exemple montre que $(t-a)^{lp} \equiv (t^p-a)^l \bmod lp\mathbb{Z}_p[t]$ (ceci est aussi confirmé par la proposition 1 du chapitre suivant). De plus, il est clair que dans $\mathcal{A} = \mathbb{Z}_p[t]$ (comme dans tout anneau commutatif qui contient $\mathbb{Z}$), si deux éléments α et β sont congrus modulo $kp\mathcal{A}$, alors $\binom{n}{k}\alpha$ et $\binom{n}{k}\beta$ sont congrus modulo $np\mathcal{A}$. Cette évidence permet d'écrire

$$A_{np}(t) \equiv \sum_{k=0}^{n} \binom{n}{k} A_k(a)(t^p-a)^{n-k} = A_n(t^p) \bmod np\mathbb{Z}_p[t],$$

et la dernière implication est démontrée. Remarquons qu'à partir d'une famille d'Appell quelconque dans $\mathbb{Z}_p[t]$, nous avons été ramenés à voir que la famille d'Appell particulière $f_n(t) = (t-a)^n$ (avec $a \in \mathbb{Z}_p$) vérifiait les assertions équivalentes du théorème. □

1.3 Polynômes d'Euler généralisés

Les coefficients de $E_n^r(t)$, donnés par $\binom{n}{m}E_m^r(0) = \binom{n}{m}2^r \frac{d^m}{dx^m}\big((1+e^x)^{-r}\big)\Big|_{x=0}$, appartiennent visiblement à $\mathbb{Z}[\frac{1}{2}]$ donc, pour p premier impair, on a $E_n^r(t) \in \mathbb{Z}[\frac{1}{2}][t] \subset \mathbb{Z}_p[t]$. Les congruences établies dans [40] se généralisent de la manière suivante.

Proposition 2. *Si p est impair, alors $E_{np}^r(t) \equiv E_n^r(t^p) \bmod np\mathbb{Z}_p[t]$ pour tout $n \geqslant 0$.*

PREUVE. L'assertion est vérifiée pour $r = 0$ (on a même l'égalité $E_{np}^0(t) = t^{np} = E_n^0(t^p)$) et par induction, supposons qu'elle le soit pour $r-1 \geqslant 0$. Pour tout entier p-adique $k \in \mathbb{Z}_p$, on a donc

$$E_{np}^{r-1}(k) \equiv E_n^{r-1}(k^p) \equiv E_n^{r-1}(k) \bmod np\mathbb{Z}_p,$$

la deuxième congruence découlant du TAF : $|E_n^{r-1}(k^p) - E_n^{r-1}(k)| \leqslant |k^p-k| \cdot \|nE_{n-1}^{r-1}\| \leqslant |np|$. Ainsi, pour un entier fixé $N \geqslant 1$, nous avons

$$2\sum_{k=0}^{N-1}(-1)^{k+1}E_{np}^{r-1}(k) \equiv 2\sum_{k=0}^{N-1}(-1)^{k+1}E_n^{r-1}(k) \bmod np\mathbb{Z}_p,$$

autrement dit $(-1)^N E_{np}^r(N) - E_{np}^r(0) \equiv (-1)^N E_n^r(N) - E_n^r(0)$ modulo $np\mathbb{Z}_p$, ou encore $(-1)^N[E_{np}^r(N) - E_n^r(N)] \equiv E_{np}^r(0) - E_n^r(0) \bmod np\mathbb{Z}_p$.

Si on considère un entier $N = r + lp$ (avec $l \in \mathbb{Z}$), le TAF fournit alors $E_{np}^r(N) \equiv E_{np}^r(r)$ et $E_n^r(N) \equiv E_n^r(r)$ modulo $np\mathbb{Z}_p$. On obtient ainsi

$$E_{np}^r(0) - E_n^r(0) \equiv (-1)^N[E_{np}^r(N) - E_n^r(N)] \equiv (-1)^N[E_{np}^r(r) - E_n^r(r)] \bmod np\mathbb{Z}_p$$

et par le fait que $E_n^r(r) = (-1)^n E_n^r(0)$, il suit

$$E_{np}^r(0) - E_n^r(0) \equiv (-1)^N[(-1)^{np}E_{np}^r(0) - (-1)^n E_n^r(0)] \bmod np\mathbb{Z}_p.$$

Comme p est impair, on peut choisir $l \in \mathbb{N}$ de manière à ce que $N = r + lp$ et n soient de parité différente (il suffit de prendre $l = 0$ ou 1 selon la parité de $n + r + 1$). Cela nous conduit à la congruence

$$E^r_{np}(0) - E^r_n(0) \equiv (-1)^{N+n}[E^r_{np}(0) - E^r_n(0)] = -[E^r_{np}(0) - E^r_n(0)] \bmod np\mathbb{Z}_p.$$

On a donc $E^r_{np}(0) \equiv E^r_n(0) \bmod np\mathbb{Z}_p$ pour tout entier $n \geqslant 0$ (pour $r \geqslant 0$ fixé) et on conclut par le théorème. □

Proposition 3. *Soient p un nombre premier impair, $a \in \mathbb{Z}_p$ et $n, r \geqslant 0$. Alors*

$$E^r_{m+np}(a) \equiv E^r_{m+n}(a) \bmod np\mathbb{Z}_p \quad \textit{pour tout} \quad m \geqslant 0.$$

PREUVE. Le cas $m = 0$ découle de la proposition précédente et de l'inégalité

$$|E^r_n(a^p) - E^r_n(a)| \leqslant |a^p - a| \cdot \|nE^r_{n-1}\| \leqslant |np| \quad \text{pour} \quad n \geqslant 1.$$

D'autre part, en dérivant $e_r(x,t)$ par rapport à x, on trouve

$$\partial_x e_r(x,t) = 2^r e^{xt}\frac{t(e^x+1) - re^x}{(e^x+1)^{r+1}} = 2^r e^{xt}\frac{(t-r)(e^x+1)+r}{(e^x+1)^{r+1}} = (t-r)e_r(x,t) + \frac{r}{2}e_{r+1}(x,t),$$

autrement dit $E^r_{n+1}(a) = (a-r)E^r_n(a) + \frac{r}{2}E^{r+1}_n(a)$. La proposition se démontre alors par induction sur m, à l'aide de cette formule. □

En particulier, pour tout $a \in \mathbb{Z}_p$, la suite $(E^r_n(a))_{n\geqslant 1}$ est $(p-1)$-périodique modulo $p\mathbb{Z}_p$:

$$E^r_{m+(p-1)}(a) = E^r_{(m-1)+p}(a) \equiv E^r_{(m-1)+1}(a) = E^r_m(a) \bmod p\mathbb{Z}_p \quad \text{pour tout } m \geqslant 1.$$

1.4 Nombres de Bernoulli

La version p-adique du théorème des accroissements finis permet d'améliorer aisément plusieurs résultats connus sur les nombres de Bernoulli ordinaires.

Théorème 4. *Pour $n \geqslant 1$, le nombre de Bernoulli ordinaire $B_n = B^1_n(0)$ vérifie*

$$pB_n \equiv \sum_{k=1}^{p-1} k^n \equiv \begin{cases} 0 & \textit{si } (p-1) \nmid n \\ p-1 & \textit{si } (p-1) \mid n \end{cases} \bmod \frac{np}{2}\mathbb{Z}_p.$$

PREUVE. L'assertion est vérifiée pour $n = 1$ ($B_1 = -1/2$) et, procédant par induction, supposons qu'elle le soit pour tout indice strictement inférieur à $n \geqslant 2$. On considère alors

le polynôme $f(t) = \frac{B_{n+1}(t)}{n+1} \in \mathbb{Q}_p[t]$, dont les deux premières dérivées sont $f'(t) = B_n(t)$ et $f''(t) = nB_{n-1}(t)$. Le TAF permet d'écrire

$$\left|\frac{B_{n+1}(p) - B_{n+1}}{n+1} - pB_n\right| = |f(p) - f(0) - pf'(0)| \leqslant \left|\frac{p^2}{2}\right| \cdot \|f''\| = \left|\frac{np}{2}\right| \cdot \|pB_{n-1}(t)\|.$$

Par hypothèse d'induction et le fait que $B_0 = 1 \in \mathbb{Z}_p$, on a

$$\big\|pB_{n-1}(t)\big\| = \max\left\{\left|\binom{n-1}{k} pB_k\right| \ : \ k = 0, 1, \ldots, n-1\right\} \leqslant 1$$

et il suit que

$$pB_n - \frac{B_{n+1}(p) - B_{n+1}}{n+1} = pB_n - \sum_{k=1}^{p-1} k^n$$

se trouve dans $(np/2)\mathbb{Z}_p$. Nous concluons comme dans [33] : le lemme de Hensel assure l'existence (et l'unicité) d'éléments $\zeta_1, \ldots, \zeta_{p-1} \in \mathbb{Z}_p^\times$ tels que $\zeta_k^{p-1} = 1$ et $\zeta_k \equiv k \mod p\mathbb{Z}_p$. En appliquant le TAF au polynôme $f(t) = t^n$, on trouve $|\zeta_k^n - k^n| \leqslant |\zeta_k - k| \cdot \|f'\| \leqslant |np|$, autrement dit, $\zeta_k^n \equiv k^n \mod np\mathbb{Z}_p$. L'ensemble $\{\zeta_1, \ldots, \zeta_{p-1}\} \subset \mathbb{Z}_p^\times$ des racines $(p-1)^{\text{èmes}}$ de l'unité formant un groupe cyclique, il est engendré par les puissances d'un élément ζ, de sorte que, modulo $(np/2)\mathbb{Z}_p$ (et même modulo $np\mathbb{Z}_p$), la somme

$$\sum_{k=1}^{p-1} k^n \equiv \sum_{k=1}^{p-1} \zeta_k^n = \sum_{k=0}^{p-2} (\zeta^n)^k = \frac{1 - \zeta^{n(p-1)}}{1 - \zeta^n}$$

est nulle si n n'est pas un multiple de $p-1$ et vaut $p-1$ sinon. □

De ce théorème découlent les résultats de Kummer et de Clausen-von Staudt

- Si $p-1$ ne divise pas n, alors $B_n \in n\mathbb{Z}_p$ et plus précisément $B_n(a) \in n\mathbb{Z}_p$ pour tout $a \in \mathbb{Z}_p$. On a aussi $pB_n \equiv -1 \mod p\mathbb{Z}_p$ lorsque $p-1$ divise n pair $\geqslant 2$.
- $B_n + \displaystyle\sum_{(p-1)|n} \frac{1}{p}$ est un nombre entier (pour tout n pair).

De plus, on sait que si $p-1$ ne divise pas $m \geqslant 2$, alors $\frac{B_{m+p-1}}{m+p-1} \equiv \frac{B_m}{m} \mod p\mathbb{Z}_p$. Ce résultat, également dû à Kummer, peut être amélioré comme suit :

Théorème 5. *Si $m \geqslant 1$ et $p-1$ ne divise pas $m+n$, alors on a la congruence*

$$\frac{B_{m+np}(a)}{m+np} \equiv \frac{B_{m+n}(a)}{m+n} \mod np\mathbb{Z}_p \quad \textit{pour tout entier p-adique } a \in \mathbb{Z}_p.$$

PREUVE. Comme $p-1$ ne divise pas $m+n$, le polynôme $R(t) := \dfrac{B_{m+np}(t)}{m+np} - \dfrac{B_{m+n}(t)}{m+n}$ décrit une fonction $\mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ et, pour un entier $N \geqslant 1$ donné, la dernière propriété énoncée

dans le premier paragraphe fournit

$$|R(N)-R(0)| = \Big|\sum_{k=0}^{N-1}(k^{m-1+np}-k^{m-1+n})\Big| \leqslant \max\{|k^{np}-k^n| \ : \ k=0,\dots,N-1\}.$$

En posant $x=0$ dans la congruence déjà établie $(x+k)^{np} \equiv (x^p+k)^n \bmod np\mathbb{Z}_p[x]$, on voit que $k^{np} \equiv k^n \bmod np\mathbb{Z}_p$ (on peut également démontrer ce fait en appliquant le TAF au polynôme $f(t)=t^n \in \mathbb{Q}_p[t]$), et il suit que $R(N) \equiv R(0) \bmod np\mathbb{Z}_p$. Ceci étant valable pour tout entier $N \geqslant 0$, l'application $\overline{R} : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p/np\mathbb{Z}_p$ est constante (par densité de $\mathbb{N}$ dans $\mathbb{Z}_p$). Considérons une unité p-adique $a \in \mathbb{Z}_p^\times$ afin que les termes $1+\frac{k}{a}$ $(k \geqslant 0)$ se trouvent dans $\mathbb{Z}_p$. En utilisant l'identité de Raabe et à nouveau le fait que $a^{np} \equiv a^n \bmod np\mathbb{Z}_p$, nous obtenons alors

$$R(0) \equiv R(a) \equiv a^{m-1+n}\sum_{k=0}^{a-1} R\Big(1+\frac{k}{a}\Big) \equiv a^{m+n}R(0) \bmod np\mathbb{Z}_p,$$

c'est-à-dire $(a^{m+n}-1)R(0) \equiv 0 \bmod np\mathbb{Z}_p$. Choisissons pour $a \in \{1,2,\dots,p-1\}$ un générateur du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$. De cette façon, $a^{m+n}-1$ est inversible dans $\mathbb{Z}_p$ (puisque $p-1$ ne divise pas $m+n$) et l'application $\overline{R}$ est identiquement nulle. □

La stratégie utilisée dans cette preuve permet d'établir d'autres congruences intéressantes.

Théorème 6. *Si c est divisible par $(p-1)p^s$ $(s \geqslant 0)$ et $p-1$ ne divise pas m, alors*

$$\sum_{k=0}^{n}\binom{n}{k}(-1)^{n-k}\frac{B_{m+kc}(a)}{m+kc} \in p^{\min\{m-1,n(s+1)\}}\mathbb{Z}_p$$

pour tout entier p-adique $a \in \mathbb{Z}_p$ et tout $n \in \mathbb{N}$.

PREUVE. Comme $p-1$ divise c mais pas m, le polynôme

$$Q(t) = \sum_{k=0}^{n}\binom{n}{k}(-1)^{n-k}\frac{B_{m+kc}(t)}{m+kc}$$

décrit une fonction $\mathbb{Z}_p \longrightarrow \mathbb{Z}_p$. Pour tout entier $N \geqslant 1$, on peut écrire

$$Q(N)-Q(0) = \sum_{k=0}^{n}\binom{n}{k}(-1)^{n-k}\sum_{l=0}^{N-1} l^{m-1+kc} = \sum_{l=0}^{N-1} l^{m-1}(l^c-1)^n$$

et on raisonne sur les indices intervenant dans cette dernière somme : si l est divisible par p, alors $l^{m-1} \in p^{m-1}\mathbb{Z}$. Dans le cas contraire, on a $l^{p-1} \equiv 1 \bmod p\mathbb{Z}$ et le TAF d'ordre 1 (appliqué au polynôme $f(t)=t^{c/(p-1)}$) donne $|l^c-1| \leqslant |cp|$, donc en particulier $l^c \equiv 1 \bmod p^{s+1}\mathbb{Z}$ et $(l^c-1)^n \in p^{n(s+1)}\mathbb{Z}$. Au total, ces considérations montrent que la

réduction $\overline{Q} : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p/p^{\min\{m-1,n(s+1)\}}\mathbb{Z}_p$ est constante (par densité de $\mathbb{N}$ dans $\mathbb{Z}_p$). Choisissons un entier $b \in \{1, 2, \dots, p-1\}$ générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ et considérons une puissance $a = b^q$ avec $\mathrm{ord}_p(q) \geqslant \min\{m-1, n(s+1)\}$. On a ainsi $|a^c - 1| \leqslant |qcp|$ et donc $a^c \equiv 1 \bmod p^{\min\{m-1,n(s+1)\}}\mathbb{Z}$. L'identité de Raabe nous donne alors

$$Q(0) \equiv Q(a) \equiv a^{m-1} \sum_{l=0}^{a-1} Q\Big(1 + \frac{k}{a}\Big) \equiv a^m Q(0) \bmod p^{\min\{m-1,n(s+1)\}}\mathbb{Z}_p$$

et comme $(a^m - 1)$ est inversible dans $\mathbb{Z}_p$ (puisque $p - 1$ ne divise pas m), il suit que l'application $\overline{Q}$ est identiquement nulle. □

Ce résultat se place dans le contexte général suivant que P.T. Young utilise dans [39] : on dénote par K une extension finie de $\mathbb{Q}_p$ et on considère la clôture intégrale de $\mathbb{Z}_p$ dans K, qui coïncide avec la boule unité $\mathcal{A} = B_{\leqslant 1}(0) := \{\alpha \in K \ : \ |\alpha| \leqslant 1\}$. Etant donné un entier positif $c \geqslant 0$ et une suite $(a_n)_{n\geqslant 0}$ dans $\mathcal{A}$, on regarde alors les puissances de l'opérateur Δ_c qui agit sur $(a_n)_{n\geqslant 0}$ par $\Delta_c a_m = a_{m+c} - a_m$. Afin de ne pas oublier le caractère linéaire de cet opérateur, il est commode d'introduire l'application linéaire $\Phi : \mathcal{A}[x] \longrightarrow \mathcal{A}$ définie sur la base canonique par $\Phi(x^n) = a_n$: on a ainsi $\Delta_c\Phi(f(x)) = \Phi((x^c - 1)f(x))$ pour tout polynôme $f(x) \in \mathcal{A}[x]$ (puisque ceci est par définition le cas pour tous les polynômes de la base canonique) et par itération, on trouve

$$\Delta_c^n a_m = \Delta_c^n \Phi(x^m) = \Phi(x^m(x^c - 1)^n) = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} a_{m+kc}.$$

On obtient ainsi une forme générale de l'expression considérée dans le théorème 6.

Théorème 7. *Etant donnée une série formelle $f(T) \in \mathcal{A}[[T-1]]$, les éléments*

$$a_m = \frac{d^m}{dx^m} f(e^x)\Big|_{x=0} \quad \textit{resp.} \quad \widehat{a}_m = \frac{d^m}{dx^m}\Big(f(e^x) - \frac{1}{p}\sum_{\zeta^p=1} f(\zeta e^x)\Big)\Big|_{x=0}$$

sont dans $\mathcal{A}$ et pour tout entier $c \geqslant 0$ divisible par $(p-1)p^s$ $(s \geqslant 0)$, on a

$$\Delta_c^n a_m \in p^{\min\{m,n(s+1)\}}\mathcal{A} \quad \textit{resp.} \quad \Delta_c^n \widehat{a}_m \in p^{n(s+1)}\mathcal{A}$$

PREUVE. Alors que Young utilise des intégrales et des mesures p-adiques, nous donnons quelques indications pour une preuve directe. Par linéarité, on se ramène à ne traiter que le cas $f(T) = (T-1)^l$ pour un entier $l \geqslant 0$ fixé. On trouve ainsi

$$\Phi(x^m) := a_m = \sum_{k=0}^{m} \binom{l}{k} (-1)^{l-k} k^m \in \mathbb{Z} \subset \mathcal{A}$$

(notons que a_m est nul lorsque $m < l$ puisque $f(e^x) = (e^x - 1)^l$ admet le développement $(x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots)^l$) et par linéarité, on obtient

$$\Delta_c^n a_m = \Phi(x^m(x^c - 1)^n) = \sum_{k=0}^{n} \binom{l}{k} (-1)^{l-k} k^m (k^c - 1)^n.$$

Les éléments $\widehat{\Phi}(x^m) := \widehat{a}_m$ et $\Delta_c^n \widehat{a}_m$ se développent comme ci-dessus, à la différence que les sommes portent sur les indices k qui ne sont pas divisibles par p (on utilise ici le fait que $\sum_{\zeta^p=1} \zeta^k$ vaut p si p divise k, et est nul sinon). On conclut alors comme dans la preuve du théorème 6 en raisonnant sur chaque indice intervenant dans ces sommes. □

Avant d'illustrer ce résultat avec $\mathcal{A} = \mathbb{Z}_p$ (= boule-unité de $\mathbb{Q}_p$), rappelons que le *caractère de Teichmüller* $\omega_p : \mathbb{Z}_p^\times \longrightarrow \mathbb{Q}_p$ associe à chaque unité p-adique $a \in \mathbb{Z}_p^\times$ l'unique racine $(p-1)$-ième de l'unité $\omega_p(a)$ qui lui est congrue modulo $p\mathbb{Z}_p$. On sait que $\omega_p(a) \in \mathbb{Z}_p$ est la limite de la suite $(a^{p^n})_{n \geqslant 0}$.

Remarque : Nous avons déjà rencontré les éléments $\omega_p(1), \ldots, \omega_p(p-1)$ dans la preuve du théorème 4. De même, pour démontrer le théorème 6, nous avons utilisé $a = b^q$ avec $\mathrm{ord}_p(q)$ assez grand (et b générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$). En fait, q peut simplement être une puissance (assez grande) de p et $\omega_p(b)$ apparaît de manière naturelle comme "cas limite".

Exemple 1

Considérons tout d'abord un nombre premier $p \neq 2$ et deux entiers $a, r \geqslant 0$. La fonction $f(T) = T^a\big(2/(T+1)\big)^r$ peut alors s'écrire comme un élément de $\mathbb{Z}_p[[T-1]]$ puisque c'est le cas pour T et $2/(T+1) = \sum_{n \geqslant 0}(-1/2)^n (T-1)^n$. Le théorème est donc valable pour les éléments $a_m = E_m^r(a)$ (pour tout entier $r \geqslant 0$ et tout $a \in \mathbb{Z}_p$ par densité de $\mathbb{N}$ dans $\mathbb{Z}_p$).

Exemple 2

On considère ici un nombre premier p quelconque et un entier $b \geqslant 1$ non divisible par p. On remarque tout d'abord que $\dfrac{T^b - 1}{b(T-1)} \in 1 + (T-1)\mathbb{Z}_p[T-1]$. Son inverse est donc donné par $\dfrac{b(T-1)}{T^b - 1} \in 1 + (T-1)\mathbb{Z}_p[[T-1]]$ et la fonction rationnelle $f(T) = \dfrac{b}{T^b - 1} - \dfrac{1}{T-1}$ est un élément de $\mathbb{Z}_p[[T-1]]$. Avec les notations du théorème, on obtient alors

$$a_m = (b^{m+1} - 1)\frac{B_{m+1}}{m+1} \quad \text{et} \quad \widehat{a}_m = (1 - p^m)(b^{m+1} - 1)\frac{B_{m+1}}{m+1}.$$

Le raisonnement est valable pour tout entier $b \geqslant 1$ non divisible par p et la conclusion du théorème est donc vérifiée (par densité) pour toute unité p-adique $b \in \mathbb{Z}_p^\times$. En prenant $b = \omega(a)$ où a est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$, on trouve

$$\Delta_c^n a_m = (\omega(a)^{m+1} - 1)\Delta_c^n\Big\{\frac{B_{m+1}}{m+1}\Big\} \quad , \quad \Delta_c^n \widehat{a}_m = (\omega(a)^{m+1} - 1)\Delta_c^n\Big\{(1 - p^m)\frac{B_{m+1}}{m+1}\Big\}.$$

Dans le cas où $p-1$ ne divise pas $m+1$, on a $(\omega(a)^{m+1}-1) \in \mathbb{Z}_p^\times$, et donc

$$\Delta_c^n\Big\{\frac{B_{m+1}}{m+1}\Big\} \in p^{\min\{m,n(s+1)\}}\mathbb{Z}_p \quad \text{resp.} \quad \Delta_c^n\Big\{(1-p^m)\frac{B_{m+1}}{m+1}\Big\} \in p^{n(s+1)}\mathbb{Z}_p$$

chaque fois que c est divisible par $(p-1)p^s$. On trouve un cas particulier du théorème 6.

1.5 Polynômes de Bernoulli généralisés

L'ensemble des séries de Hurwitz à coefficients dans $\mathbb{Z}_p$,

$$\mathcal{H}_p := \Big\{f(x) = \sum a_n \frac{x^n}{n!} \ \text{ avec } \ a_n \in \mathbb{Z}_p\Big\},$$

est un anneau commutatif qui contient $\mathbb{Z}_p$ et qui est stable par dérivation. Son introduction dans notre contexte est très naturelle puisque le résultat de Kummer (qui découle directement du théorème 4) implique $\frac{px}{e^x-1} \in \mathcal{H}_p$. On a également $e^{ax} \in \mathcal{H}_p$ pour tout entier p-adique $a \in \mathbb{Z}_p$ et comme $\mathcal{H}_p$ est stable par multiplication, on trouve $p^r\big(\frac{x}{e^x-1}\big)^r e^{ax} \in \mathcal{H}_p$, autrement dit $p^r B_n^r(a) \in \mathbb{Z}_p$ pour tout indice $n \geqslant 0$. Dans [5], Carlitz démontre plus précisément le résultat d'intégralité suivant :

Théorème 8. *Soit $\sigma(r) = \sigma_p(r) \geqslant 1$ le nombre de digits non nuls dans le développement p-adique de $r \geqslant 1$. Alors $p^{\sigma(r)}B_n^r(a)$ est un entier p-adique pour tout $a \in \mathbb{Z}_p$ et $n \geqslant 0$.*

PREUVE. Le théorème 4 affirme que

$$\frac{px}{e^x-1} = \sum_{n\geqslant 0} pB_n\frac{x^n}{n!} \equiv \sum_{n\geqslant 0}\Big(\sum_{k=0}^{p-1} k^n\Big)\frac{x^n}{n!} \bmod p\mathcal{H}_p$$

et comme $\binom{p-1}{k} = \binom{p-1}{p-1-k} \equiv (-1)^{p-1-k} \bmod p\mathbb{Z}$ (pour $k = 0, 1, \ldots, p-1$), on peut écrire

$$\frac{px}{e^x-1} \equiv \sum_{n\geqslant 0}\sum_{k=0}^{p-1}\binom{p-1}{k}(-1)^{p-1-k}\frac{(kx)^n}{n!} = \sum_{k=0}^{p-1}\binom{p-1}{k}(-1)^{p-1-k}e^{kx} \bmod p\mathcal{H}_p,$$

ou encore $\quad \dfrac{x}{e^x-1} = \dfrac{(e^x-1)^{p-1}}{p} + h_0(x)$ avec $h_0(x) \in \mathcal{H}_p$.

D'autre part, pour $r = lp^m$ avec $l \in \{1, 2, \ldots, p-1\}$ et $m \in \mathbb{N}$, l'ordre p-adique de $(r(p-1))!$ est exactement

$$l(p-1)(p^{m-1}+p^{m-2}+\cdots+p+1) + \Big\lfloor\frac{l(p-1)}{p}\Big\rfloor = l(p^m-1) + (l-1) = lp^m - 1 = r-1.$$

Ceci montre (avec l'introduction des nombres de Stirling de deuxième espèce [10]) que

$$p^{\sigma(r)}\Big(\frac{(e^x-1)^{p-1}}{p}\Big)^r = p^{\sigma(r)-r}(r(p-1))!\sum_{k\geqslant 0}\left\{ {k \atop r(p-1)} \right\}\frac{x^k}{k!}$$

appartient à $\mathcal{H}_p$ chaque fois que $\sigma(r)=1$ (comme $\mathcal{H}_p$ est stable par multiplication, ceci est d'ailleurs valable pour tous les entiers $r\geqslant 1$). Par induction sur $m\geqslant 1$, nous pouvons alors écrire

$$\Big(\frac{x}{e^x-1}\Big)^{p^m} = \Big(\frac{(e^x-1)^{p-1}}{p}\Big)^{p^m} + h_m(x)$$

où $h_m(x)=\displaystyle\sum_{k=0}^{p-1}\binom{p}{k}\Big(\frac{(e^x-1)^{p-1}}{p}\Big)^{kp^{m-1}} h_{m-1}(x)^{p-k}$ (pour $m\geqslant 1$) est un élément de $\mathcal{H}_p$. Finalement, pour $l=1,2,\dots,p-1$, on trouve $p\big(\frac{x}{e^x-1}\big)^{lp^m}\in\mathcal{H}_p$ et comme $\mathcal{H}_p$ est stable par multiplication, il suit que $p^{\sigma(r)}\big(\frac{x}{e^x-1}\big)^r e^{ax}\in\mathcal{H}_p$ pour tout entier $r\geqslant 1$ et $a\in\mathbb{Z}_p$. □

Le TAF permet de raffiner le théorème dans certaines circonstances : lorsque n est impair, on a $B_n^{rp}(rp)=-B_n^{rp}(0)$ et

$$|2p^{\sigma(r)-1}B_n^{rp}(0)| = |p^{\sigma(r)-1}|\cdot|B_n^{rp}(0)-B_n^{rp}(rp)| \leqslant |p^{\sigma(r)-1}|\cdot\|nrpB_{n-1}^{rp}(x)\| \leqslant |nr|,$$

autrement dit $2p^{\sigma(r)-1}B_n^{rp}(0)\in nr\mathbb{Z}_p$. En fait, nous n'aurons pas besoin de résultats d'intégralité aussi précis et on pourra se contenter de savoir que $p^rB_n^r(a)$ se trouve dans $\mathbb{Z}_p$ pour tout $a\in\mathbb{Z}_p$ et $n\geqslant 0$.

Le théorème 4 implique que $pB_{np}\equiv pB_n \bmod (np/2)\mathbb{Z}_p$. Le théorème ci-dessus pourrait nous tenter de généraliser ce fait avec la congruence

$$p^{\sigma(r)}B_{np}^r(0)\equiv p^{\sigma(r)}B_n^r(0) \bmod \frac{np}{2}\mathbb{Z}_p$$

mais des essais numériques montrent que ce n'est pas le cas en toute généralité.

Proposition 9. *Pour tout indice $n\geqslant 0$, on a* $p^rB_{np}^r(t)\equiv p^rB_n^r(t^p) \bmod \dfrac{np}{2}\mathbb{Z}_p[t]$.

PREUVE. L'assertion est vérifiée pour $r=0$ et dès qu'elle l'est pour un ordre $r\geqslant 0$, le TAF fournit $p^rB_{np}^r(k)\equiv p^rB_n^r(k^p)\equiv p^rB_n^r(k) \bmod (np/2)\mathbb{Z}_p$ pour tout entier p-adique $k\in\mathbb{Z}_p$. De même, en appliquant le TAF au polynôme $f(t)=p^{r+1}B_{n+1}^{r+1}(t)/(n+1)$, on trouve

$$p^{r+1}B_n^{r+1}(0)\equiv p^r\sum_{k=0}^{p-1}B_n^r(k) \bmod \frac{np}{2}\mathbb{Z}_p.$$

Par induction, ceci nous montre que $p^{r+1}B_{np}^{r+1}(0)\equiv p^{r+1}B_n^{r+1}(0) \bmod (np/2)\mathbb{Z}_p$ (pour tout entier $n\geqslant 0$) et on conclut à l'aide du théorème 1, également valable si on considère les congruences modulo $(np/2)\mathbb{Z}_p$ au lieu de $np\mathbb{Z}_p$. □

Proposition 10. *Pour tous les entiers $m, n \geqslant 0$ et tout $a \in \mathbb{Z}_p$, on a la congruence*

$$p^r B^r_{m+np}(a) \equiv p^r B^r_{m+n}(a) \bmod \frac{np}{2}\mathbb{Z}_p.$$

PREUVE. L'assertion est évidente pour $r = 0$ et par la proposition précédente (et le TAF), elle est également vérifiée pour $m = 0$. La relation

$$p^{r-1}\sum_{k=0}^{p-1} B^{r-1}_{m+n}(a+k) = p^{r-1}\frac{B^r_{m+1+n}(a+p) - B^r_{m+1+n}(a)}{m+1+n}$$

s'écrit de manière plus explicite sous la forme

$$p^{r-1}\sum_{k=0}^{p-1} B^{r-1}_{m+n}(a+k) = p^{r-1}\frac{1}{m+1+n}\sum_{k=1}^{m+1+n}\binom{m+1+n}{k}p^k B^r_{m+1+n-k}(a)$$

$$= p^r B^r_{m+n}(a) + \sum_{k=2}^{m+1+n}(m+n)(m+n-1)\cdots(m+2+n-k)\frac{p^{k-1}}{k!}p^r B^r_{m+1+n-k}(a).$$

Comme $p^{k-1}/k! \in (p/2)\mathbb{Z}_p$ (pour $k \geqslant 2$) et $p^r B^r_{m+1+n-k}(a) \in \mathbb{Z}_p$, on voit ainsi que la somme $p^{r-1}\sum_{k=0}^{p-1} B^{r-1}_{m+n}(a+k)$ est congrue, modulo $(np/2)\mathbb{Z}_p$, à

$$p^r B^r_{m+n}(a) + \sum_{k=2}^{m+1+n} m(m-1)\cdots(m+2-k)\frac{p^{k-1}}{k!}p^r B^r_{m+1+n-k}(a).$$

En d'autres termes, on a (modulo $(np/2)\mathbb{Z}_p$)

$$p^r B^r_{m+n}(a) \equiv p^{r-1}\sum_{k=0}^{p-1} B^{r-1}_{m+n}(a+k) - \frac{1}{m+1}\sum_{k=2}^{m+1}\binom{m+1}{k}p^{k-1}p^r B^r_{m+1+n-k}(a).$$

On peut remplacer n par np en gardant la congruence modulo $(np/2)\mathbb{Z}_p$. Il en résulte que $p^r(B^r_{m+np}(a) - B^r_{m+n}(a))$ est congru (toujours modulo $(np/2)\mathbb{Z}_p$) à

$$\sum_{k=0}^{p-1} p^{r-1}\big[B^{r-1}_{m+np}(a+k) - B^{r-1}_{m+n}(a+k)\big] - \sum_{k=2}^{m+1}\binom{m+1}{k}p^{k-1}p^r\big[B^r_{m+1-k+np}(a) - B^r_{m+1-k+n}(a)\big].$$

On démontre alors la proposition par induction lexicographique sur (r, m). □

1.6 Synthèse

Les congruences établies dans les propositions de ce chapitre généralisent celles que M. Zuber démontre dans [40] en considérant $r = 1$ et $a = 0$. En admettant ses résultats, nous aurions pu les présenter plus directement comme suit.

Théorème 11. *Notons $\partial = \partial_x$ la dérivation formelle par rapport à x. L'ensemble*

$$\mathcal{I}_p := \Big\{ f(x) \in \mathcal{H}_p \ : \ \partial^{np} f(x) \equiv \partial^n f(x) \bmod \frac{np}{2}\mathcal{H}_p \ \text{ pour tout entier } n \geqslant 0 \Big\}$$

est alors un sous-anneau de $\mathcal{H}_p$.

PREUVE. C'est évidemment un sous-groupe additif et pour $f, g \in \mathcal{I}_p$, on a (par l'exemple qui suit l'énoncé du TAF et le fait que $\mathcal{H}_p$ est un $\mathbb{Z}_p$-module stable par dérivation)

$$\begin{aligned}
\partial^{np} f(x)g(x) &= \sum_{k\geqslant 0} \binom{np}{k} \partial^k f(x) \cdot \partial^{np-k} g(x) \\
&\equiv \sum_{k\geqslant 0} \binom{n}{k} \partial^{kp} f(x) \cdot \partial^{(n-k)p} g(x) \\
&\overset{hyp}{\equiv} \sum_{k\geqslant 0} \binom{n}{k} \partial^{k} f(x) \cdot \partial^{n-k} g(x) \\
&= \partial^n f(x)g(x) \qquad \bmod (np/2)\mathcal{H}_p,
\end{aligned}$$

ce qui montre que $\mathcal{I}_p$ est bien stable par multiplication. □

Les éléments de $\mathcal{I}_p$ sont exactement les séries de Hurwitz $f(x) = \sum a_n \frac{x^n}{n!} \in \mathcal{H}_p$ qui vérifient

$$a_{m+np} \equiv a_{m+n} \bmod \frac{np}{2}\mathbb{Z}_p \ \text{ pour tous les entiers } \ m, n \geqslant 0.$$

Les suites $(a_n)_{n\geqslant 0}$ de $\mathbb{Z}_p$ qui ont la propriété ci-dessus forment d'ailleurs un anneau isomorphe à $\mathcal{I}_p$ pour l'addition usuelle et le produit de convolution binomial. En d'autres termes, si l'on considère les ensembles

$$E_m = \big\{ (a_n)_{n\geqslant 0} \in \mathbb{Z}_p^{\mathbb{N}} \ : \ a_{m+np} \equiv a_{m+n} \bmod (np/2)\mathbb{Z}_p \text{ pour tout } n \geqslant 0 \big\},$$

nous venons de montrer que $\bigcap_{m\geqslant 0} E_m$ est un sous-anneau de $\mathbb{Z}_p^{\mathbb{N}}$ (pour l'addition et le produit de convolution binomial). Ce résultat ne semble pas évident à établir sans l'aide des fonctions génératrices exponentielles (via $\mathcal{H}_p$ et $\mathcal{I}_p$), alors qu'il est facile de montrer directement que E_0 est un anneau.

Dans [40] il est montré que $2/(e^x+1) \in \mathcal{I}_p$ pour p impair et que $px/(e^x-1) \in \mathcal{I}_p$. Pour $a \in \mathbb{Z}_p$ fixé, on a également $e^{ax} \in \mathcal{I}_p$ et comme $\mathcal{I}_p$ est stable par multiplication, on a

$$\Big(\frac{2}{e^x+1}\Big)^r e^{ax} \in \mathcal{I}_p \ \text{ (pour } p \text{ impair) } \text{ et } \ p^r \Big(\frac{x}{e^x-1}\Big)^r e^{ax} \in \mathcal{I}_p.$$

On reconnaît les propositions 3 et 10, à partir desquelles on peut déduire les propositions 2 et 9 (grâce au théorème 1).

Partie 2
Nombres et polynômes de Bell

"L'oeuvre d'un mathématicien est surtout un enchevêtrement de conjectures, d'analogies, de souhaits et de frustrations. La démonstration, loin d'être le noyau de la découverte, n'est souvent que le moyen de s'assurer que notre esprit ne nous joue pas des tours."

Gian Carlo Rota

2.1 Définitions

Nous désignerons par $\mathcal{A}$ un anneau unitaire commutatif intègre qui contient $\mathbb{Z}$. Cela peut être aussi bien $\mathbb{Z}$, $\mathbb{Z}_p$ ou $\mathbb{Z}_{(p)} = \mathbb{Q} \cap \mathbb{Z}_p$ (pour un certain nombre premier p) que les anneaux polynomiaux associés $\mathbb{Z}[t]$, $\mathbb{Z}_p[t]$ ou $\mathbb{Z}_{(p)}[t]$. Les polynômes de Pochhammer

$$(x)_0 = 1\ ,\ (x)_n = x(x-1)\cdots(x-(n-1)) \qquad (n \geqslant 1)$$

constituent une base du $\mathcal{A}$-module libre $\mathcal{A}[x]$ et on peut considérer l'application linéaire

$$\Phi : \mathcal{A}[x] \longrightarrow \mathcal{A}[x],\ (x)_n \longmapsto x^n.$$

On définit alors les *polynômes et nombres de Bell* par

$$B_n(x) = \Phi(x^n) \quad \text{resp.} \quad B_n = B_n(1) = \Phi(x^n)\big|_{x=1}.$$

Les nombres de Stirling de deuxième espèce $\left\{ {n \atop k} \right\}$ donnent de manière explicite

$$B_n(x) = \Phi(x^n) = \Phi\Big(\sum_{k=0}^{n} \left\{ {n \atop k} \right\} (x)_k\Big) = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} x^k \quad \text{resp.} \quad B_n = \sum_{k=0}^{n} \left\{ {n \atop k} \right\}$$

donc $B_n(x) \in \mathbb{Z}[x]$ et $B_n \in \mathbb{Z}$. Les premières valeurs sont les suivantes :

n	B_n	polynôme de Bell $B_n(x)$
0	1	1
1	1	x
2	2	$x + x^2$
3	5	$x + 3x^2 + x^3$
4	15	$x + 7x^2 + 6x^3 + x^4$
5	52	$x + 15x^2 + 25x^3 + 10x^4 + x^5$
6	203	$x + 31x^2 + 90x^3 + 65x^4 + 15x^5 + x^6$
7	877	$x + 63x^2 + 301x^3 + 350x^4 + 140x^5 + 21x^6 + x^7$
8	4140	$x + 127x^2 + 966x^3 + 1701x^4 + 1050x^5 + 266x^6 + 28x^7 + x^8$
9	21147	$x + 255x^2 + 3025x^3 + 7770x^4 + 6951x^5 + 2646x^6 + 462x^7 + 36x^8 + x^9$

En analyse combinatoire, on définit B_n comme le nombre de partitions d'un ensemble à n éléments en sous-ensembles non vides. C'est aussi le nombre de relations d'équivalence sur un ensemble à n éléments et plus précisément, $\left\{ {n \atop k} \right\}$ est le nombre de telles relations qui admettent exactement k classes d'équivalence. On peut également voir B_n comme le nombre de vecteurs $(a_1, \ldots, a_n)$ dans $\mathbb{N}^n$ tels que $a_i = i$ ou $a_i = a_j$ pour un certain $j < i$ et $\left\{ {n \atop k} \right\}$ comme le nombre de tels vecteurs admettant exactement k composantes distinctes.

2.2 Premières propriétés

Pour tous les entiers $m, n \geqslant 0$, on a la relation

$$x^n \Phi((x)_m) = x^{m+n} = \Phi((x)_{m+n}) = \Phi((x)_n (x-n)_m),$$

et par linéarité, on obtient

$$x^n \Phi(f(x)) = \Phi((x)_n f(x-n)) \text{ pour tout polynôme } f(x) \in \mathcal{A}[x]. \qquad (*)$$

En particulier, avec $n = 1$, cela donne

$$x\Phi(f(x)) = \Phi(xf(x-1)) \text{ pour tout polynôme } f(x) \in \mathcal{A}[x]$$

et en prenant $f(x) = (x+1)^n$, on trouve la *relation de récurrence*

$$B_{n+1}(x) = x \sum_{k=0}^{n} \binom{n}{k} B_k(x) \quad , \quad B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k.$$

On peut également écrire

$$\Phi((x)_n) = x^n = e^{-x} \sum_{k \geqslant 0} \frac{x^{n+k}}{k!} = e^{-x} \sum_{k \geqslant n} \frac{x^k}{(k-n)!} = e^{-x} \sum_{k \geqslant n} \frac{(k)_n}{k!} x^k = e^{-x} \sum_{k \geqslant 0} \frac{(k)_n}{k!} x^k$$

ce qui montre par linéarité

$$\Phi(f(x)) = e^{-x} \sum_{k \geqslant 0} \frac{f(k)}{k!} x^k \text{ pour tout polynôme } f(x) \in \mathcal{A}[x]. \qquad (**)$$

En considérant en particulier $f(x) = x^n$, on obtient la *formule de Dobinski*

$$B_n(x) = \Phi(x^n) = e^{-x} \sum_{k \geqslant 0} \frac{k^n}{k!} x^k \quad , \quad B_n = \frac{1}{e} \sum_{k \geqslant 0} \frac{k^n}{k!}.$$

Ceci fournit une interprétation probabiliste des polynômes de Bell : étant donné $\lambda > 0$, $B_n(\lambda) = \mathbb{E}(X^n)$ est le moment d'ordre n d'une variable aléatoire $X : \Omega \longrightarrow \mathbb{N}$ de loi $Pr(X = k) = e^{-\lambda}\lambda^k/k!$ (variable aléatoire de Poisson de paramètre λ). De cette formule découle également la *fonction génératrice exponentielle*

$$\sum_{n \geqslant 0} B_n(x) \frac{z^n}{n!} = e^{x(e^z - 1)} \quad , \quad \sum_{n \geqslant 0} B_n \frac{z^n}{n!} = e^{(e^z - 1)}$$

ainsi que l'*identité binomiale* $B_n(x+y) = \sum_{k=0}^{n} \binom{n}{k} B_k(x) B_{n-k}(y)$.

2.3 Rudiments de "calcul ombral"

Etant placé dans le contexte du calcul ombral, il convient de rappeler les premiers concepts de cette théorie [31],[36], tout en les illustrant avec le cas considéré dans ce chapitre. On appelle *base polynomiale* (de $\mathcal{A}[x]$) une suite de polynômes $P_n(x) \in \mathcal{A}[x]$ vérifiant $\deg P_n(x) = n$ (en particulier, $P_0(x) \in \mathcal{A}$ est une constante non nulle) et on dit qu'une telle suite est *associée à un opérateur* $\delta : \mathcal{A}[x] \longrightarrow \mathcal{A}[x]$ si

- $P_0(x) = 1$ et $P_n(0) = 0$ pour tout $n > 0$ [*normalisation*]
- $\delta P_n(x) = nP_{n-1}(x)$ chaque fois que $n > 0$. [*propriété de Scheffer*]

Par exemple, la base canonique $(x^n)_{n\geqslant 0}$ est associée à l'opérateur de dérivation

$$\partial : \mathcal{A}[x] \longrightarrow \mathcal{A}[x],\ f(x) \longmapsto f'(x)$$

et la base de Pochhammer $((x)_n)_{n\geqslant 0}$ est associée à l'opérateur de différence finie

$$\nabla : \mathcal{A}[x] \longrightarrow \mathcal{A}[x],\ f(x) \longmapsto f(x+1) - f(x).$$

L'application Φ, qui relie ces deux bases, relie de manière naturelle les opérateurs associés : on remarque que $\Phi(\nabla^k(x)_n) = \Phi((n)_k(x)_{n-k}) = (n)_k\Phi((x)_{n-k}) = (n)_k x^{n-k}$ correspond à la k-ième dérivée de $\Phi((x)_n)$. Par linéarité, il suit alors $\Phi\nabla^k = \partial^k\Phi$, c'est-à-dire

$$\Phi(\nabla^k f(x)) = \partial^k\Phi(f(x)) \text{ pour tout polynôme } f(x) \in \mathcal{A}[x].$$

Le cas particulier $\partial B_n(x) = \partial\Phi(x^n) = \Phi\nabla x^n = \Phi((x+1)^n - x^n)$ fournit la relation

$$B_n'(x) = \frac{1}{x}B_{n+1}(x) - B_n(x) \ \text{ i.e. } \ B_{n+1}(x) = x(B_n(x) + B_n'(x))$$

(que l'on trouve également en dérivant formellement l'identité de Dobinski). En introduisant l'opérateur de multiplication $\mathcal{X} : \mathcal{A}[x] \longrightarrow \mathcal{A}[x], f(x) \longmapsto xf(x)$, on peut écrire

$$B_n(x) = \mathcal{X}(1+\partial)B_{n-1}(x) = \cdots = (\mathcal{X}(1+\partial))^n(1)$$

(on note indifféremment "1" le polynôme constant et l'opérateur identité). Nous voyons apparaître de manière naturelle l'*algèbre de Weyl* $\mathcal{W} = \mathcal{A}[[\partial, \mathcal{X}]]$ définie formellement par la relation $[\partial, \mathcal{X}] = \partial\mathcal{X} - \mathcal{X}\partial = 1$. Plus généralement, pour une série formelle $F(x) \in \mathcal{A}[[x]]$ dont la dérivée est $F'(x) \in \mathcal{A}[[x]]$, on a

$$[F(\partial), \mathcal{X}] = F'(\partial) \quad \text{ et } \quad [\partial, F(\mathcal{X})] = F'(\mathcal{X}).$$

L'application qui à un opérateur $T : \mathcal{A}[x] \longrightarrow \mathcal{A}[x]$ associe le commutateur $T' = [T, \mathcal{X}] = T\mathcal{X} - \mathcal{X}T$ est appelée *dérivation de Pincherle* et on peut vérifier que $(TS)' = T'S + TS'$.

Remarquons encore que les polynômes de Bell sont associés à l'opérateur $\triangle = \log(1+\partial)$ car $B_0(x) = 1$ et pour tout $n \geqslant 1$, on a $B_n(0) = 0$ ainsi que

$$\triangle B_n(x) = \log(1+\partial)\Phi(x^n) = \Phi \log(1+\nabla)x^n = \Phi(nx^{n-1}) = nB_{n-1}(x),$$

l'avant-dernière égalité provenant de la relation $e^\partial = 1 + \nabla$, qui traduit un développement de Taylor et que l'on peut facilement vérifier avec la base canonique :

$$\exp(\partial)x^n = \sum_{k\geqslant 0} \frac{\partial^k}{k!}x^n = \sum_{k\geqslant 0} \frac{(n)_k}{k!}x^{n-k} = (x+1)^n = (1+\nabla)x^n.$$

Un opérateur linéaire $\delta : \mathcal{A}[x] \longrightarrow \mathcal{A}[x]$ est appelé *delta-opérateur* si $\delta(x) \in \mathcal{A} \setminus \{0\}$ est une constante non nulle et s'il commute avec les opérateurs de translation

$$\tau_a : \mathcal{A}[x] \longrightarrow \mathcal{A}[x], \quad \tau_a f(x) = f(x+a) \quad (a \in \mathcal{A}).$$

Ces conditions impliquent que $\delta(a)$ est nul pour toute constante $a \in \mathcal{A}$ et d'autre part, que $\deg(\delta f(x)) = \deg f(x) - 1$ pour tout polynôme non constant $f(x) \in \mathcal{A}[x]$. A un tel opérateur δ est associée une unique base polynomiale $(P_n(x))_{n\geqslant 0}$. Tout opérateur T qui commute aux translations peut alors s'écrire

$$T = \sum_{n\geqslant 0} a_n \frac{\delta^n}{n!} \quad \text{avec } a_n = [TP_n(x)]_{x=0} \in \mathcal{A}$$

(en particulier $a_0 = 0$ et $a_1 \neq 0$ si T est un delta-opérateur) et tout polynôme $f(x) \in \mathcal{A}[x]$ admet le développement

$$f(x+y) = \sum_{n\geqslant 0} \frac{\delta^n f(y)}{n!} P_n(x).$$

Cela généralise les développements de Taylor et de Mahler, et montre que les polynômes $P_n(x)$ vérifient l'identité binomiale. Réciproquement, toute base polynomiale de type binomial peut être associée à un delta-opérateur.

On peut résumer les différentes bases rencontrées avec les delta-opérateurs associés par le diagramme commutatif suivant :

$$\begin{array}{ccccc}
(x)_n & \xrightarrow{\Phi} & x^n & \xrightarrow{\Phi} & B_n(x) \\
\downarrow{\scriptstyle \nabla} & \circlearrowleft & \downarrow{\scriptstyle \partial} & \circlearrowleft & \downarrow{\scriptstyle \triangle} \\
\underbrace{n(x)_{n-1}}_{Mahler} & \xrightarrow{\Phi} & \underbrace{nx^{n-1}}_{Taylor} & \xrightarrow{\Phi} & nB_{n-1}(x)
\end{array}$$

$$\begin{array}{rcl}
\nabla & = & e^\partial - 1 \\
\partial & = & \log(1+\nabla) \\
\triangle & = & \log(1+\partial) \\
\Phi\nabla^k & = & \partial^k\Phi \\
\Phi\partial^k & = & \triangle^k\Phi
\end{array}$$

On peut de même envisager des "opérateurs d'enchaînement", qui permettent de passer d'un polynôme au suivant à l'intérieur d'une base donnée :

$$\begin{array}{ccc} (x)_{n+1} & \xrightarrow{\Phi} & x^{n+1} \\ \uparrow{\scriptstyle \tau} & \circlearrowleft & \uparrow{\scriptstyle \chi} \\ (x)_n & \xrightarrow{\Phi} & x^n \end{array} \qquad \left| \begin{array}{rcl} \tau & : & f(x) \longmapsto xf(x-1) \\ \chi & : & f(x) \longmapsto xf(x) \\ \Phi\tau^k & = & \chi^k\Phi \end{array} \right.$$

La relation $\chi = \tau e^{\partial} = \tau(1+\nabla)$ montre que $x^n = (\tau e^{\partial})^n(1) = (\tau(1+\nabla))^n(1)$ et en appliquant Φ, on retrouve le fait que $B_n(x) = (\chi e^{\triangle})^n(1) = (\chi(1+\partial))^n(1)$.

On vérifie également que $(\tau\nabla)e^{\tau}(x)_n = (n+\tau)e^{\tau}(x)_n$ pour tout entier $n \geqslant 0$. On en déduit $\chi = e^{-\tau}(\tau\nabla)e^{\tau}$ et donc $x^n = e^{-\tau}(\tau\nabla)^n e^{\tau}(1)$. On retrouve alors l'identité de Dobinski :

$$B_n(x) = e^{-\chi}(\chi\partial)^n e^{\chi}(1) = e^{-x}(\chi\partial)^n e^x = e^{-x}\sum_{k\geqslant 0}\frac{k^n}{k!}x^k.$$

Nous allons définir maintenant des polynômes de Bell à indices négatifs de sorte à respecter le diagramme de la page précédente. On commence par prolonger les polynômes de Pochhammer : comme $(x)_{n+1} = (x-n)(x)_n$ avec $(x)_0 = 1$, il convient de poser

$$(x)_{-1} = \frac{1}{x+1} \quad , \quad (x)_{-2} = \frac{1}{(x+1)(x+2)} \quad , \quad \cdots \quad , \quad (x)_{-n} = \frac{1}{(x+n)_n}$$

et on vérifie que $\nabla(x)_{-n} = -n(x)_{-n-1}$. Pour que le diagramme commute, on doit respecter la relation $x^n\Phi(f(x)) = \Phi((x)_n f(x-n))$. On peut ainsi écrire

$$\Phi((x)_{-n}) = x^{-n}\Phi((x)_n(x-n)_{-n}) = x^{-n}\Phi\Big((x)_n\frac{1}{(x)_n}\Big) = x^{-n}\Phi(1) = x^{-n}$$

ce qui prolonge de manière naturelle $\Phi((x)_n) = x^n$. A l'aide des nombres de Stirling de première espèce [10], on montre (par induction avec la relation $\left[\begin{smallmatrix}k\\n\end{smallmatrix}\right] = \left[\begin{smallmatrix}k+1\\n+1\end{smallmatrix}\right] - k\left[\begin{smallmatrix}k\\n+1\end{smallmatrix}\right]$) que

$$x^{-n} = \sum_{k\geqslant 0}\begin{bmatrix}k\\n\end{bmatrix}\frac{1}{(x+k)_k} = \sum_{k\geqslant 0}\begin{bmatrix}k\\n\end{bmatrix}(x)_{-k}$$

et il ne reste ainsi plus qu'à poser

$$B_{-n}(x) = \Phi(x^{-n}) = \sum_{k\geqslant 0}\begin{bmatrix}k\\n\end{bmatrix}x^{-k} \quad (\text{pour } n \geqslant 0).$$

On peut unifier la définition des polynômes de Bell à indices positifs et négatifs par

$$B_n(x) = \sum_{k\in\mathbb{Z}}\left\{\begin{matrix}n\\k\end{matrix}\right\}x^k \quad \text{avec} \quad \left\{\begin{matrix}-n\\-k\end{matrix}\right\} = \begin{bmatrix}k\\n\end{bmatrix} \quad \text{pour } k,n \in \mathbb{Z}.$$

Les "polynômes de Bell à indices négatifs" sont en fait des séries formelles dans $\mathbb{Z}[[x^{-1}]]$.

2.4 Produits scalaires et polynômes orthogonaux

Dans ce paragraphe, on suppose que $\mathcal{A}$ est un sous-anneau de $\mathbb{R}$. Ainsi, pour $a > 0$ fixé, l'application symétrique bilinéaire

$$(f,g) \longmapsto \Phi_a(f(x)g(x)) := \Phi(f(x)g(x))|_{x=a} = e^{-a} \sum_{k \geqslant 0} \frac{f(k)g(k)}{k!} a^k$$

est un produit scalaire sur $\mathcal{A}[x]$. Nous pouvons nous restreindre à un sous-ensemble

$$V_N = \{\text{polynômes } \in \mathcal{A}[x] \text{ de degré } \leqslant N\} \subset \mathcal{A}[x].$$

Il s'agit d'un $\mathcal{A}$-module libre de rang $N+1 < \infty$ et la matrice de Gram associée au produit scalaire $(\,\cdot\,|\,\cdot\,)_a : V_N \times V_N \longrightarrow \mathbb{R}$ par rapport à la base $\{1, x, \ldots, x^N\}$ est donnée par $(B_{i+j}(a))_{0 \leqslant i,j \leqslant N}$: pour deux polynômes $f(x) = \sum a_k x^k$ et $g(x) = \sum b_k x^k$ dans V_N, nous avons

$$\Phi(f(x)g(x)) = (a_0\ a_1\ \ldots\ a_N) \cdot H_N(x) \cdot (b_0\ b_1\ \ldots\ b_N)^t$$

avec $H_N(x) = (B_{i+j}(x))_{0 \leqslant i,j \leqslant N}$.

Nous nous proposons de trouver la famille de polynômes unitaires $P_n(x) = P_{a,n}(x)$, avec $\deg P_{a,n}(x) = n$, qui sont orthogonaux pour le produit scalaire $(\,\cdot\,|\,\cdot\,)_a$ issu de Φ_a. L'orthogonalité de $P_{a,n}(x)$ face aux polynômes de V_{n-1} se traduit par le fait que $\Phi_a((x)_m P_{a,n}(x))$ est nul pour $m = 0, 1, \ldots, n-1$. Mais nous avons

$$\begin{aligned}\Phi_a((x)_m P_{a,n}(x)) &= a^m \Phi_a(P_{a,n}(x+m)) = a^m \Phi_a\Big(\sum_{k=0}^{m} \binom{m}{k} \nabla^k P_{a,n}(x)\Big) \\ &= a^m \sum_{k=0}^{m} \binom{m}{k} \Phi \nabla^k P_{a,n}(x)\Big|_{x=a} = a^m \sum_{k=0}^{m} \binom{m}{k} \partial^k \Phi(P_{a,n}(x))\Big|_{x=a}\end{aligned}$$

et en considérant successivement les entiers $m = 0, 1, \ldots, n-1$, il suit que $x = a$ annule le polynôme $\Phi(P_{a,n}(x))$ ainsi que ses $n-1$ premières dérivées. Autrement dit $(x-a)^n$ divise $\Phi(P_{a,n}(x))$ mais comme ces polynômes sont unitaires et de même degré, il sont identiques. Au total, on obtient le développement de Mahler

$$P_{a,n}(x) = \Phi^{-1}((x-a)^n) = \sum_{k=0}^{n} \binom{n}{k} (-a)^{n-k} (x)_k.$$

En prenant $m = n$ dans la relation précédente, on trouve de même

$$\|P_{a,n}(x)\|_a^2 = (P_{a,n}(x)|(x)_n)_a = a^n \sum_{k=0}^{n} \binom{n}{k} \partial^k \Phi(P_{a,n}(x))\Big|_{x=a} = a^n \partial^n \Phi(P_{a,n}(x))\Big|_{x=a}.$$

Comme $\Phi(P_{a,n}(x))$ est un polynôme unitaire de degré n, sa n-ième dérivée vaut $n!$ en tout point, et on a donc $\|P_{a,n}(x)\|_a^2 = a^n n!$.

D'autre part, le procédé d'orthogonalisation de Gram-Schmidt permet d'écrire

$$P_{a,N}(x) = \frac{1}{\det H_{N-1}(a)} \begin{vmatrix} B_0(a) & B_1(a) & \cdots & B_N(a) \\ B_1(a) & B_2(a) & \cdots & B_{N+1}(a) \\ \vdots & \vdots & & \vdots \\ B_{N-1}(a) & B_N(a) & \cdots & B_{2N-1}(a) \\ 1 & x & \cdots & x^N \end{vmatrix}$$

On voit que $\|P_{a,N}(x)\|_a^2 = (P_{a,N}(x)|P_{a,N}(x))_a = (P_{a,N}(x)|x^N)_a = \det H_N(a)/\det H_{N-1}(a)$ et il s'ensuit

$$\det H_N(a) = \|P_{a,N}(x)\|_a^2 \cdot \det H_{N-1}(a) = \|P_{a,N}(x)\|_a^2 \cdot \|P_{a,N-1}(x)\|_a^2 \cdots \|P_{a,0}(x)\|_a^2,$$

c'est-à-dire $\det H_N(a) = a^{N(N+1)/2}\, 0!\, 1! \cdots N!$. Ceci étant valable pour tout entier $a > 0$, on en déduit le

Théorème. *La matrice $H_N(x) = (B_{i+j}(x))_{0\leqslant i,j\leqslant N}$ admet le déterminant*

$$\det H_N(x) = \Big(\prod_{k=0}^{N} k!\Big)\, x^{N(N+1)/2}$$

L'encyclopédie [38] attribue ce "curieux" résultat à A. Lenard (1986) au détriment de P. Delsarte [6] qui le démontrait en 1978 (c'était alors une conjecture de C. Radoux).

Terminologie

On dit que $H_N(x)$ est la *matrice de Hankel* d'ordre N construite avec les polynômes de Bell et on remarque que pour $a > 0$, la matrice de Hankel $H_N(a)$ correspond à la matrice de Gram associée au produit scalaire issu de $\Phi_a : x^n \longmapsto B_n(a)$. Les polynômes $P_{a,n}(x)$ sont appelés *polynômes de Poisson-Charlier*. Nous préférons ces polynômes unitaires aux polynômes normalisés $P_{a,n}(x)/\sqrt{n!a^n}$ que certaines personnes prennent pour définition.

Remarque 1 (Preuve de Delsarte)

Dans la base canonique $\{1, x, \ldots, x^n\}$ de V_n, nous pouvons exprimer (avec les nombres de Stirling de première espèce [10])

$$P_{a,n}(x) = \left\langle {n \atop 0} \right\rangle + \left\langle {n \atop 1} \right\rangle x + \cdots + \left\langle {n \atop n} \right\rangle x^n \quad \text{avec} \quad \left\langle {n \atop i} \right\rangle = (-1)^{n-i} \sum_{k=0}^{n} \binom{n}{k} \begin{bmatrix} k \\ i \end{bmatrix} a^{n-k} = \left\langle {n \atop i} \right\rangle_a$$

(en particulier $\left\langle {n \atop n} \right\rangle = 1$ et $\left\langle {n \atop k} \right\rangle = 0$ si $k > n$) et former la matrice triangulaire

$$Q_N(a) = \left(\left\langle {i \atop j} \right\rangle_a\right)_{0\leqslant i,j\leqslant N} = \begin{pmatrix} \left\langle {0 \atop 0} \right\rangle & 0 & \cdots & 0 \\ \left\langle {1 \atop 0} \right\rangle & \left\langle {1 \atop 1} \right\rangle & & \vdots \\ \vdots & & \ddots & 0 \\ \left\langle {N \atop 0} \right\rangle & \left\langle {N \atop 1} \right\rangle & \cdots & \left\langle {N \atop N} \right\rangle \end{pmatrix}$$

de déterminant $\det Q_N(a) = 1$. Les conditions d'orthogonalité de la suite $(P_{a,n}(x))_{n\geqslant 0}$ se traduisent par la relation matricielle $Q_N(a)H_N(a)Q_N(a)^t = \mathrm{Diag}(0!a^0, 1!a^1, \dots, N!a^N)$ et le théorème est immédiat en prenant le déterminant.

Remarque 2

Pour p premier impair, le théorème fournit

$$\begin{aligned} H_{p-1}(1) &= \prod_{k=1}^{p-1} k! = \prod_{k=1}^{p-1} k^{p-k} = \prod_{k=1}^{(p-1)/2} k^{p-k}(p-k)^k \equiv \prod_{k=1}^{(p-1)/2} (-1)^k k^p \\ &= (-1)^{(p^2-1)/8}\Big[\Big(\frac{p-1}{2}\Big)!\Big]^p \equiv (-1)^{(p^2-1)/8}\Big(\frac{p-1}{2}\Big)! \mod p\mathbb{Z}. \end{aligned}$$

En particulier, $H_{p-1}(1)$ est une racine carrée de -1 dans $\mathbb{Z}/p\mathbb{Z}$ lorsque $p \equiv 1 \mod 4$.

Remarque 3

Lorsque $a > 0$, les polynômes de Poisson-Charlier $P_{a,n}(x)$ $(n \geqslant 0)$ forment un système orthogonal (pour le produit scalaire issu de Φ_a) et vérifient de ce fait certaines relations de récurrence (qui restent valables pour tout $a \in \mathbb{R}$) :

1) $P_{a,n+1}(x) = xP_{a,n}(x-1) - aP_{a,n}(x)$,

2) $P_{a,n+1}(x) = (x-n-a)P_{a,n}(x) - naP_{a,n-1}(x)$.

PREUVE. Par calcul direct, on trouve

$$\begin{aligned} P_{a,n}(x) &= \Phi^{-1}((x-a)^n) = \Phi^{-1}(x(x-a)^{n-1}) - a\Phi^{-1}((x-a)^{n-1}) \\ &= xP_{a,n-1}(x-1) - a\Phi^{-1}((x-a)^{n-1}) = xP_{a,n-1}(x-1) - aP_{a,n-1}(x). \end{aligned}$$

Variante : comme la base de Pochhammer est associée à ∇, on voit que

$$P_{a,0}(x) = 1 \quad \text{et} \quad \nabla P_{a,n}(x) = nP_{a,n-1}(x) \quad \text{pour } n \geqslant 1$$

(en particulier $(P_{a,n}(x))_{n\geqslant 0}$ est une *suite de Scheffer* par rapport à l'opérateur ∇). Pour tout entier $m \geqslant 0$, on a donc $mP_{a,m-1}(n) = P_{a,m}(n+1) - P_{a,m}(n)$ et la première relation de récurrence en découle pour $x = m$ si l'on remarque que $P_{a,n}(m) = (-a)^{n-m}P_{a,m}(n)$. Avec ce premier résultat, on calcule directement (pour $n \geqslant 1$)

$$\begin{aligned} (x-n-a)P_{a,n}(x) - naP_{a,n-1}(x) &= (x-a)P_{a,n}(x) - n(P_{a,n}(x) + aP_{a,n-1}(x)) \\ &\overset{1)}{=} (x-a)P_{a,n}(x) - nxP_{a,n-1}(x-1) \\ &= x(P_{a,n}(x) - nP_{a,n-1}(x-1)) - aP_{a,n}(x) \\ &= xP_{a,n}(x-1) - aP_{a,n}(x) \overset{1)}{=} P_{a,n+1}(x) \end{aligned}$$

et la deuxième relation de récurrence est ainsi démontrée. □

Remarque 4

L'orthogonalité des polynômes de Charlier $P_{a,n}(x)$ pour le produit scalaire engendré par Φ_a (lorsque $a > 0$) découle immédiatement de la propriété

$$\Phi(f(x)g(x)) = \sum_{k\geqslant 0} \frac{x^k}{k!}(\partial^k \Phi f(x))(\partial^k \Phi g(x)),$$

valable pour tous les polynômes $f(x), g(x) \in \mathcal{A}[x]$.

PREUVE. Les polynômes de Pochhammer $(x)_n$ étant de type binomial (puisqu'ils sont associés à un delta-opérateur), on a

$$\Phi((x)_m(x)_n) = x^m \Phi((x+m)_n) = x^m \Phi\Big(\sum_{k=0}^{n} \binom{n}{k} (x)_{n-k}(m)_k\Big) = x^m \sum_{k\geqslant 0} \binom{n}{k} x^{n-k}(m)_k,$$

autrement dit $\Phi((x)_m(x)_n) = \displaystyle\sum_{k\geqslant 0} \frac{x^k}{k!}(n)_k x^{n-k}(m)_k x^{m-k} = \sum_{k\geqslant 0} \frac{x^k}{k!}(\partial^k \Phi(x)_m)(\partial^k \Phi(x)_n)$ et on conclut alors par bilinéarité. □

On en déduit immédiatement l'*identité de Radoux* [28] :

$$B_{m+n}(x) = \sum_{k\geqslant 0} \frac{x^k}{k!}(\partial^k B_m(x))(\partial^k B_n(x))$$

et le fait que les *polynômes de Charlier généralisés*

$$P_{z,n}(x) = \Phi^{-1}\big((x-z)^n\big) = \sum_{k=0}^{n} \binom{n}{k} (-z)^{n-k}(x)_k$$

(dans $\mathcal{A}[x]$ avec $\mathcal{A} = \mathbb{Z}[z]$ ou $\mathbb{Z}_p[z]$) vérifient

$$\Phi_z(P_{z,m}(x)P_{z,n}(x)) = \sum_{k\geqslant 0} \frac{x^k}{k!}(\partial^k (x-z)^m)(\partial^k (x-z)^n)\Big|_{x=z} = \begin{cases} n!z^n & \text{si } m = n \\ 0 & \text{sinon} \end{cases}$$

On dit alors que les polynômes unitaires $P_{z,n}(x) \in \mathcal{A}[x]$ constituent un *système orthogonal* pour l'opérateur ombral $\Phi_z : \mathcal{A}[x] \longrightarrow \mathcal{A}, f(x) \longmapsto \Phi(f(x))\big|_{x=z}$ et que ce dernier est un *produit scalaire généralisé*. Une théorie plus générale sera donnée dans la troisième partie de ce travail.

2.5 Opérateurs de convolution T^a

A partir d'un élément $a \in \mathcal{A}$ et d'une suite $P : \mathbb{N} \longrightarrow \mathcal{A}[x]$, on peut construire une nouvelle suite $T^a P : \mathbb{N} \longrightarrow \mathcal{A}[x]$ en posant

$$(T^a P)_n(x) = T^a P_n(x) := \sum_{k=0}^{n} \binom{n}{k} a^{n-k} P_k(x) = \text{“}(P(x)+a)^n\text{”}.$$

Il s'agit de la *convolution exponentielle* des suites $(a^n)_{n\geqslant 0}$ et $(P_n(x))_{n\geqslant 0}$, dont la fonction génératrice exponentielle est donnée par

$$\sum_{k\geqslant 0} T^a P_k(x)\frac{z^k}{k!} = e^{az}\sum_{k\geqslant 0} P_k(x)\frac{z^k}{k!}.$$

On vérifie que $T^0 = 1$ (opérateur “Identité”) et $T^a T^b = T^{a+b}$. Ainsi, si on note $\mathcal{S} = \mathcal{F}(\mathbb{N}, \mathcal{A})$ l'ensemble des suites dans $\mathcal{A}$ et $\mathcal{S}^* = \{\text{applications } \mathcal{A}\text{-linéaires } \mathcal{S} \longrightarrow \mathcal{S}\}$ l'ensemble des endomorphismes de $\mathcal{S}$ (qui est un $\mathcal{A}$-module libre), on a un homomorphisme (de groupes)

$$\begin{array}{rccc} T: & \mathcal{A} & \longrightarrow & \mathcal{S}^* \\ & a & \longmapsto & T^a : \begin{array}{ccc} \mathcal{S} & \longrightarrow & \mathcal{S} \\ P & \longmapsto & T^a P \end{array} \end{array}$$

Il est clair que les opérateurs de convolution préservent les bases polynomiales et on peut établir le diagramme commutatif suivant (entre les différentes bases rencontrées) :

$$\begin{array}{ccccc} (x)_n & \xrightarrow{\Phi} & x^n & \xrightarrow{\Phi} & B_n(x) \\ {\scriptstyle T^a}\uparrow\downarrow{\scriptstyle T^{-a}} & \circlearrowleft & {\scriptstyle T^a}\uparrow\downarrow{\scriptstyle T^{-a}} & \circlearrowleft & {\scriptstyle T^a}\uparrow\downarrow{\scriptstyle T^{-a}} \\ P_{a,n}(x) & \xrightarrow{\Phi} & (x-a)^n & \xrightarrow{\Phi} & B_{a,n}(x) \end{array}$$

(Les polynômes $B_{a,n}(x) = T^{-a}B_n(x)$ sont rattachés aux polynômes de Bell à deux variables introduits par A. Mazouz dans [20] et que l'on reconsidérera ultérieurement). Les bases polynomiales de la première ligne vérifient l'égalité binomiale (car elles sont associées à des delta-opérateurs), alors que les bases de la deuxième vérifient une relation du type

$$P_{a+b,n}(x+y) = \sum_{k=0}^{n} \binom{n}{k} P_{a,k}(x) P_{b,n-k}(y).$$

PREUVE. En effet, si l'on applique T^{-a} à une relation binomiale, on obtient

$$T^{-a}P_n(x+y) = T^{-a}\sum_k \binom{n}{k} P_k(x)P_{n-k}(y) = \sum_k \binom{n}{k} P_{a,k}(x)P_{n-k}(y).$$

Par symétrie, on peut permuter x et y et il ne reste qu'à appliquer T^{-b} pour obtenir le résultat désiré (à permutation de x et y près). On peut également raisonner avec les fonctions génératrices exponentielles. □

Remarque 1

On peut montrer [36] qu'une suite $P_{a,n}(x)$ à deux indices ($a \in \mathcal{A}$ et $n \geqslant 0$) vérifie la relation ci-dessus (on parle alors de "*cross-suite*") si, et seulement si, il existe une suite $(P_n(x))_{n\geqslant 0}$ de type binomial et un groupe à un paramètre d'opérateurs Q^a qui commutent aux translations et tels que $P_{a,n}(x) = Q^a P_n(x)$. Par exemple, on a $T^a x^n = (x+a)^n = \tau_a x^n$ (rappelons que par abus de notation, T^a agit sur une base polynomiale (ici la base canonique) de $\mathcal{A}[x]$ alors que τ_a agit sur un seul polynôme). Les polynômes généralisés d'Euler $E_n^r(x)$ et de Bernoulli $B_n^r(x)$, considérés dans le chapitre précédent, sont également des cross-suites.

Remarque 2

La relation $P_{a,n}(x+y) = \sum_{k=0}^{n} \binom{n}{k} (y)_{n-k} P_{a,k}(x)$ (pour les polynômes de Charlier) fournit

$$\begin{aligned}(P_{a,m}(x+\alpha)|P_{a,n}(x+\beta))_a &= \sum_{k\geqslant 0}\sum_{l\geqslant 0} \binom{m}{k}\binom{n}{l} (\alpha)_{m-k}(\beta)_{n-l}(P_{a,k}(x)|P_{a,l}(x))_a \\ &= \sum_{i\geqslant 0} \binom{m}{i}\binom{n}{i} (\alpha)_{m-i}(\beta)_{n-i} a^i i!\end{aligned}$$

cette dernière somme étant finie puisqu'elle porte sur les indices $i = 0, 1, \ldots, \min(m,n)$.

Remarque 3

Les sommes de factorielles sont en étroite relation avec les polynômes orthogonaux $P_{a,n}(x)$: par le théorème de Pythagore, on peut écrire

$$\kappa_p(a) := \sum_{k=0}^{p-1} k! a^k = \sum_{k=0}^{p-1} \|P_{a,k}(x)\|_a^2 = \Big\| \sum_{k=0}^{p-1} P_{a,k}(x) \Big\|_a^2$$

ce que l'on peut encore expliciter

$$\kappa_p(a) = \Big\| \Phi^{-1} \sum_{k=0}^{p-1} (x-a)^k \Big\|_a^2 = \Big\| \Phi^{-1}\Big(\frac{(x-a)^p - 1}{x-a-1} \Big) \Big\|_a^2 = \Big\| \Phi^{-1} \sum_{k=1}^{p} \binom{p}{k} (x-a-1)^{k-1} \Big\|_a^2.$$

Il s'ensuit la congruence $\kappa_p(a) \equiv \|\Phi^{-1}(x-a-1)^{p-1}\|_a^2 = \|P_{a+1,p-1}(x)\|_a^2 \bmod p\mathbb{Z}$.

2.6 Quelques résultats utiles

Dans le but d'établir des congruences pour les polynômes de Bell, nous démontrons tout d'abord trois résultats très élémentaires mais d'une grande utilité. Le premier généralise un résultat de [8].

Proposition 1. *On considère un nombre premier p, deux entiers $m, n \geqslant 0$ ainsi que deux éléments $\alpha, \beta \in \mathcal{A}$, où $\mathcal{A}$ est un anneau commutatif qui contient $\mathbb{Z}_p$. Si* $\mathrm{ord}_p(m) \geqslant 1$ *et $\alpha \equiv \beta \mod m\mathcal{A}$, alors $\alpha^n \equiv \beta^n \mod mn\mathcal{A}$.*

PREUVE. Par hypothèse, on peut écrire $\alpha = \beta + m\gamma$ avec $\gamma \in \mathcal{A}$ et comme p divise m,

$$\alpha^p = \sum_{k=0}^{p} \binom{p}{k} \beta^{p-k} m^k \gamma^k = \beta^p + mp\tilde{\gamma} \quad \text{avec} \quad \tilde{\gamma} \in \mathcal{A}.$$

On a donc $\alpha^p \equiv \beta^p \mod mp\mathcal{A}$ et par induction

$$\alpha^{p^k} \equiv \beta^{p^k} \mod mp^k\mathcal{A} \quad \text{pour tout entier} \quad k \geqslant 0.$$

En écrivant $n = lp^k$ avec l non divisible par p, on obtient ainsi

$$\alpha^n = (\alpha^{p^k})^l \equiv (\beta^{p^k})^l = \beta^n \mod mp^k\mathcal{A}.$$

Comme l est une unité dans $\mathbb{Z}_p$, c'est également une unité dans $\mathcal{A}$ et $mp^k\mathcal{A} = mn\mathcal{A}$. □

Remarques :

- La proposition reste valable pour un anneau commutatif $\mathcal{A}$ qui contient $\mathbb{Z}$, à condition que l'entier n soit une puissance de p (car les unités de $\mathbb{Z}$ sont $l = \pm 1$).
- On utilisera souvent cette proposition avec $\mathcal{A} = \mathbb{Z}_p[x]$:
  si $\mathrm{ord}_p(m) \geqslant 1$ et $f(x) \equiv g(x) \mod m\mathbb{Z}_p[x]$, alors $f(x)^n \equiv g(x)^n \mod mn\mathbb{Z}_p[x]$.

Le prochain résultat montre comment la propriété $x^m x^n = x^{m+n}$ se traduit dans la base de Pochhammer.

Proposition 2. *Soient p un nombre premier et $m, n \geqslant 0$ deux entiers. Si* $\mathrm{ord}_p(m) \geqslant 1$, *alors*

$$(x)_m (x)_n \equiv (x)_{m+n} \mod \Big(\frac{mn}{p}\Big)\mathbb{Z}_p[x],$$

en particulier

$$(x)_m^n \equiv (x)_{mn} \mod \Big(\frac{m^2}{p}\Big)\mathbb{Z}_p[x].$$

PREUVE. La formule $(*)$ du premier paragraphe affirme que $x^n \Phi f(x) = \Phi((x)_n f(x-n))$ pour tout polynôme $f(x) \in \mathbb{Z}_p[x]$ et en considérant $f(x) = (x+n)_m$, nous obtenons

$x^n\Phi((x+n)_m) = \Phi((x)_m(x)_n)$. Les polynômes de Pochhammer étant de type binomial, nous pouvons ainsi écrire

$$\Phi((x)_m(x)_n) = x^n\Phi((x+n)_m) = x^n\Phi\Big(\sum_{k=0}^{m}\binom{m}{k}(n)_k(x)_{m-k}\Big) = \sum_{k=0}^{m} A_k x^{m+n-k}$$

avec $A_k = \binom{m}{k}(n)_k = \binom{m}{k}\binom{n}{k}k!$. On remarque alors que pour $k \geqslant 1$, le coefficient

$$A_k \;=\; \frac{m}{k}\binom{m-1}{k-1}\frac{n}{k}\binom{n-1}{k-1}k! \;=\; \frac{mn(k-1)!}{k}\binom{m-1}{k-1}\binom{n-1}{k-1}$$

appartient à $(mn/p)\mathbb{Z}_p$ puisque $p(k-1)!/k \in \mathbb{Z}_p$. On obtient donc (avec le terme $k=0$) $\Phi((x)_m(x)_n) \equiv x^{m+n} = \Phi((x)_{m+n})$ mod $(mn/p)\mathbb{Z}_p[x]$. Ceci démontre la première affirmation et la deuxième en découle par induction sur $n \geqslant 1$. □

Le résultat suivant a déjà été utilisé dans [8], il améliore la deuxième assertion de la proposition ci-dessus lorsque $m = p$.

Proposition 3. *Pour tout entier $n \geqslant 0$ et tout nombre premier p, nous avons*

$$(x^p - x)^n \equiv (x)_{np} \bmod \Big(\frac{np}{2}\Big)\mathbb{Z}_p[x].$$

PREUVE. Les polynômes $f(x) = (x)_p$ et $g(x) = x^p - x$ étant unitaires, de même degré et possédant les mêmes racines dans $\mathbb{Z}/p\mathbb{Z}$, on a évidemment $(x)_p \equiv x^p - x$ mod $p\mathbb{Z}[x]$. D'autre part, un développement de Taylor fournit $f(x-kp) \equiv f(x) - kpf'(x)$ mod $p^2\mathbb{Z}[x]$ pour tout entier $k \geqslant 0$, de sorte que

$$(x)_{p^2} = \prod_{k=0}^{p-1}(x-kp)_p \equiv f(x)^p - p\frac{p(p-1)}{2}f'(x)f(x)^{p-1} \bmod p^2\mathbb{Z}[x].$$

Au total, on obtient $(x)_{p^2} \equiv (x)_p^p$ mod $(p^2/2)\mathbb{Z}_p[x]$, c'est-à-dire $(x)_4 \equiv (x)_2^2$ mod $2\mathbb{Z}[x]$ et $(x)_{p^2} \equiv (x)_p^p$ mod $p^2\mathbb{Z}[x]$ pour p premier impair (ceci améliore légèrement la proposition 2 qui fournit cette même congruence modulo $p\mathbb{Z}_p[x]$). On conclut alors inductivement à l'aide des deux propositions précédentes :

$$(x^p - x)^{np^\nu} \equiv (x)_p^{np^\nu} = ((x)_p^p)^{np^{\nu-1}} \equiv (x)_{p^2}^{np^{\nu-1}} \equiv (x)_{p^3}^{np^{\nu-2}} \equiv \cdots \equiv (x)_{p^{\nu+1}}^{n} \equiv (x)_{np^{\nu+1}},$$

chacune de ces congruences étant valable modulo $(np^{\nu+1}/2)\mathbb{Z}_p[x]$. □

En remarquant que $(1-x)(1-2x)\cdots(1-(np-1)x) = x^{np}(1/x)_{np}$, cette proposition peut s'énoncer de manière équivalente

$$(1-x)(1-2x)\cdots(1-(np-1)x) \equiv (1-x^{p-1})^n \bmod \Big(\frac{np}{2}\Big)\mathbb{Z}_p[x].$$

Elle admet en outre la généralisation suivante :

Proposition 4. *On considère un nombre premier p, deux entiers $m, n \geqslant 0$ et un polynôme $f(x) \in \mathbb{Z}_p[x]$. Si $\mathrm{ord}_p(m) \geqslant 1$, alors*

$$\prod_{0 \leqslant k < n} f(x - km) \equiv f(x)^n \bmod \Big(\frac{mn}{2}\Big)\mathbb{Z}_p[x].$$

PREUVE. La congruence est évidente lorsque $\mathrm{ord}_p(n) = 0$ (car elle est vérifiée modulo $m\mathbb{Z}_p[x]$) et dès qu'elle est valable pour un entier $n \geqslant 1$, on a

$$\prod_{k=0}^{np-1} f(x - km) = \prod_{k=0}^{p-1} \prod_{l=0}^{n-1} f(x - (lp + k)m) \equiv \prod_{k=0}^{p-1} f(x - km)^n \bmod \Big(\frac{mp \cdot n}{2}\Big)\mathbb{Z}_p[x].$$

Si $\mathrm{ord}_p(m) \geqslant 1$, un développpement de Taylor permet d'écrire

$$f(x - km) \equiv f(x) - kmf'(x) \bmod mp\mathbb{Z}_p[x],$$

et il suit que $\displaystyle\prod_{k=0}^{p-1} f(x - km) \equiv f(x)^p - f'(x)f(x)^{p-1}m\tfrac{p(p-1)}{2} \equiv f(x)^p \bmod (mp/2)\mathbb{Z}_p[x]$.
Par la première proposition, on a alors

$$\Big(\prod_{k=0}^{p-1} f(x - km)\Big)^n \equiv (f(x)^p)^n = f(x)^{np} \bmod \Big(\frac{mnp}{2}\Big)\mathbb{Z}_p[x],$$

ce qui démontre l'assertion pour l'entier np. □

Corollaire 1. *En considérant $f(x) = (x)_m$ avec $\mathrm{ord}_p(m) \geqslant 1$, on obtient*

$$(x)_{mn} = \prod_{0 \leqslant k < n} (x - km)_m \equiv (x)_m^n \bmod \Big(\frac{mn}{2}\Big)\mathbb{Z}_p[x].$$

Avec $m = p$, on retrouve la proposition 3 (en utilisant la première proposition et le fait que $(x)_p \equiv x^p - x \bmod p\mathbb{Z}_p[x]$).

Corollaire 2. *Soit n un entier divisible par p premier et $E(n) = (\mathbb{Z}/n\mathbb{Z})^\times$ l'ensemble des classes inversibles modulo n. Pour tout polynôme $f(x) \in \mathbb{Z}_p[x]$, on a alors*

$$\prod_{k \in E(n)} f(x - k) \equiv \Big(\prod_{k \in E(p)} f(x - k)\Big)^{\varphi(n)/(p-1)} \bmod \Big(\frac{n}{2}\Big)\mathbb{Z}_p[x]$$

où $\varphi(n) = \#E(n)$ est la fonction d'Euler.

PREUVE. Ecrivons $n = Np^\nu$ avec $\mathrm{ord}_p(N) = 0$ et $\nu \geqslant 1$. Par le théorème chinois, on a

$$\prod_{k\in E(n)} f(x-k) \equiv \prod_{a\in E(N)} \prod_{b\in E(p^\nu)} f(x-ap^\nu-bN) \equiv \prod_{a\in E(N)} \prod_{b\in E(p^\nu)} f(x-bN) \bmod p^\nu\mathbb{Z}_p[x]$$

et comme N est une unité p-adique, il suit que

$$\prod_{k\in E(n)} f(x-k) \equiv \Big(\prod_{k\in E(p^\nu)} f(x-k)\Big)^{\varphi(N)} \bmod p^\nu\mathbb{Z}_p[x].$$

Or la proposition ci-dessus montre que

$$\prod_{k\in E(p^\nu)} f(x-k) \equiv \prod_{0\leqslant l<p} \prod_{m\in E(p^{\nu-1})} f(x-m-lp^{\nu-1}) \equiv \prod_{m\in E(p^{\nu-1})} f(x-m)^p \bmod \Big(\frac{p^\nu}{2}\Big)\mathbb{Z}_p[x]$$

et par induction avec la proposition 1, il s'ensuit

$$\prod_{k\in E(p^\nu)} f(x-k) \equiv \Big(\prod_{m\in E(p^{\nu-1})} f(x-m)\Big)^p \equiv \cdots \equiv \Big(\prod_{m\in E(p)} f(x-m)\Big)^{p^{\nu-1}} \bmod \Big(\frac{p^\nu}{2}\Big)\mathbb{Z}_p[x].$$

On conclut alors avec la proposition 1 et la relation $\varphi(N)p^{\nu-1} = \varphi(n)/(p-1)$. □

Avec $f(x) = x$, on obtient la *congruence de Bauer* (théorème 126 de [13]) :

$$\prod_{k\in E(n)} (x-k) \equiv (x^{p-1}-1)^{\varphi(n)/(p-1)} \bmod \Big(\frac{n}{2}\Big)\mathbb{Z}_p[x]$$

pour tout entier n divisible par p premier.

2.7 Congruences

Nous allons établir une nouvelle congruence pour les polynômes de Bell, généralisant du même coup celles de Touchard, Radoux ([21],[22],[23],[8]), Comtet-Zuber ([8],[9]) et Carlitz pour les nombres de Bell. Les trois premières propositions de §2.6 joueront un rôle capital.

Nous désignons toujours par p un nombre premier quelconque, sans distinguer le cas $p = 2$ du cas p impair. La proposition 3 fournit avec la relation $(*)$ de §2.2

$$\Phi((x^p-x)^n f(x)) \equiv \Phi((x)_{np} f(x)) = x^{np}\Phi(f(x+np)) \equiv x^{np}\Phi(f(x)) \bmod \Big(\frac{np}{2}\Big)\mathbb{Z}_p[x]$$

pour tout entier $n \geqslant 0$. Cette formule peut être généralisée comme suit :

Théorème 5. *Pour tous les entiers $n \geqslant 0$ et $\nu \geqslant 1$, on a*

$$\Phi((x^{p^\nu}-x)^n f(x)) \equiv (x^p + x^{p^2} + \cdots + x^{p^\nu})^n \Phi(f(x)) \bmod \Big(\frac{np}{2}\Big)\mathbb{Z}_p[x].$$

PREUVE. Nous avons de manière évidente

$$(x^p + x^{p^2} + \cdots + x^{p^\nu} + x^{p^{\nu+1}})^n \Phi(f(x)) = \sum_{k=0}^{n} \binom{n}{k} x^{(n-k)p^{\nu+1}} (x^p + x^{p^2} + \cdots + x^{p^\nu})^k \Phi(f(x)).$$

En supposant que le théorème est vérifié pour $\nu \geqslant 1$ et par le fait que

$$\operatorname{ord}_p \tbinom{n}{k} \geqslant \operatorname{ord}_p(n) - \operatorname{ord}_p(k) \ \text{ pour } \ k = 1, \ldots, n,$$

on voit que ceci est congru, modulo $(np/2)\mathbb{Z}_p[x]$, à

$$\begin{aligned} \sum_{k=0}^{n} \binom{n}{k} x^{(n-k)p^{\nu+1}} \Phi((x^{p^\nu} - x)^k f(x)) \ &\equiv \Phi\Big(\sum_{k=0}^{n} \binom{n}{k} (x^p - x)^{(n-k)p^\nu} (x^{p^\nu} - x)^k f(x) \Big) \\ &\equiv \Phi\Big(\big((x^p - x)^{p^\nu} + (x^{p^\nu} - x) \big)^n f(x) \Big). \end{aligned}$$

Comme $(x^p - x)^{p^\nu} + (x^{p^\nu} - x) \equiv x^{p^{\nu+1}} - x \bmod p\mathbb{Z}_p[x]$, on a par la proposition 1

$$\big((x^p - x)^{p^\nu} + (x^{p^\nu} - x) \big)^n \equiv (x^{p^{\nu+1}} - x)^n \bmod np\mathbb{Z}_p[x]$$

et le théorème est ainsi démontré pour $\nu + 1$. □

Pour tout polynôme $f(x) \in \mathbb{Z}_p[x]$, nous avons

$$\Phi(x^{np^\nu} f(x)) = \Phi\big(((x^{p^\nu} - x) + x)^n f(x) \big) = \Phi\Big(\sum_{k=0}^{n} \binom{n}{k} (x^{p^\nu} - x)^k x^{n-k} f(x) \Big).$$

Par le résultat ci-dessus et le fait que $\operatorname{ord}_p \binom{n}{k} \geqslant \operatorname{ord}_p(n) - \operatorname{ord}_p(k)$ (pour $k = 1, \ldots, n$), on obtient, modulo $(np/2)\mathbb{Z}_p[x]$, la congruence

$$\Phi(x^{np^\nu} f(x)) \equiv \sum_{k=0}^{n} \binom{n}{k} (x^p + x^{p^2} + \cdots + x^{p^\nu})^k \Phi(x^{n-k} f(x)).$$

Par exemple, en considérant $f(x) = x^m$, on trouve

Théorème 6. *Pour tous les entiers $n, m \geqslant 0$ et $\nu \geqslant 1$, on a*

$$B_{m+np^\nu}(x) \equiv \sum_{k=0}^{n} \binom{n}{k} (x^p + x^{p^2} + \cdots + x^{p^\nu})^{n-k} B_{m+k}(x) \bmod \Big(\frac{np}{2} \Big) \mathbb{Z}_p[x].$$

Variante de preuve : le théorème découle de l'identité de Radoux (remarque 4 de §2.4)

$$B_{m+n}(x) = \sum_{k \geqslant 0} \frac{x^k}{k!} (\partial^k B_m(x))(\partial^k B_n(x)),$$

du fait que $\partial^k B_m(x) \in k!\mathbb{Z}[x]$ et du résultat suivant :

Théorème 7. *Pour tous les entiers $n, k \geqslant 0$ et $\nu \geqslant 1$, on a*

$$\partial^k B_{np^\nu}(x) \equiv \sum_{l=0}^{n} \binom{n}{l} (x^p + x^{p^2} + \cdots + x^{p^\nu})^l \partial^k B_{n-l}(x) \mod \Big(\frac{np}{2}\Big)\mathbb{Z}_p[x].$$

PREUVE. Par la relation $\partial^k \Phi = \Phi \nabla^k$ et le théorème 5, la somme de droite est

$$\sum_{l=0}^{n} \binom{n}{l} (x^p + x^{p^2} + \cdots + x^{p^\nu})^l \Phi(\nabla^k x^{n-l}) \equiv \Phi\Big(\sum_{l=0}^{n} \binom{n}{l} (x^{p^\nu} - x)^l \nabla^k x^{n-l}\Big) \mod \Big(\frac{np}{2}\Big)\mathbb{Z}_p[x].$$

Grâce à la proposition 1, nous pouvons remarquer que

$$\begin{aligned} \nabla((x^{p^\nu} - x)^l f(x)) &= ((x+1)^{p^\nu} - (x+1))^l f(x+1) - (x^{p^\nu} - x)^l f(x) \\ &\equiv (x^{p^\nu} - x)^l f(x+1) - (x^{p^\nu} - x)^l f(x) \\ &= (x^{p^\nu} - x)^l \nabla f(x) \mod lp\mathbb{Z}_p[x] \end{aligned}$$

et par itération, on trouve $\nabla^k((x^{p^\nu} - x)^l f(x)) \equiv (x^{p^\nu} - x)^l \nabla^k f(x) \mod lp\mathbb{Z}_p[x]$. Avec cette constatation, nous obtenons

$$\sum_{l=0}^{n} \binom{n}{l} (x^p + x^{p^2} + \cdots + x^{p^\nu})^l \Phi(\nabla^k x^{n-l}) \equiv \Phi\nabla^k\Big(\sum_{l=0}^{n} \binom{n}{l} (x^{p^\nu} - x)^l x^{n-l}\Big) = \Phi\nabla^k x^{np^\nu}$$

modulo $(np/2)\mathbb{Z}_p[x]$, et l'assertion est ainsi démontrée. □

En introduisant une nouvelle variable z, le théorème 6 peut être écrit plus simplement

$$\Phi_z(x^{np^\nu} f(x)) \equiv \Phi_z((x + z^p + z^{p^2} + \cdots + z^{p^\nu})^n f(x)) \mod \Big(\frac{np}{2}\Big)\mathbb{Z}_p[z]$$

pour tout polynôme $f(x) \in \mathbb{Z}_p[x]$. Voici un énoncé équivalent :

Corollaire 1. *Pour tous les entiers $n, m \geqslant 0$ et $\nu \geqslant 1$, on a*

$$B_{m+n}(x) \equiv \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} (x^p + x^{p^2} + \cdots + x^{p^\nu})^{n-k} B_{m+kp^\nu}(x) \mod \Big(\frac{np}{2}\Big)\mathbb{Z}_p[x]$$

PREUVE. Soit $\mathcal{A}$ un anneau commutatif qui contient $\mathbb{Z}$. La formule d'*inversion binomiale* affirme que pour un élément α et deux suites $(a_n)_{n\geqslant 0}$, $(b_n)_{n\geqslant 0}$ dans $\mathcal{A}$, on a l'équivalence

$$a_n = \sum_{k=0}^{n} \binom{n}{k} \alpha^{n-k} b_k \iff b_n = \sum_{k=0}^{n} \binom{n}{k} (-\alpha)^{n-k} a_k.$$

Avec les opérateurs de convolution, elle se reformule "$a_n = T^\alpha b_n \iff b_n = T^{-\alpha} a_n$" et découle de la propriété $T^\alpha T^\beta = T^{\alpha+\beta}$. On peut remarquer que cette équivalence est encore valable si l'on remplace l'égalité par des congruences modulo $(np/2)\mathcal{A}$. En effet, si on suppose que $a_k \equiv T^\alpha b_k \mod (kp/2)\mathcal{A}$ pour tout $k \geqslant 0$, alors, modulo $(np/2)\mathcal{A}$, on obtient

$$(T^{-\alpha}a)_n = \sum_{k=0}^{n} \binom{n}{k} (-\alpha)^{n-k} a_k \equiv \sum_{k=0}^{n} \binom{n}{k} (-\alpha)^{n-k} (T^\alpha b)_k = (T^{-\alpha}T^\alpha b)_n = b_n.$$

Le corollaire est alors obtenu en considérant l'élément $\alpha = (x^p + x^{p^2} + \cdots + x^{p^\nu})$ et les suites $a_n(x) = B_{m+np^\nu}(x)$, $b_n(x) = B_{m+n}(x)$ dans $\mathcal{A} = \mathbb{Z}_p[x]$ (m et ν sont fixés). □

On sait que les nombres de Bell vérifient une certaine périodicité dans tout corps fini (Carlitz, [3]). Le théorème 6 permet de généraliser ce fait.

Corollaire 2. *Soient $m, n \geqslant 0$, $a \in \mathbb{Z}$ et $\omega_p = 1 + p + p^2 + \cdots + p^{p-1}$. Alors*

$$B_{m+n\omega_p}(a) \equiv \begin{cases} a^n B_m(a) \mod (np/2)\mathbb{Z}_p & \text{si } \operatorname{ord}_p(a) = 0 \\ B_{m+n}(a) \mod (np/2)\mathbb{Z}_p & \text{si } p \text{ divise } a \end{cases}$$

PREUVE. Un entier $a \in \mathbb{Z}$ étant fixé, le théorème se formule (avec la proposition 1)

$$\Phi_a(x^{np^\nu} f(x)) \equiv \Phi_a((x + \nu a)^n f(x)) \mod \Big(\frac{np}{2}\Big)\mathbb{Z}_p,$$

ce qui nous permet d'écrire $B_{m+n\omega_p}(a)$ sous la forme

$$\Phi_a(x^n x^{np} x^{np^2} \cdots x^{np^{p-1}} x^m) \equiv \Phi_a\big([x(x+a)(x+2a)\cdots(x+(p-1)a)]^n x^m\big) \mod \Big(\frac{np}{2}\Big)\mathbb{Z}_p.$$

– Si p ne divise pas a, alors $x(x+a)\cdots(x+(p-1)a) \equiv x^p - x \mod p\mathbb{Z}[x]$ car les deux polynômes sont unitaires, de même degré et ont les mêmes racines dans $\mathbb{Z}/p\mathbb{Z}$. Par la proposition 1, on obtient $(x(x+a)\cdots(x+(p-1)a))^n \equiv (x^p - x)^n \mod np\mathbb{Z}_p[x]$ et donc

$$\Phi_a(x^{m+n\omega_p}) \equiv \Phi_a((x^p - x)^n x^m) \equiv a^{np}\Phi_a(x^m) = a^{np} B_m(a) \mod \Big(\frac{np}{2}\Big)\mathbb{Z}_p.$$

On conclut alors par le petit théorème de Fermat (et la proposition 1).

– Si p divise a, alors $(x(x+a)(x+2a)\cdots(x+(p-1)a))^n \equiv x^{np} \mod np\mathbb{Z}_p[x]$, et donc

$$\Phi_a(x^{m+n\omega_p}) \equiv \Phi_a(x^{np}x^m) = B_{m+np}(a) \equiv \sum_{k=0}^{n} \binom{n}{k} a^{kp} B_{m+n-k}(a) \mod \Big(\frac{np}{2}\Big)\mathbb{Z}_p.$$

Pour $k > 0$, on a $a^{kp} \equiv 0 \mod kp\mathbb{Z}_p$ (proposition 1) donc $\binom{n}{k} a^{kp} \equiv 0 \mod np\mathbb{Z}_p$, ce qui nous permet de conclure également dans ce cas. □

Ainsi, si a n'est pas divisible par p, la suite $(B_m(a))_{m\geqslant 0}$ est périodique (modulo p) et la période divise $n\omega_p$ où n est l'ordre (multiplicatif) de a dans $\mathbb{Z}/p\mathbb{Z}$.

Congruences pour les polynômes de Bell

Soit p un nombre premier impair et $\omega_p = 1 + p + p^2 + \cdots + p^{p-1}$. Alors

1) $$B_{m+np^\nu}(x) \equiv \sum_{k=0}^{n} \binom{n}{k} (x^p + x^{p^2} + \cdots + x^{p^\nu})^{n-k} B_{m+k}(x) \bmod np\mathbb{Z}_p[x]$$

2) $$B_{m+np}(x) \equiv \sum_{k=0}^{n} \binom{n}{k} x^{(n-k)p} B_{m+k}(x) \bmod np\mathbb{Z}_p[x]$$

3) $$B_{m+n\omega_p}(a) \equiv \begin{cases} a^n B_m(a) \bmod np\mathbb{Z}_p & \text{si } \operatorname{ord}_p(a) = 0 \\ B_{m+n}(a) \bmod np\mathbb{Z}_p & \text{si } p \text{ divise } a \end{cases}$$

4) $$B_{np}(x) \equiv \sum_{k=0}^{n} \binom{n}{k} x^{(n-k)p} B_k(x) \bmod np\mathbb{Z}_p[x]$$

5) $$B_{m+p^\nu}(x) \equiv (x^p + x^{p^2} + \cdots + x^{p^\nu}) B_m(x) + B_{m+1}(x) \bmod p\mathbb{Z}[x]$$

6) $$B_{m+p}(x) \equiv x^p B_m(x) + B_{m+1}(x) \bmod p\mathbb{Z}[x]$$

Congruences pour les nombres de Bell

1′) $$B_{m+np^\nu} \equiv \sum_{k=0}^{n} \binom{n}{k} \nu^{n-k} B_{m+k} \bmod np\mathbb{Z}_p$$

2′) $$B_{m+np} \equiv \sum_{k=0}^{n} \binom{n}{k} B_{m+k} \bmod np\mathbb{Z}_p$$

3′) *Carlitz* : $B_{m+n\omega_p} \equiv B_m \bmod np\mathbb{Z}_p$

4′) *Comtet − Zuber* : $B_{np} \equiv B_{n+1} \bmod np\mathbb{Z}_p$

5′) *Radoux* : $B_{m+p^\nu} \equiv B_{m+1} + \nu B_m \bmod p\mathbb{Z}$

6′) *Touchard* : $B_{m+p} \equiv B_m + B_{m+1} \bmod p\mathbb{Z}$

2.8 Le cas $p = 2$

Le théorème 6 est valable modulo $n\mathbb{Z}_2[x]$ lorsque $p = 2$. On perd donc un facteur 2 par rapport aux congruences obtenues modulo $np\mathbb{Z}_p[x]$ lorsque p est un premier impair. Notre objectif est de récupérer ce facteur et établir des congruences modulo $2n\mathbb{Z}_2[x]$. Afin de simplifier les énoncés, nous introduisons tout d'abord une nouvelle notation : Pour deux entiers $k > 0$ et $n \in \mathbb{Z}$, on pose

$$\xi_k(n) = \begin{cases} n & \text{si } n \text{ est divisible par } k, \\ 0 & \text{sinon.} \end{cases}$$

On a évidemment $\xi_k(-n) = -\xi_k(n)$ et la moyenne

$$d(n) = \frac{1}{n}\sum_{k=1}^{n} \xi_k(n) = \frac{1}{n}\big(\xi_1(n) + \xi_2(n) + \cdots + \xi_n(n)\big)$$

fournit le nombre de diviseurs (positifs) de n. Lorsque $p = 2$, la proposition 3 (qui tient une place importante dans la preuve du théorème 6) se formule de la manière suivante :

Proposition 8. *Pour tout entier $n \geqslant 0$, on a*

$$(x^2 - x)^n \equiv (x)_{2n} + \xi_2(n)(x)_{2n-2} + \xi_4(n)(x)_{2n-4} \bmod 2n\mathbb{Z}_2[x].$$

PREUVE. On a $x^2 - x = (x)_2$ et on vérifie que $(x^2 - x)^2 \equiv (x)_4 + 2(x)_2 \bmod 4\mathbb{Z}[x]$. Par les propositions 1 et 2, on trouve alors

$$(x^2 - x)^4 \equiv ((x)_4 + 2(x)_2)^2 = (x)_4^2 + 4(x)_4(x)_2 + 4(x)_2^2 \equiv (x)_8 + 4(x)_6 + 4(x)_4 \bmod 8\mathbb{Z}[x].$$

On continue de démontrer la proposition pour les puissances de 2 en procédant par induction sur $\nu = \mathrm{ord}_2(n) \geqslant 2$. A nouveau par la proposition 1, on a par hypothèse

$$(x^2 - x)^{2^{\nu+1}} \equiv \Big((x)_{2^{\nu+1}} + 2^{\nu}\big((x)_{2^{\nu+1}-2} + (x)_{2^{\nu+1}-4}\big)\Big)^2 \bmod 2^{\nu+2}\mathbb{Z}[x]$$

et comme $2^{2\nu}$ est divisible par $2^{\nu+2}$ (puisque $\nu \geqslant 2$), on peut écrire

$$(x^2 - x)^{2^{\nu+1}} \equiv (x)_{2^{\nu+1}}^2 + 2^{\nu+1}(x)_{2^{\nu+1}}\big((x)_{2^{\nu+1}-2} + (x)_{2^{\nu+1}-4}\big) \bmod 2^{\nu+2}\mathbb{Z}[x].$$

La proposition 2 fournit alors

$$(x^2 - x)^{2^{\nu+1}} \equiv (x)_{2^{\nu+2}} + 2^{\nu+1}\big((x)_{2^{\nu+2}-2} + (x)_{2^{\nu+2}-4}\big) \bmod 2^{\nu+2}\mathbb{Z}[x]$$

et l'assertion est a fortiori vérifiée pour toute puissance de 2. Pour conclure dans le cas général, on considère un nombre n impair et la proposition 1 qui donne

$$(x^2 - x)^{2^\nu n} \equiv \big((x)_{2^{\nu+1}} + \xi_2(2^\nu)(x)_{2^{\nu+1}-2} + \xi_4(2^\nu)(x)_{2^{\nu+1}-4}\big)^n \bmod 2^{\nu+1}\mathbb{Z}_2[x].$$

Comme les produits $\xi_2(2^\nu)\xi_2(2^\nu)$, $\xi_2(2^\nu)\xi_4(2^\nu)$ et $\xi_4(2^\nu)\xi_4(2^\nu)$ sont tous divisibles par $2^{\nu+1}$ (quel que soit $\nu \geqslant 0$), il suit

$$(x^2-x)^{2^\nu n} \equiv (x)_{2^{\nu+1}}^n + n(x)_{2^{\nu+1}}^{n-1}\big(\xi_2(2^\nu)(x)_{2^{\nu+1}-2} + \xi_4(2^\nu)(x)_{2^{\nu+1}-4}\big) \bmod 2^{\nu+1}\mathbb{Z}_2[x].$$

Finalement, la proposition 2 (avec les relations $n\xi_2(2^\nu) = \xi_2(2^\nu n)$ et $n\xi_4(2^\nu) = \xi_4(2^\nu n)$ pour n impair) montre que

$$(x^2-x)^{2^\nu n} \equiv (x)_{2^{\nu+1}n} + \xi_2(2^\nu n)(x)_{2^{\nu+1}n-2} + \xi_4(2^\nu n)(x)_{2^{\nu+1}n-4} \bmod 2^{\nu+1}\mathbb{Z}_2[x]$$

et la proposition est complètement démontrée. □

A l'aide de la relation $(*)$ de §2.2, il suit immédiatement que

$$\Phi((x^2-x)^n f(x)) \equiv (x^{2n} + \xi_2(n)x^{2n-2} + \xi_4(n)x^{2n-4})\Phi(f(x)) \bmod 2n\mathbb{Z}_2[x]$$

pour tout polynôme $f(x) \in \mathbb{Z}[x]$ et tout entier $n \geqslant 0$. En appliquant cette congruence à

$$\Phi(x^{m+2n}) = \Phi((x^2-x+x)^n x^m) = \Phi\sum_{k=0}^{n}\binom{n}{k}(x^2-x)^k x^{m+n-k},$$

on obtient finalement le

Théorème 9. *Pour tous les entiers $m, n \geqslant 0$, les polynômes de Bell vérifient*

$$B_{m+2n}(x) \equiv \sum_{k=0}^{n}\binom{n}{k}(x^{2k} + \xi_2(k)x^{2k-2} + \xi_4(k)x^{2k-4})B_{m+n-k}(x) \bmod 2n\mathbb{Z}_2[x].$$

Nous pouvons simplifier l'expression de droite en étudiant modulo $2n\mathbb{Z}_2[x]$ la somme

$$S_{m,n}(x) := \sum_{k=0}^{n}\binom{n}{k}(\xi_2(k)x^{2k-2} + \xi_4(k)x^{2k-4})B_{m+n-k}(x).$$

Il s'agit du "terme correctif" qui doit intervenir dans la congruence 2) de §2.7 lorsque $p = 2$. Comme il est nul pour $n = 0$ et $n = 1$, on considérera pour la suite $n \geqslant 2$. Les termes non nuls de cette somme sont obtenus sur l'ensemble d'indices $E = \{k \text{ pair} > 0\}$:

$$S_{m,n}(x) = \sum_{k\in E}\frac{n(n-1)}{k(k-1)}\binom{n-2}{k-2}(\xi_2(k)x^{2k-2} + \xi_4(k)x^{2k-4})B_{m+n-k}(x).$$

Si k est pair, alors $k-1$ est une unité dans $\mathbb{Z}_2$, $1/(k-1) \equiv 1 \bmod 2\mathbb{Z}_2$, et donc

$$S_{m,n}(x) \equiv n(n-1)\sum_{k\in E}\binom{n-2}{k-2}\Big(x^{2k-2} + \frac{\xi_4(k)}{k}x^{2k-4}\Big)B_{m+n-k}(x) \bmod 2n\mathbb{Z}_2[x].$$

On voit déjà que $S_{m,n}(x) \equiv 0 \mod 2n\mathbb{Z}_2[x]$ lorsque n est impair et les congruences 2)4)6)2') 4') et 6') de §2.7 restent valables pour $p = 2$ dans ce cas.

Lorsque n est pair, on a $n(n-1) \equiv n \mod 2n$ (car $n - 1 \equiv 1 \mod 2$) et on peut écrire

$$S_{m,n}(x) \equiv n \sum_{l \geqslant 1} \binom{n-2}{2l-2} \Big(x^{4l-2} + \frac{\xi_2(l)}{l} x^{4l-4} \Big) B_{m+n-2l}(x) \mod 2n\mathbb{Z}_2[x]$$

ou encore, par le théorème de Lucas,

$$S_{m,n}(x) \equiv n \sum_{l \geqslant 1} \binom{(n-2)/2}{l-1} \Big(x^{4l-2} + \frac{\xi_2(l)}{l} x^{4l-4} \Big) B_{m+n-2l}(x) \mod 2n\mathbb{Z}_2[x].$$

Il ne semble pas évident de trouver un énoncé plus facile mais en considérant $x = 1$, les calculs deviennent beaucoup plus simples.

Théorème 10. *Modulo $2n\mathbb{Z}_2$, les nombres de Bell vérifient (pour tout entier $m \geqslant 0$)*

$$B_{m+2n} - \sum_{k=0}^{n} \binom{n}{k} B_{m+k} \equiv S_{m,n}(1) \equiv \begin{cases} n & \text{si } n \text{ est pair et } m \not\equiv 2 + [n/4] \mod 3 \\ 0 & \text{sinon} \end{cases}$$

PREUVE. Par ce qui précède, on peut supposer que n est pair et le théorème revient à dire que la somme

$$\widetilde{S}_{m,n} = \sum_{l \geqslant 1} \binom{(n-2)/2}{l-1} \Big(1 + \frac{\xi_2(l)}{l} \Big) B_{m+n-2l}$$

est paire uniquement si $m \equiv 2 + [n/4] \mod 3$. Dans cette somme, les indices l pairs fournissent des termes pairs, de même que si $m + n - 2l \equiv 2 \mod 3$ car la formule de Touchard (valable pour $p = 2$) montre que $B_s \in 2\mathbb{Z}$ uniquement si $s \equiv 2 \mod 3$. L'ensemble des indices "intéressants" est donc $F = \{l \text{ impair } \not\equiv 2m + 2n - 1 \mod 3\}$ et le théorème de Lucas donne

$$\widetilde{S}_{m,n} \equiv \sum_{l \in F} \binom{(n-2)/2}{l-1} \equiv \sum_{l \in F} \binom{[(n-2)/4]}{(l-1)/2} = \sum_{k \in G} \binom{[(n-2)/4]}{k} \mod 2$$

avec $G = \{k \ : \ k \not\equiv m + n - 1 \mod 3\}$. Le lemme suivant montre que la dernière somme est paire uniquement si

$$m \equiv 2\Big[\frac{n-2}{4}\Big] - n + 1 \equiv 2\Big(\Big[\frac{n-2}{4}\Big] + n + 2\Big) = 2\Big[\frac{5n+6}{4}\Big] \mod 3,$$

c'est-à dire ssi $m \equiv 2 + [n/4] \mod 3$ comme on le voit en testant les classes $n \equiv 0, 2, 4, 6, 8, 10$ modulo 12 (il est clair que la classe de $2\big[\frac{5n+6}{4}\big]$ modulo 3 ne dépend que de la classe de n modulo 12, et on a supposé que n est pair). □

Le résultat utilisé dans la preuve du théorème est :

Lemme. *La somme* $\sigma(i,n) := \sum_{k\not\equiv i \bmod 3} \binom{n}{k}$ *est paire uniquement si* $i \equiv 2n \bmod 3$.

PREUVE. Soit ξ une racine primitive 3-ième de l'unité. Alors $\mathbb{F}_2[\xi] = \{0, 1, \xi, \xi^2 = \xi + 1\}$ est une extension galoisienne (de degré 2) de $\mathbb{F}_2$. Le groupe de Galois est engendré par l'automorphisme de Frobenius $\alpha \longmapsto \alpha^2$ et la trace est donnée par

$$\mathrm{Tr} : \mathbb{F}_2[\xi] \longrightarrow \mathbb{F}_2, \alpha \longmapsto \alpha + \alpha^2.$$

Comme $\xi^3 = 1$, la trace de ξ^k ne dépend que de la classe de k modulo 3, mais on a $\mathrm{Tr}\,\xi^0 = \mathrm{Tr}(1) = 0$, $\mathrm{Tr}\,\xi = \xi + \xi^2 = 1$ et $\mathrm{Tr}\,\xi^2 = \xi^2 + \xi^4 = \xi^2 + \xi = 1$, ce qui se résume par

$$\mathrm{Tr}\,\xi^k = \begin{cases} 0 & \text{si } k \text{ est divisible par 3,} \\ 1 & \text{sinon.} \end{cases}$$

Ainsi dans $\mathbb{F}_2$, on voit que

$$\sum_{k\not\equiv i \bmod 3} \binom{n}{k} = \sum_k \binom{n}{k} \mathrm{Tr}\,\xi^{k-i} = \mathrm{Tr}\left(\sum_k \binom{n}{k} \xi^{k-i}\right) = \mathrm{Tr}(\xi^{-i}(1+\xi)^n) = \mathrm{Tr}\,\xi^{2n-i}$$

est nul uniquement lorsque $2n - i \equiv 0 \bmod 3$. □

Nous avons adapté et généralisé un raisonnement de O. Hadas qui établit dans [12] l'équivalent de la congruence de Comtet-Zuber dans le cas $p = 2$. Il travaille avec l'algèbre de Weyl dont nous avons parlé dans §2.3, mais pour notre part, il suffit de considérer $m = 0$ dans le théorème ...

Corollaire (Congruence à la Comtet-Zuber pour $p = 2$) Modulo $2n\mathbb{Z}_2$, on a

$$B_{2n} \equiv \begin{cases} B_{n+1} + n & \text{si } n \equiv 0, 2, 8 \text{ ou } 10 \bmod 12 \\ B_{n+1} & \text{sinon} \end{cases}$$

2.9 Polynômes de Bell généralisés

Les polynômes de Bell à deux variables définis par A. Mazouz [20] sont

$$B_n(x,y) = \sum_{k=0}^{n} \binom{n}{k} y^{n-k} B_k(x) = T^y B_n(x).$$

On remarque que $B_n(1,x)$ est le n-ième polynôme de Bell-Carlitz (noté $B_n^c(x)$ dans [9]), que $B_n(x,0)$ est le n-ième polynôme de Bell $B_n(x)$ et que les nombres de Bell peuvent s'écrire $B_n = B_n(1,0)$, $B_{n+1} = B_n(1,1)$. Nous pouvons établir quelques congruences intéressantes :

Proposition 11. *Pour tous les paramètres $m, n, \mu \geqslant 0$, $\nu \geqslant 1$ et $a \in \mathbb{Z}$, les polynômes de Bell-Mazouz vérifient*

$$1) \quad B_{np^\nu}(x,y) \equiv B_n(x, x^p + x^{p^2} + \cdots + x^{p^\nu} + y^{p^\nu}) \bmod \Big(\frac{np}{2}\Big)\mathbb{Z}_p[x,y]$$

$$2) \quad B_{m+np^\nu}(a,\mu a) \equiv \sum_{k=0}^{n} \binom{n}{k} (\nu a)^{n-k} B_{m+k}(a,\mu a) \bmod \Big(\frac{np}{2}\Big)\mathbb{Z}_p.$$

PREUVE. On remarque tout d'abord que $B_n(x,y) = \Phi((x+y)^n)$ (l'application linéaire Φ agissant sur la variable x). D'autre part, il est clair que $(x+y)^p \equiv (x^p + y^p) \bmod p\mathbb{Z}_p[x,y]$ et la proposition 1 montre que

$$(x+y)^{np^\nu} \equiv (x^p + y^p)^{np^{\nu-1}} \equiv (x^{p^2} + y^{p^2})^{np^{\nu-2}} \equiv \cdots \equiv (x^{p^\nu} + y^{p^\nu})^n \bmod np\mathbb{Z}_p[x,y].$$

On peut ainsi écrire $B_{np^\nu}(x,y) = \Phi((x+y)^{np^\nu}) \equiv \Phi((x^{p^\nu} + y^{p^\nu})^n) \bmod np\mathbb{Z}_p[x,y]$ et par le théorème 6, il en résulte modulo $(np/2)\mathbb{Z}_p[x,y]$

$$B_{np^\nu}(x,y) \equiv \Phi\Big(\sum_{k=0}^{n} \binom{n}{k} y^{(n-k)p^\nu} x^{kp^\nu}\Big) \equiv \Phi\Big(\sum_{k=0}^{n} \binom{n}{k} y^{(n-k)p^\nu} (x + z^p + \cdots + z^{p^\nu})^k\Big)\Big|_{z=x},$$

c'est-à-dire $B_{np^\nu}(x,y) \equiv \Phi\big((x + z^p + \cdots + z^{p^\nu} + y^{p^\nu})^n\big)\Big|_{z=x} = B_n(x, x^p + \cdots + x^{p^\nu} + y^{p^\nu})$.

La deuxième assertion s'obtient également avec le théorème 6 :

$$B_{m+np^\nu}(a,\mu a) = \Phi_a((x+\mu a)^{m+np^\nu}) \equiv \Phi_a(x^{np^{\nu+\mu}}(x+\mu a)^m) \equiv \Phi_a((x+\nu a+\mu a)^n (x+\mu a)^m)$$

chacune de ces congruences étant valable modulo $(np/2)\mathbb{Z}_p$. $\square$

Remarques : La première assertion fournit $B^c_{np^\nu}(x) \equiv B^c_n(\nu + x^{p^\nu}) \bmod (np/2)\mathbb{Z}_p[x]$ et avec $\nu = 1$, on retrouve une congruence de type Comtet-Zuber établie dans [9]. Quant à la deuxième, elle généralise la congruence 1') pour les nombres de Bell (prendre $a = 1$ et $\mu = 0$), et donne en particulier $B_{np^\nu}(a,\mu a) \equiv B_n(a,(\nu+\mu)a) \bmod (np/2)\mathbb{Z}_p$.

2.10 Nombres de Stirling

Les polynômes de Bell à indices positifs sont des fonctions génératrices ordinaires de nombres de Stirling de deuxième espèce, alors que ceux à indices négatifs sont des fonctions génératrices paraordinaires de nombres de Stirling de première espèce (voir §2.3). Les congruences qui mettent en jeu les polynômes de Bell permettent donc d'obtenir des congruences entre les nombres de Stirling des deux espèces.

Par exemple, pour $m \geqslant 0$ et p premier impair, la congruence 5) s'écrit

$$\sum_{i=0}^{m+p^\nu} \left\{ {m+p^\nu \atop i} \right\} x^i \equiv \sum_{i=0}^{m} \left\{ {m \atop i} \right\} (x^{i+p} + x^{i+p^2} + \cdots + x^{i+p^\nu}) + \sum_{i=0}^{m+1} \left\{ {m+1 \atop i} \right\} x^i \mod p\mathbb{Z}_p[x]$$

et si l'on compare les coefficients devant x^k, on trouve

$$\left\{ {m+p^\nu \atop k} \right\} \equiv \left\{ {m \atop k-p} \right\} + \left\{ {m \atop k-p^2} \right\} + \cdots + \left\{ {m \atop k-p^\nu} \right\} + \left\{ {m+1 \atop k} \right\} \mod p\mathbb{Z}$$

en rappelant que $\left\{ {i \atop j} \right\}$ est nul si $j < 0 \leqslant i$ ou si $j > i$. En utilisant la relation $\left\{ {i \atop j} \right\} = \left[{-j \atop -i} \right]$, on obtient pour $0 \leqslant m \leqslant p^\nu$:

$$\left\{ {p^\nu - m \atop k} \right\} \equiv \left[{p-k \atop m} \right] + \left[{p^2-k \atop m} \right] + \cdots + \left[{p^\nu - k \atop m} \right] + \left[{-k \atop m-1} \right] \mod p\mathbb{Z}$$

(on retrouve évidemment ce résultat si l'on écrit la congruence 5) en développant des polynômes de Bell à indices négatifs ...) et comme $\left[{i \atop j} \right]$ est nul si $j < 0 \leqslant i$ ou $j > i$, on a

$$\left\{ {p^\nu - m \atop p^\nu - k} \right\} \equiv \left[{k \atop m} \right] \mod p\mathbb{Z} \text{ pour tout } k, m = 0, 1, \ldots, p^\nu.$$

Dans une certaine mesure, on peut améliorer ce résultat à l'aide de la congruence 2). Pour $m \geqslant 0$, elle s'écrit

$$\sum_{i=0}^{m+np} \left\{ {m+np \atop i} \right\} x^i \equiv \sum_{j=0}^{n} \binom{n}{j} \sum_{i=0}^{m+j} \left\{ {m+j \atop i} \right\} x^{i+(n-j)p} \mod np\mathbb{Z}_p[x]$$

et en comparant les coefficients devant x^k, on trouve

$$\left\{ {m+np \atop k} \right\} \equiv \sum_{j=0}^{n} \binom{n}{j} \left\{ {m+j \atop k-(n-j)p} \right\} = \sum_{j=0}^{n} \binom{n}{j} \left\{ {m+n-j \atop k-jp} \right\} \mod np\mathbb{Z}.$$

Avec $n = p^\nu$, on obtient en particulier

$$\left\{ {p^{\nu+1} - m \atop p^{\nu+1} - k} \right\} \equiv \sum_{j=0}^{p^\nu} \binom{p^\nu}{j} \left\{ {p^\nu - m - j \atop p^{\nu+1} - k - jp} \right\} \mod p^{\nu+1}\mathbb{Z}.$$

Si $0 \leqslant k - m < p - 1$, on a $p^{\nu+1} - k - jp > p^\nu - m - j$ pour tout $j = 0, 1, \ldots, p^\nu - 1$ (car $p^\nu - p^{\nu+1} + k - m = p^\nu(1-p) + k - m < (1-p)(p^\nu - 1) \leqslant (1-p)j = j - jp$) et donc

$$\left\{ {p^{\nu+1} - m \atop p^{\nu+1} - k} \right\} \equiv \left\{ {-m \atop -k} \right\} = \left[{k \atop m} \right] \mod p^{\nu+1}\mathbb{Z} \quad (\nu \geqslant 0).$$

On retrouve ainsi un résultat de [8].

2.11 Congruences de Radoux

Dans [22], C. Radoux établit qu'une période de la suite $(B_n)_{n\geqslant 0}$ (mod p) comporte

- une séquence (maximale) de $p-1$ zéros consécutifs,
- une séquence de p nombres identiques consécutifs non nuls.

Dans [24] et [25], il localise exactement les deux séquences et N. Kahale les retrouvera quinze ans plus tard dans [18]. Le calcul ombral permet de généraliser facilement ces résultats. Dans ce paragraphe, nous considérons un nombre premier $p \neq 2$.

Proposition 12. *Pour* $\tau_p = (p^p - \omega_p)/(p-1) = 1 + 2p + 3p^2 + \cdots + (p-1)p^{p-2}$, *on a*

$$B_{\tau_p+1} \equiv B_{\tau_p+2} \equiv \cdots \equiv B_{\tau_p+p-1} \equiv 0 \mod p\mathbb{Z}$$

alors que $B_{\tau_p} \equiv (-1)^{(p^2+4p-5)/8}\Big(\frac{p-1}{2}\Big)! \mod p\mathbb{Z}$.

PREUVE. L'opérateur $\varphi = \Phi_1$ permet d'écrire $B_{\tau_p} = \varphi(x^{\tau_p}) = \varphi(f(x))$ avec

$$f(x) = x(x+1)^2(x+2)^3\cdots(x+p-2)^{p-1}.$$

Pour tout entier $n \geqslant 0$, on a $(x)_p \equiv (x+n)_p \mod p\mathbb{Z}[x]$ et donc (toujours modulo $p\mathbb{Z}[x]$)

$$\begin{aligned}(x)_p f(x+n+1) &\equiv (x+n+p-1)_p f(x+n+1) = (x+n+p-1)^p f(x+n)\\ &\equiv (x^p+n-1)f(x+n) \equiv [(x)_p + x + (n-1)]f(x+n).\end{aligned}$$

En appliquant $\varphi = \Phi_1$, il vient alors (grâce à $(*)$ de §2.2)

$$\varphi(f(x+n+1)) \equiv \varphi(f(x+n)) + \varphi(f(x+n+1)) + (n-1)\varphi(f(x+n)) \mod p\mathbb{Z}$$

ou encore $n\varphi(f(x+n)) \equiv 0 \mod p\mathbb{Z}$. En particulier, on a $\varphi(f(x+n)) \equiv 0 \mod p\mathbb{Z}$ chaque fois que l'entier n est inversible modulo p. On en tire que

$$B_{\tau_p+n} = \varphi\Big(\sum_{k=0}^{n} \left\{ {n \atop k} \right\} (x)_k f(x)\Big) = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} \varphi((x)_k f(x)) = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} \varphi(f(x+k))$$

est nul (modulo p) lorsque $n = 1, 2, \ldots, p-1$. La congruence de Touchard permet d'étendre ce résultat pour $n = p+1, p+2, \ldots, 2(p-1)$ et montre que

$$B_{\tau_p+p} \equiv B_{\tau_p} + B_{\tau_p+1} \equiv B_{\tau_p} \mod p\mathbb{Z}.$$

On voit ainsi que les matrices (de taille $p \times p$)

$$\begin{pmatrix} B_{\tau_p} & B_{\tau_p+1} & \cdots & B_{\tau_p+p-1} \\ B_{\tau_p+1} & B_{\tau_p+2} & \cdots & B_{\tau_p+p} \\ \vdots & \vdots & & \vdots \\ B_{\tau_p+p-1} & B_{\tau_p+p} & \cdots & B_{\tau_p+2(p-1)} \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} B_{\tau_p} & 0 & \cdots & \cdots & 0 \\ 0 & 0 & \cdots & 0 & B_{\tau_p} \\ \vdots & \vdots & \ddots & \ddots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ 0 & B_{\tau_p} & 0 & \cdots & 0 \end{pmatrix}$$

sont congrues modulo $p\mathbb{M}_p(\mathbb{Z})$ (c'est-à-dire que les coefficients correspondants sont congrus modulo $p\mathbb{Z}$). Le déterminant de la première matrice est, modulo $p\mathbb{Z}$, celui de la matrice de Hankel $H_{p-1}(1)$ (on applique la congruence de Touchard à la dernière colonne, on ramène cette colonne en première position, sans changer le signe puisque p est impair, et on continue inductivement), alors que le déterminant de la deuxième matrice vaut exactement $(-1)^{(p-1)/2}B_{\tau_p}$. Au total, on a donc

$$B_{\tau_p} \equiv (-1)^{(p-1)/2} \det H_{p-1}(1) \equiv (-1)^{(p^2+4p-5)/8} \Big(\frac{p-1}{2}\Big)! \mod p\mathbb{Z}$$

et la proposition est ainsi démontrée. □

De nouvelles séquences intéressantes peuvent être obtenues en permutant de manière cyclique les digits dans l'expression p-adique de τ_p : formellement, on considère l'application

$$\sigma : a_0 + a_1 p + a_2 p^2 + \cdots + a_{p-1}p^{p-1} \longmapsto a_1 + a_2 p + a_3 p^2 + \cdots + a_{p-1}p^{p-2} + a_0 p^{p-1}.$$

Il s'agit d'une permutation sur l'ensemble $\{0, 1, \ldots, p^p - 1\}$, qui admet pour points fixes les multiples de $\omega_p = 1 + p + p^2 + \cdots + p^{p-1}$ (modulo $p^p - 1$).

Théorème 13. *Considérons un entier $m \in \{0, 1, \ldots, p-1\}$ et posons $\tau_p(m) = \sigma^m \tau_p$. Alors pour $n = 0, 1, \ldots, p-1+m$, on a la congruence*

$$B_{\tau_p(m)+n} \equiv \left\{ {n \atop m} \right\} B_{\tau_p} \mod p\mathbb{Z}.$$

PREUVE. Le nombre $\tau_p(m)$ a été "construit" de manière à respecter la congruence

$$B_{\tau_p(m)+n} = \varphi(x^{n+\tau_p(m)}) \equiv \varphi(x^n f(x-m)) \mod p\mathbb{Z}$$

avec $f(x) = x(x+1)^2(x+2)^3 \cdots (x+p-2)^{p-1}$ comme dans la preuve précédente. En développant x^n dans la base de Pochhammer, il vient

$$B_{\tau_p(m)+n} \equiv \sum_{k=0}^{n} \left\{ {n \atop k} \right\} \varphi\big((x)_k f(x-m)\big) = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} \varphi(f(x+k-m)).$$

Or nous avons montré que $\varphi(f(x+k-m)) \equiv 0 \mod p\mathbb{Z}$ chaque fois que $k-m$ n'est pas divisible par p. Par choix de m et n, il n'y a qu'un seul terme $\varphi(f(x+k-m))$ intéressant (i.e. a priori non nul modulo p) dans la somme ci-dessus : il est donné pour $k = m$. □

Avec $m = 1$, on obtient une séquence explicite de p nombres identiques dans la suite des nombres de Bell modulo p : comme $\left\{ {0 \atop 1} \right\} = 0$ et $\left\{ {n \atop 1} \right\} = 1$ pour $n \geqslant 1$, on trouve

$$B_{\tau_p(1)} \equiv 0 \quad \text{et} \quad B_{\tau_p(1)+1} \equiv B_{\tau_p(1)+2} \equiv \cdots \equiv B_{\tau_p(1)+p} \equiv B_{\tau_p} \mod p\mathbb{Z}.$$

En prenant $m = 2$, on trouve de même

$$B_{\tau_p(2)} \equiv 0 \quad \text{et } B_{\tau_p(2)+n} \equiv (2^{n-1} - 1)B_{\tau_p} \mod p\mathbb{Z} \quad \text{pour } n = 1, \ldots, p+1.$$

Pour $n = m+1$ avec $m \in \{0, 1, \ldots, p-1\}$, on a $B_{\tau_p(m)+m+1} \equiv \frac{m(m+1)}{2} B_{\tau_p} \mod p\mathbb{Z}$.

2.12 Fonction génératrice ordinaire

Pour préparer le prochain paragraphe, nous établissons une congruence pour la fonction génératrice ordinaire des polynômes de Bell [3] et montrons que cette dernière est "compatible" avec le prolongement des polynômes de Bell aux indices négatifs établi dans §2.3. Par définition, cette fonction génératrice est donnée par

$$F(x,z) := \sum_{n\geqslant 0} B_n(x)z^n = 1 + \Phi\Big(xz\sum_{n\geqslant 0}(xz)^n\Big)$$

en rappelant que Φ agit sur x mais pas sur z. Avec la propriété $(*)$ de §2.2, il vient alors

$$F(x,z) = 1 + xz\ \Phi\Big(\sum_{n\geqslant 0}\big((x+1)z\big)^n\Big) = 1 + xz\ \Phi\Big(\frac{1}{1-z-xz}\Big)$$

(après avoir reconnu une série géométrique) et donc

$$F(x,z) = 1 + \frac{xz}{1-z}\ \Phi\Big(\frac{1}{1-xz/(1-z)}\Big) = 1 + \frac{xz}{1-z}\ \Phi\Big(\sum_{n\geqslant 0}\Big(\frac{xz}{1-z}\Big)^n\Big).$$

Ceci peut se résumer par la relation

$$F(x,z) = 1 + x\cdot h(z)F(x,h(z))$$

où $h(z) = \dfrac{z}{1-z}$ est l'homographie de matrice $\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$. Les composées de $h(z)$ sont $h^k(z) = \dfrac{z}{1-kz}$ et pour tout entier $m \geqslant 1$, on établit par induction

$$F(x,z) = \sum_{k=0}^{m-1} x^k h(z)h^2(z)\cdots h^k(z) + x^m h(z)h^2(z)\cdots h^m(z)F(x,h^m(z)).$$

Comme $h^m(z) \equiv z \bmod m\mathbb{Z}_p[[z]]$, on obtient modulo $m\mathbb{Z}_p[x][[z]]$ (après avoir réarrangé les termes dans la somme)

$$F(x,z) \equiv \sum_{k=0}^{m-1} x^{m-1-k}h(z)h^2(z)\cdots h^{m-1-k}(z) + x^m h(z)h^2(z)\cdots h^{m-1}(z)zF(x,z)$$

et donc $(1-z)(1-2z)\cdots(1-(m-1)z)F(x,z)$ est congru (modulo $m\mathbb{Z}_p[x][[z]]$) à

$$\sum_{k=0}^{m-1}\big[(xz)^{m-1-k}(1+kz)(1+(k-1)z)\cdots(1+z)\big] + (xz)^m F(x,z).$$

Le cas où $m = np$ avec p premier est particulièrement intéressant car la proposition 3 (ou plutôt l'énoncé équivalent qui en suit la preuve) affirme que

$$(1-z)(1-2z)\cdots(1-(np-1)z) \equiv (1-z^{p-1})^n \bmod \Big(\frac{np}{2}\Big)\mathbb{Z}_p[z].$$

Tout ceci conduit finalement au

Théorème 14. *Modulo $(np/2)\mathbb{Z}_p[x][[z]]$, la fonction génératrice $F(x,z)$ vérifie*

$$\big((1-z^{p-1})^n-(xz)^{np}\big)F(x,z)\equiv\sum_{k=0}^{np-1}(xz)^{np-1-k}(1+z)(1+2z)\cdots(1+kz).$$

Le terme de droite est un polynôme de degré $np-1$ en z. Ainsi, en comparant les coefficients de z^{m+np} (avec $m\geqslant 0$), on voit que

$$\sum_{k=0}^{n}\binom{n}{k}(-1)^k B_{m+np-k(p-1)}(x)-x^{np}B_m(x)\equiv 0 \bmod \Big(\frac{np}{2}\Big)\mathbb{Z}_p[x]. \qquad (*)$$

D'autre part, les nombres de Stirling de première espèce permettent d'expliciter

$$(1+z)(1+2z)\cdots(1+kz)=\sum_{l=0}^{k+1}\begin{bmatrix}k+1\\ l\end{bmatrix}z^{k+1-l}$$

et en comparant les coefficients de z^{np-m} (avec $m\geqslant 0$), on trouve

$$\sum_{k=0}^{n}\binom{n}{k}(-1)^k B_{np-m-k(p-1)}(x)\equiv\sum_{k=0}^{np}\begin{bmatrix}k\\ m\end{bmatrix}x^{np-k} \bmod \Big(\frac{np}{2}\Big)\mathbb{Z}_p[x]$$

(en rappelant que $\left[\begin{smallmatrix}k\\ m\end{smallmatrix}\right]$ est nul si $0\leqslant k<m$). Dans cette dernière relation, on peut exiger que $0\leqslant m\leqslant n$ pour s'assurer que les indices $np-m-k(p-1)$ qui interviennent pour $k=0,\dots,n$ soient tous positifs. On montre alors que $\left[\begin{smallmatrix}np+l\\ m\end{smallmatrix}\right]\in(np/2)\mathbb{Z}_p$ pour tout $l\geqslant 1$ (et $m=0,1,\dots,n$) simplement en comparant les coefficients dans la congruence

$$(x^p-x)^n(x)_l\equiv(x)_{np}(x-np)_l=(x)_{np+l}=\sum_{m=0}^{np+l}\begin{bmatrix}np+l\\ m\end{bmatrix}(-1)^{np+l-m}x^m$$

modulo $(np/2)\mathbb{Z}_p[x]$. Il en résulte que la suite $\big(\left[\begin{smallmatrix}k\\ m\end{smallmatrix}\right]\big)_{k\geqslant 0}$ converge p-adiquement vers 0 lorsque $k\longrightarrow\infty$ et que (pour $0\leqslant m\leqslant n$)

$$\sum_{k=0}^{np}\begin{bmatrix}k\\ m\end{bmatrix}x^{np-k}\equiv x^{np}\sum_{k\geqslant 0}\begin{bmatrix}k\\ m\end{bmatrix}x^{-k}=x^{np}B_{-m}(x) \bmod \Big(\frac{np}{2}\Big)\mathbb{Z}_p[[x^{-1}]].$$

La congruence $(*)$ ci-dessus est donc valable modulo $(np/2)\mathbb{Z}_p[[x,x^{-1}]]$ lorsque $m\geqslant -n$, ce qui n'est pas étonnant puisqu'elle traduit le fait que

$$x^{np}\Phi(x^m)=\Phi((x)_{np}(x-np)^m)\equiv\Phi((x^p-x)^n x^m) \bmod \Big(\frac{np}{2}\Big)\mathbb{Z}_p[[x,x^{-1}]]$$

grâce à la relation $(*)$ de §2.2 et la proposition 3. Elle fournit la limite (à considérer au sens p-adique)

$$B_m(x) = \lim_{n\longrightarrow 0} x^{-np} \sum_{k=0}^{n} \binom{n}{k} (-1)^k B_{m+np-k(p-1)}(x)$$

et les polynômes de Bell ont été prolongés à des indices négatifs de sorte à respecter cette relation. On peut ainsi considérer des entiers $m < 0$ dans les congruences établies (en remplaçant $\mathbb{Z}_p[x]$ par $\mathbb{Z}_p[[x, x^{-1}]]$). Par exemple, la congruence de Carlitz montre que $B_m = \lim_{n\longrightarrow 0} B_{n\omega_p+m}$ pour tout $m \in \mathbb{Z}$.

2.13 Sur les traces de Barsky-Benzaghou

Dans ce paragraphe, nous généralisons la "formule de trace" de D. Barsky et B. Benzaghou [4], valable pour un nombre premier p impair. Nous venons de montrer (théorème 14) que la fonction génératrice ordinaire $F(x, z)$ vérifie (pour p premier impair)

$$\big((1-z^{p-1})^n - (xz)^{np}\big)F(x,z) \equiv \sum_{k=0}^{np-1} (xz)^{np-1-k}(1+z)(1+2z)\cdots(1+kz) \bmod np\mathbb{Z}_p[x][[z]].$$

En particulier, pour une unité p-adique $a \in \mathbb{Z}$, on obtient

$$F(a,z) \equiv \frac{1}{g_{a,n}(z)} \sum_{k=0}^{np-1} z^{np-1}\Big(\frac{1}{z}+1\Big)\Big(\frac{1}{z}+2\Big)\cdots\Big(\frac{1}{z}+k\Big)a^{np-1-k} \bmod np\mathbb{Z}_p[[z]]$$

avec $g_{a,n}(z) = (1-z^{p-1})^n - a^n z^{np}$. Cette congruence se traduit par une égalité dans l'anneau

$$\mathbb{Z}_p[[z]]/np\mathbb{Z}_p[[z]] \cong \mathcal{A}_{np}[[z]] \text{ avec } \mathcal{A}_{np} = \mathbb{Z}_p/np\mathbb{Z}_p \cong \mathbb{Z}/p^{\nu+1}\mathbb{Z} \text{ si } \operatorname{ord}_p(n) = \nu.$$

Le polynôme $g_{a,n}(z)$ admet np racines distinctes dans une extension $\mathcal{A}_{np}^*$ assez grande de $\mathcal{A}_{np}$, au même titre que son polynôme réciproque $\widetilde{g}_{a,n}(z) = z^{np}g_{a,n}(1/z) = (z^p - z)^n - a^n$. Plus précisément, si ϑ est une racine fixée de $\widetilde{g}_{1,1}(z) = z^p - z - 1$, alors modulo $np\mathbb{Z}_p[\vartheta]$ les racines de $\widetilde{g}_{a,n}(z)$ sont $a\vartheta$, $a\vartheta+1$, …, $a\vartheta+(np-1)$: la proposition 1 montre en effet que

$$\widetilde{g}_{a,n}(a\vartheta+k) = \big[(a\vartheta+k)^p - (a\vartheta+k)\big]^n - a^n \equiv \big[(a\vartheta^p+k) - (a\vartheta+k)\big]^n - a^n = 0.$$

L'anneau $\mathcal{A}_{np}^* = \mathcal{A}_{np}[\vartheta]$ contient toutes les racines de $\widetilde{g}_{a,n}(z)$ et on vérifie qu'il contient également toutes celles de $g_{a,n}(z)$ puisque a est une unité dans $\mathbb{Z}_p$. Nous avons ainsi dans $\mathcal{A}_{np}^*[[z]]$ la décomposition

$$F(a,z) = \sum_{g_{a,n}(\theta)=0} \frac{\mu_{a,n}(\theta)}{z-\theta} \quad \text{avec } \mu_{a,n}(\theta) = \lim_{z\longrightarrow\theta}(z-\theta)F(a,z).$$

On peut expliciter dans $\mathcal{A}^*_{np}$ les coefficients

$$\mu_{a,n}(\theta) = \frac{1}{g'_{a,n}(\theta)} \sum_{k=0}^{np-1} \theta^{np-1}\Big(\frac{1}{\theta}+1\Big)\Big(\frac{1}{\theta}+2\Big)\cdots\Big(\frac{1}{\theta}+k\Big)a^{np-1-k}$$

mais comme $(a\theta)^{np} = (1-\theta^{p-1})^n$ et $g'_{a,n}(\theta) = n(1-\theta^{p-1})^{n-1}\theta^{p-2}$ pour toute racine de $g_{a,n}(z)$, il suit

$$\mu_{a,n}(\theta) = \frac{1-\theta^{p-1}}{n\theta^{p-2}} \sum_{k=0}^{np-1} \frac{1}{\theta}\Big(\frac{1}{\theta}+1\Big)\Big(\frac{1}{\theta}+2\Big)\cdots\Big(\frac{1}{\theta}+k\Big)a^{-1-k}.$$

Ceci nous permet d'exprimer (toujours dans $\mathcal{A}^*_{np}$)

$$B_m(a) = \lim_{z\longrightarrow 0} \frac{F^{(m)}(a,z)}{m!} = -\sum_{g_{a,n}(\theta)=0} \frac{\mu_{a,n}(\theta)}{\theta^{m+1}} = -\sum_{\widetilde{g}_{a,n}(\theta)=0} \theta^{m+1}\mu_{a,n}(1/\theta)$$

sous la forme

$$B_m(a) = -\sum_{\widetilde{g}_{a,n}(\theta)=0} \theta^m \frac{\theta^{p-1}-1}{n} \sum_{k=0}^{np-1} \theta(\theta+1)(\theta+2)\cdots(\theta+k)a^{-1-k}.$$

En remarquant que, dans $\mathcal{A}^*_{np}$, toute racine de $\widetilde{g}_{a,n}(z)$ peut s'écrire $a\theta$ où θ est une racine de $\widetilde{g}_{1,n}(z) = (z^p-z)^n - 1$, on arrive finalement au

Théorème 15. *Pour toute unité p-adique $a \in \mathbb{Z}$, on a dans $\mathbb{Z}_p[\vartheta]/np\mathbb{Z}_p[\vartheta]$*

$$B_m(a) = -\sum (a\theta)^m \frac{(a\theta)^{p-1}-1}{n} \sum_{k=0}^{np-1} \theta(\theta+a^{-1})(\theta+2a^{-1})\cdots(\theta+ka^{-1}),$$

la première somme portant sur les racines θ du polynôme $\widetilde{g}_n(z) = \widetilde{g}_{1,n}(z) = (z^p-z)^n - 1$.

Remarque

Dans $\mathcal{A}^*_{np}$, toute racine de $\widetilde{g}_n(z) = (z^p-z)^n - 1$ vérifie $\theta^{np^\nu} = (\theta+\nu)^n$ pour tout entier $\nu \geqslant 1$. En effet, dans $\mathcal{A}^*_{np}$, ces racines sont exactement ϑ, $\vartheta+1$, ... ,$\vartheta+np-1$ où ϑ est une racine fixée de $\widetilde{g}_1(z) = z^p - z - 1$. La proposition 1 montre alors que

$$(\vartheta+l)^{np^\nu} \equiv (\vartheta^p+l)^{np^{\nu-1}} = (\vartheta+(l+1))^{np^{\nu-1}} \bmod np\mathbb{Z}_p[\vartheta]$$

et par itération, on obtient $(\vartheta+l)^{np^\nu} \equiv (\vartheta+(l+\nu))^n \bmod np\mathbb{Z}_p[\vartheta]$. $\square$

Conséquences

1) Pour toute racine de $\widetilde{g}_n(z)$ et tout entier $\nu \geqslant 1$, on a dans $\mathcal{A}_{np}^*$

$$(a\theta)^{np^\nu} = (a(\theta+\nu))^n = \sum_{k=0}^{n} \binom{n}{k} (\nu a)^{n-k} (a\theta)^k$$

et par le théorème il suit $B_{m+np^\nu}(a) \equiv \sum_{k=0}^{n} \binom{n}{k} (\nu a)^{n-k} B_{m+k}(a) \bmod np\mathbb{Z}_p[\vartheta]$. Comme les deux termes sont des entiers, cette congruence est valable modulo $np\mathbb{Z}_p$. Nous retrouvons ainsi la congruence 1) (pour les polynômes de Bell) évaluée en $x = a$.

2) Par la remarque ci-dessus (et les propositions 1-4), toute racine θ de $\widetilde{g}_n(z) = (z^p - z)^n - 1$ vérifie dans $\mathcal{A}_{np}^*$

$$1 = (\theta^p - \theta)^n = ((\theta)_p)^n = \big(\theta(\theta+1)\cdots(\theta+p-1)\big)^n = \big(\theta \cdot \theta^p \cdots \theta^{p^{p-1}}\big)^n = \theta^{n\omega_p}.$$

Le nombre $\omega_p = 1 + p + p^2 + \cdots + p^{p-1}$ apparaît ici de manière naturelle et comme $a^{n\omega_p} \equiv a^n \bmod np\mathbb{Z}_p$, le théorème donne $B_{m+n\omega_p}(a) \equiv a^n B_m(a) \bmod np\mathbb{Z}_p[\vartheta]$. On retrouve ainsi la congruence 3) dans le cas où $\mathrm{ord}_p(a) = 0$.

Un cas particulier intéressant

La "formule de trace" est obtenue en considérant $n = a = 1$. Nous désignons toujours par ϑ une racine fixée de $\widetilde{g}_1(z) = z^p - z - 1$. Dans ce cas, $\mathcal{A}_p^* = \mathcal{A}_p[\vartheta] = \mathbb{F}_p[\vartheta] \cong \mathbb{F}_p[z]/(z^p - z - 1)$ est une extension cyclique de $\mathbb{F}_p$ $(= \mathcal{A}_p)$ de degré p. Il s'agit d'une extension galoisienne de type *Artin-Schreier*, dont le groupe de Galois $\mathrm{Gal}(\mathbb{F}_p[\vartheta] : \mathbb{F}_p)$, isomorphe au groupe additif $\mathbb{Z}/p\mathbb{Z}$, est engendré par l'*automorphisme de Frobenius* : $\mathbb{F}_p[\vartheta] \longrightarrow \mathbb{F}_p[\vartheta],\ \alpha \longmapsto \alpha^p$.

Le théorème montre que dans $\mathbb{F}_p[\vartheta]$, on a

$$B_m = -\sum_{\theta^p = \theta+1} \theta^{m-1} \sum_{k=0}^{p-1} \theta(\theta+1)(\theta+2)\cdots(\theta+k) = -\sum_{\theta^p=\theta+1} \theta^{m-1} \sum_{k=0}^{p-1} \theta^{1+p+p^2+\cdots+p^k}$$

L'exposant de θ dans la deuxième somme est $1 + p + p^2 + \cdots + p^k = \frac{p^{(k+1)}-1}{p-1}$ et par la congruence de Carlitz, seule sa classe modulo ω_p est intéressante. Nous allons montrer que $p - 1$ est inversible modulo ω_p, et plus généralement

Lemme. *Si $n \geqslant 1$ est inversible modulo p, alors $p^n - 1$ est inversible modulo ω_p et son inverse admet le développement p-adique*

$$\alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots + \alpha_{p-1} p^{p-1}$$

où $\alpha_k \in \{0, 1, \ldots, p-1\}$ vérifie $n\alpha_k \equiv k + 1 \bmod p$ (en particulier $\alpha_{p-1} = 0$).

PREUVE. Comme $(p-1)\omega_p = p^p - 1$, seule la classe de n modulo p est importante et on peut supposer que $1 \leqslant n \leqslant p-1$. Le polynôme cyclotomique $\omega(x) = 1+x+x^2+\cdots+x^{p-1}$ est le polynôme minimal de chacune de ses racines (en l'occurence les racines primitives p-ièmes de l'unité). Il n'a donc aucune racine commune avec le polynôme $x^n - 1$ et lui est relativement premier dans $\mathbb{Z}[x]$. Par Bézout, on conclut alors que $\omega(p)$ et $p^n - 1$ sont relativement premiers dans $\mathbb{Z}$ et donc que $p^n - 1$ est inversible modulo ω_p. Pour expliciter son inverse, considérons maintenant le polynôme

$$\tau(x) = \omega'(x) = 1 + 2x + 3x^2 + \cdots + (p-1)x^{p-2} = \Big(\frac{x^p - 1}{x-1}\Big)' = \frac{px^{p-1} - \omega(x)}{x-1}.$$

Nous avons alors

$$p^{n-1}\tau(p^n)(p^n - 1) = p^{n-1}(p \cdot p^{n(p-1)} - \omega(p^n)) = p^{np} - p^{n-1}\omega(p^n) \equiv 1 \bmod \omega_p,$$

compte tenu du fait que $p^{np} \equiv 1 \bmod p^p - 1$ et que

$$\omega(p^n) = 1 + p^n + p^{2n} + \cdots + p^{(p-1)n} \equiv 1 + p + p^2 + \cdots + p^{p-1} = \omega_p \bmod p^p - 1.$$

Modulo ω_p, l'inverse de $p^n - 1$ est donc

$$p^{n-1}\tau(p^n) = p^{n-1} + 2p^{2n-1} + 3p^{3n-1} + \cdots + (p-1)p^{(p-1)n-1}$$

et le développement p-adique s'ensuit en comparant les coefficients. □

Dénotons par $\tau_p = \tau(p) = 1 + 2p + 3p^2 + \cdots + (p-1)p^{p-2}$ l'inverse de $p-1$ modulo ω_p. Par ce qui précède, on peut alors écrire (dans $\mathbb{F}_p[\vartheta]$)

$$B_m = -\sum_{\widetilde{g}(\theta)=0} \theta^{m-1-\tau_p} \sum_{k=0}^{p-1} \theta^{\tau_p p^{(k+1)}} = -\sum_{\widetilde{g}(\theta)=0} \theta^{m-1-\tau_p} \sum_{k=0}^{p-1} (\theta + (k+1))^{\tau_p}.$$

La deuxième somme $\sum(\theta + (k+1))^{\tau_p}$ ne dépend pas de la racine θ considérée puisqu'elle vaut $\sum_{\widetilde{g}(\theta)=0} \theta^{\tau_p} = \operatorname{Tr}(\vartheta^{\tau_p})$ où $\operatorname{Tr} : \mathbb{F}_p[\vartheta] \longrightarrow \mathbb{F}_p$ désigne la *trace* de $\mathbb{F}_p[\vartheta]$ sur $\mathbb{F}_p$ que l'automorphisme de Frobenius permet de définir par $\operatorname{Tr}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{p-1}}$. On obtient ainsi simplement

$$B_m = -\operatorname{Tr}(\vartheta^{m-1-\tau_p}) \operatorname{Tr}(\vartheta^{\tau_p}) \quad (\text{dans } \mathbb{F}_p).$$

Par exemple, comme ϑ^{-1} est racine du polynôme $z^p + z^{p-1} - 1$, on a $\operatorname{Tr}(\vartheta^{-1}) = -1$ et en prenant $m = \tau_p$ dans la relation ci-dessus, on trouve $B_{\tau_p} = \operatorname{Tr}(\vartheta^{\tau_p})$ dont on connaît la valeur dans $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$ grâce à la congruence de Radoux (voir §2.11). Nous pouvons résumer tout ceci comme Barsky et Benzaghou [4] :

Théorème 16. *Soit p un nombre premier $\neq 2$, ϑ une racine de $\widetilde{g}(x) = x^p - x - 1$ et $\tau_p = 1 + 2p + 3p^2 + \cdots + (p-1)p^{p-2}$. Alors $B_m = -\operatorname{Tr}(\vartheta^{m-1-\tau_p})B_{\tau_p}$ dans $\mathbb{F}_p$.*

Le théorème 13, qui généralise les résultats de Radoux (proposition 12), se retrouve à partir de la formule de trace et du résultat suivant :

Proposition 17. *On a* $\mathrm{Tr}\big((\vartheta)_{n-1}\big) = 0$ *chaque fois que* p *ne divise pas* $n \geqslant 1$. *De même, si on peut écrire* $n \equiv n_0 + n_1 p + \cdots + n_{p-1}p^{p-1} \pmod{\omega_p}$ *avec une somme de digits* $S_p(n) = n_0 + n_1 + \cdots + n_{p-1}$ *inférieure ou égale à* $p-2$, *alors* $\mathrm{Tr}(\vartheta^n) = 0$.

PREUVE. La relation évidente $(\vartheta)_n = (\vartheta - n + n)\cdot(\vartheta-1)_{n-1} = (\vartheta-1)_n + n(\vartheta-1)_{n-1}$ montre que $\mathrm{Tr}\big((\vartheta)_n\big) = \mathrm{Tr}\big((\vartheta-1)_n\big) + n\,\mathrm{Tr}\big((\vartheta-1)_{n-1}\big)$ et on conclut en remarquant que $\mathrm{Tr}\big((\vartheta-1)_k\big) = \mathrm{Tr}\big((\vartheta)_k\big)$ pour tout entier $k \geqslant 0$. La deuxième assertion provient alors simplement du fait que $\vartheta^n = \vartheta^{n_0}(\vartheta+1)^{n_1}\cdots(\vartheta+p-1)^{n_{p-1}}$ peut être écrit dans la base de Pochhammer sous la forme $\alpha_0 + \alpha_1(\vartheta)_1 + \cdots + \alpha_{S_p(n)}(\vartheta)_{S_p(n)}$. □

La proposition montre en particulier que $\mathrm{Tr}(\vartheta^n)$ est nul pour $n = 0, 1, \ldots, p-2$, et fournit ainsi la séquence des $p-1$ zéros consécutifs dans la suite des nombres de Bell modulo p. De manière plus générale, en reprenant les notations de §2.11, on peut remarquer que

$$\tau_p(m+1) - \tau_p(m) \equiv -p^{p-m-1} \bmod \omega_p$$

(il suffit de le vérifier pour $m = 0$). Ainsi, pour $m = 0, 1, \ldots, p-1$, on a

$$\tau_p(m) - \tau_p \equiv \omega_p - p^{p-m} - p^{p-(m-1)} - \cdots - p^p = 1 + p + p^2 + \cdots + p^{p-m-1} \bmod \omega_p$$

et on pose par commodité $s = p - m - 1$. Le théorème 13 découle alors de la formule de trace et du fait que

$$\mathrm{Tr}(\vartheta^{n+p+p^2+\cdots+p^s}) \equiv -\left\{ {n \atop p-1-s} \right\} = -\left\{ {n \atop m} \right\} \bmod p\mathbb{Z}_p$$

pour tout $s \in \{0, 1, \ldots, p-1\}$ et $n \in \{0, 1, \ldots, 2p-2-s\}$ (autrement dit pour tout $m \in \{0, 1, \ldots, p-1\}$ et $n \in \{0, 1, \ldots, p-1+m\}$).

PREUVE. En développant ϑ^n dans la base de Pochhammer, on obtient

$$\mathrm{Tr}(\vartheta^{n+p+p^2+\cdots+p^s}) = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} \mathrm{Tr}(\vartheta^{p+p^2+\cdots+p^s}(\vartheta)_k)$$

et comme $\vartheta^{p^l} = \vartheta + l$ dans $\mathbb{F}_p[\vartheta]$, on peut écrire

$$\begin{aligned} \mathrm{Tr}(\vartheta^{n+p+p^2+\cdots+p^s}) &= \sum_{k=0}^{n} \left\{ {n \atop k} \right\} \mathrm{Tr}((\vartheta+1)(\vartheta+2)\cdots(\vartheta+s)(\vartheta)_k) \\ &= \sum_{k=0}^{n} \left\{ {n \atop k} \right\} \mathrm{Tr}((\vartheta+s)_{s+k}) = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} \mathrm{Tr}((\vartheta)_{s+k}). \end{aligned}$$

Par choix de n et s, la proposition 17 montre que toutes les traces intervenant dans la somme ci-dessus sont nulles sauf éventuellement pour $k = p-s-1 = m$, auquel cas $\mathrm{Tr}((\vartheta)_{s+k}) = \mathrm{Tr}(\vartheta^{\omega_p - p^{p-1}}) = \mathrm{Tr}(\vartheta^{-p^{p-1}}) = \mathrm{Tr}((\vartheta+p-1)^{-1}) = \mathrm{Tr}(\vartheta^{-1}) = -1$. □

2.14 Somme de factorielles

L'étude des polynômes de Bell a été motivée par le problème ouvert suivant

Conjecture (Kurepa). *Si p est un nombre premier impair, alors la somme*

$$\kappa_p := 0! + 1! + 2! + \cdots + (p-1)!$$

n'est pas divisible par p, en d'autres termes $|\kappa_p|_p = 1$.

Un entier $n \neq 2$ est divisible par $m = 4$ ou par un nombre premier impair $m = p$. Si κ_n était divisible par n, alors κ_m serait divisible par m et comme ce n'est pas le cas pour $m = 4$ (puisque $\kappa_4 = 10 \equiv 2 \bmod 4$), la conjecture est donc équivalente à chacun des énoncés suivants :

1) *la somme $\kappa_n = 0! + 1! + \cdots + (n-1)!$ est divisible par n uniquement lorsque $n = 2$,*
2) *si $n \neq 2$, tout diviseur impair de κ_n est strictement plus grand que n et $4 \nmid \kappa_n$,*
3) *le plus petit diviseur commun de $n!$ et de κ_n est $(n!, \kappa_n) = 2$.*

La congruence $(p-k-1)! \equiv (-1)^k (p-1)!/k! \mod p$ montre que

$$\kappa_p = \sum_{k=0}^{p-1} k! = \sum_{k=0}^{p-1} (p-1-k)! \equiv \sum_{k=0}^{p-1} (-1)^k \frac{(p-1)!}{k!} \bmod p.$$

On reconnaît tout à droite le début de la série de Taylor de $(p-1)!/e$: il ne manque qu'une série dont le terme général $a_k = (-1)^k (p-1)!/k! = (-1)^k/(p(p+1)\cdots k)$ (avec $k \geqslant p$) décroît en valeur absolue vers 0. Cette série alternée peut être encadrée par

$$(-1)^p a_p = -1/p \quad \text{et} \quad (-1)^p a_p + (-1)^{p+1} a_{p+1} = a_{p+1} - a_p = \frac{1}{p(p+1)} - \frac{1}{p} = -\frac{1}{p+1}$$

et se situe donc strictement entre -1 et 0. Au total, on obtient la formule

$$\kappa_p \equiv \Big[\frac{(p-1)!}{e}\Big] + 1 \bmod p\mathbb{Z}$$

mais ceci ne se révèle pas d'une grande utilité pour un calcul effectif lorsque p est grand. On sait [9] que κ_p est relié aux nombres de Bell par la congruence $\kappa_p \equiv B_{p-1} - 1 \bmod p$. De manière plus générale, on peut remarquer (voir §2.3) que

$$B_{-1}\Big(\frac{1}{x}\Big) = \sum_{k \geqslant 0} \begin{bmatrix} k \\ 1 \end{bmatrix} x^k = \sum_{k \geqslant 1} (k-1)! x^k = x \sum_{k \geqslant 0} k! x^k \in \mathbb{Z}_p[[x]]$$

Ainsi, pour tout entier a non divisible par p, la congruence 6) fournit

$$\sum_{k=0}^{p-1} k! a^k \equiv \sum_{k \geqslant 0} k! a^k = a^{-1} B_{-1}(a^{-1}) \equiv a^{-1}(B_{p-1}(a^{-1}) - B_0(a^{-1}))a^p \bmod p$$

et comme $a^p \equiv a \bmod p$, il s'ensuit

$$\sum_{k=0}^{p-1} k! a^k \equiv B_{p-1}(a^{-1}) - 1 \bmod p\mathbb{Z}.$$

Avec $a = 1$ et $a = -1$, on obtient en particulier

$$\sum_{k=0}^{p-1} k! \equiv B_{p-1} - 1 \bmod p \quad \text{et} \quad \sum_{k=0}^{p-1} (-1)^k k! \equiv B_{p-1}(-1) - 1 \bmod p.$$

Par addition et soustraction, on trouve respectivement

$$2(0! + 2! + \cdots + (p-1)!) \equiv B_{p-1} + B_{p-1}(-1) - 2 \bmod p,$$

$$2(1! + 3! + \cdots + (p-2)!) \equiv B_{p-1} - B_{p-1}(-1) \bmod p.$$

On peut encore remarquer que comme les congruences de Radoux et Touchard fournissent

$$B_{p^n-1} \equiv 1 + nB_{-1} \equiv 1 + n(B_{p-1} - 1) \bmod p\mathbb{Z},$$

la conjecture de Kurepa devient équivalente à la propriété suivante :

4) *si p (premier impair) ne divise pas n, alors p ne divise pas non plus $B_{p^n-1} - 1$.*

Les polynômes de Bell sont encore reliés à des sommes de factorielles par le résultat suivant, qui précise des travaux de Dragovitch [9].

Théorème 18. *Soient $a \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$ une unité p-adique et $n \geqslant 1$. Alors la série*

$$v_n(a) := \sum_{k \geqslant 0} k! a^k (k^n + a(-1)^n B_{n+1}(-a^{-1}))$$

(qui converge dans $\mathbb{Z}_p$) est une somme finie.

PREUVE. En appliquant l'opérateur linéaire $(x+m)_m \longmapsto a^{-m}$ à la fonction

$$x^n = \sum_{l=0}^{n} \binom{n}{l} (-1)^{n-l} (x+1)^l = \sum_{l=0}^{n} \binom{n}{l} (-1)^{n-l} \sum_{m=0}^{l} \left\{ {l \atop m} \right\} (-1)^{l-m} (x+m)_m \,, \qquad (*)$$

on trouve

$$(-1)^n \sum_{l=0}^{n} \binom{n}{l} \sum_{m=0}^{l} \left\{ {l \atop m} \right\} (-a^{-1})^m = (-1)^n \sum_{l=0}^{n} \binom{n}{l} B_l(-a^{-1}) = (-1)^{n+1} a B_{n+1}(-a^{-1}).$$

On peut donc écrire $x^n + (-1)^n a B_{n+1}(-a^{-1}) = \sum_{m=0}^{n} \alpha_m (x+m)_m$ avec $\sum_{m=0}^{n} a^{-m} \alpha_m = 0$.

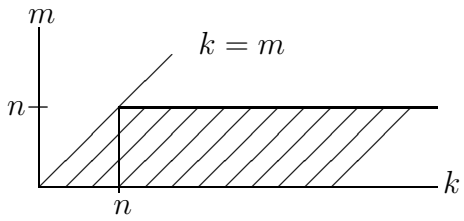
Pour être un peu plus précis, on peut d'ailleurs expliciter

$$\alpha_0 = (-1)^n a B_{n+1}(-a^{-1}) + (-1)^n \ \text{ et } \ \alpha_m = \left\{ {n+1 \atop m+1} \right\} (-1)^{n-m} \ \text{ pour } \ m \geqslant 1$$

en permutant les deux sommes dans $(*)$. On obtient alors

$$v_n(a) = \sum_{k\geqslant 0} k! a^k \sum_{m=0}^{n} \alpha_m (k+m)_m = \sum_{m=0}^{n} \alpha_m \sum_{k\geqslant 0} a^k (k+m)! = \sum_{m=0}^{n} \alpha_m \sum_{k\geqslant m} a^{k-m} k!$$

Le domaine de sommation (pour les deux sommes) est donné par la zone hachurée suivante



que l'on peut partager en deux parties. On voit ainsi que

$$v_n(a) = \sum_{k=0}^{n} k! \sum_{m=0}^{k} \alpha_m a^{k-m} + \sum_{k>n} k! a^k \sum_{m=0}^{n} \alpha_m a^{-m} = \sum_{k=0}^{n} k! \sum_{m=0}^{k} \alpha_m a^{k-m}$$

est une somme finie. □

En particulier, les sommes $v_n(\pm 1)$ décrivent des entiers, et on a par exemple

n	$v_n(1) = \sum k!(k^n + (-1)^n B_{n+1}(-1))$	$v_n(-1) = \sum k!(-1)^k (k^n + (-1)^{n+1} B_{n+1})$
1	$\sum k!k = -1$	$\sum k!(-1)^k (k+2) = 1$
2	$\sum k!(k^2+1) = 1$	$\sum k!(-1)^k (k^2-5) = -3$
3	$\sum k!(k^3-1) = 1$	$\sum k!(-1)^k (k^3+15) = 9$
4	$\sum k!(k^4-2) = -5$	$\sum k!(-1)^k (k^4-52) = -31$
5	$\sum k!(k^5+9) = 5$	$\sum k!(-1)^k (k^5+203) = 121$

Partie 3

Déterminants de Hankel et polynômes orthogonaux

"Une bonne partie des mathématiques devenues utiles se sont développées sans aucun désir d'être utiles, dans une situation où personne ne pouvait savoir dans quels domaines elles le deviendraient."

John von Neumann

3.1 Première approche

Dans le chapitre précédent, nous avons été amenés à considérer des matrices dites de Hankel, de la forme

$$H_n = \begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_n \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{n+1} \\ \vdots & \vdots & & \vdots \\ \alpha_n & \alpha_{n+1} & \cdots & \alpha_{2n} \end{pmatrix}$$

construites à l'aide des polynômes de Bell, et dont les déterminants se sont révélés d'une grande importance pour établir certaines congruences (voir §2.11). Nous développons dans cette dernière partie un contexte général qui montre comment de tels déterminants peuvent être calculés, sous certaines conditions, et comment ils permettent d'établir des congruences pour la suite initiale $(\alpha_n)_{n\geqslant 0}$ en associant une famille de polynômes orthogonaux. Nous considérons en toute généralité un anneau $\mathcal{A}$ unitaire, commutatif et intègre. Le groupe additif sous-jacent agit alors par *convolution binomiale* sur l'ensemble

$$\mathcal{F}(\mathbb{N},\mathcal{A}) = \{\text{fonctions } \alpha : \mathbb{N} \longrightarrow \mathcal{A}\} = \{\text{suites } (\alpha_n)_{n\geqslant 0} \subset \mathcal{A}\} :$$

Pour $a \in \mathcal{A}$ et $\alpha \in \mathcal{F}(\mathbb{N},\mathcal{A})$, on définit $T^a\alpha \in \mathcal{F}(\mathbb{N},\mathcal{A})$ par

$$(T^a\alpha)_n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}\alpha_k$$

et on vérifie que $T^aT^b = T^{a+b}$ $(a,b \in \mathcal{A})$. Cette action préserve les déterminants de Hankel :

Proposition 1. *Si H_n est la matrice de Hankel (d'ordre n) associée à $\alpha \in \mathcal{F}(\mathbb{N},\mathcal{A})$, alors la matrice de Hankel (d'ordre n) associée à la convolution $T^a\alpha \in \mathcal{F}(\mathbb{N},\mathcal{A})$ est*

$$H_{a,n} = SH_nS^t \quad \text{où} \quad S = S_n(a) = \left(\binom{i}{j}a^{i-j}\right)_{0\leqslant i,j\leqslant n}.$$

En particulier, $\det H_{a,n} = \det H_n$ *ne dépend pas de* $a \in \mathcal{A}$.

PREUVE. Par calcul direct, nous avons

$$(SHS^t)_{ij} = \sum_{k=0}^{n} S_{jk} \sum_{l=0}^{n} S_{il}H_{lk} = \sum_{k\geqslant 0} \binom{j}{k} a^{j-k} \sum_{l\geqslant 0} \binom{i}{l} a^{i-l}\alpha_{l+k}.$$

En posant $m = k+l$ et en utilisant la formule de convolution de Vandermonde, on obtient

$$(SHS^t)_{ij} = \sum_{m\geqslant 0}\sum_{k=0}^{m} \binom{j}{k}\binom{i}{m-k} a^{i+j-m}\alpha_m = \sum_{m\geqslant 0} \binom{i+j}{m} a^{i+j-m}\alpha_m,$$

autrement dit $(SHS^t)_{ij} = (T^a\alpha)_{i+j} = (H_{a,n})_{ij}$. □

Remarquons que, pour tout élément $a \in \mathcal{A}$, la matrice $S_n(a)$ est triangulaire inférieure et qu'elle vérifie $S_n(a)S_n(b) = S_n(a+b)$, en particulier $S_n(a) = S_n(1)^a$ lorsque $a \in \mathbb{Z}$. Les divers articles de C. Radoux [27],[28],[29] conduisent au résultat général suivant.

Proposition 2. *Notons $F(z) = \sum \alpha_n \frac{z^n}{n!}$ la série génératrice exponentielle associée à une suite $\alpha \in \mathcal{F}(\mathbb{N}, \mathcal{A})$ et $\partial = \partial_z$ l'opérateur de dérivation par rapport à la variable z. S'il existe des séries formelles $F_k(z) \in \mathcal{A}[[z]]$ et des éléments $d_k \in \mathcal{A}$ tels que*

1) $\big[\partial^n F_k(z)\big]_{z=0} = 0$ *chaque fois que* $k > n$,

2) $\sum\limits_{k\geqslant 0} d_k F_k(y) F_k(z) = F(y+z)$,

alors les déterminants de Hankel sont donnés par $\det H_n = \prod\limits_{k=0}^{n} d_k \big[\partial^k F_k(z)\big]^2_{z=0}$.

PREUVE. A l'aide de l'identité binomiale, on peut écrire

$$F(y+z) = \sum_{n\geqslant 0} \alpha_n \frac{(y+z)^n}{n!} = \sum_{m,n\geqslant 0} \alpha_{m+n} \frac{y^n}{n!}\frac{z^m}{m!}$$

alors que les développements de Taylor

$$F_k(y) = \sum_{n\geqslant 0} \partial^n F_k(0) \frac{y^n}{n!} \quad \text{et} \quad F_k(z) = \sum_{m\geqslant 0} \partial^m F_k(0) \frac{z^m}{m!}$$

permettent d'expliciter

$$\sum_{k\geqslant 0} d_k F_k(y) F_k(z) = \sum_{m,n\geqslant 0} \sum_{k\geqslant 0} d_k \ \partial^n F_k(0) \ \partial^m F_k(0) \ \frac{y^n}{n!}\frac{z^m}{m!}$$

Par identification, la deuxième condition exprime le fait que

$$\alpha_{m+n} = \sum_{k\geqslant 0} d_k \Big[\partial^n F_k(z)\Big]_{z=0} \Big[\partial^m F_k(z)\Big]_{z=0}$$

(remarquons que la somme est finie, elle porte sur les indices $k = 0, 1, \dots, \min(m,n)$). Ainsi la matrice de Hankel $H_n = (\alpha_{i+j})_{0\leqslant i,j\leqslant n}$ admet une décomposition $H_n = L_n D_n L_n^t$ où $D_n = \mathrm{Diag}(d_0, d_1, \dots, d_n)$ est une matrice diagonale et $L_n = \big(\partial^i F_j(z)\big|_{z=0}\big)_{0\leqslant i,j\leqslant n}$ une matrice triangulaire inférieure, par la condition 1). La proposition est alors évidente. □

Un cas particulier important

Si $\mathcal{A}$ est un anneau de polynômes, on peut considérer des suites $(P_n(x))_{n\geqslant 0}$ telles que $\deg P_n(x) = n$. La fonction génératrice exponentielle est alors $F(x,z) = \sum_{n\geqslant 0} P_n(x)\frac{z^n}{n!}$ et dans de nombreux cas, on peut prendre $F_k(x,z) = \partial_x^k F(x,z)$ où ∂_x est l'opérateur de

dérivation par rapport à x. La première condition de la proposition est alors automatiquement vérifiée :

$$\Big[\partial_z^n F_k(x,z)\Big]_{z=0} = \Big[\partial_z^n \partial_x^k F(x,z)\Big]_{z=0} = \partial_x^k \Big[\partial_z^n F(x,z)\Big]_{z=0} = \partial_x^k P_n(x)$$

est nul dès que $k > n$. Ainsi, s'il existe des polynômes $d_k(x)$ vérifiant

$$\sum_{k\geqslant 0} d_k(x)\partial_x^k F(x,y)\partial_x^k F(x,z) = F(x,y+z), \qquad (*)$$

alors les déterminants de Hankel sont $\det(P_{i+j}(x))_{0\leqslant i,j\leqslant n} = \prod_{k=0}^{n} d_k(x)\Big(\partial^k P_k(x)\Big)^2$.

Exemples

1. L'exemple le plus simple est celui de la *base canonique* $P_n(x) = x^n$: on a $F(x,z) = e^{xz}$ et la relation $(*)$ peut s'écrire $\sum_{k\geqslant 0} d_k(x)(yz)^k = 1$. Les polynômes constants $d_0(x) = 1$, $d_k(x) = 0$ si $k \geqslant 1$ sont bien appropriés et la proposition confirme le résultat évident

$$\det(x^{i+j})_{0\leqslant i,j\leqslant n} = d_n(x) = \begin{cases} 1 & \text{si } n = 0 \\ 0 & \text{sinon} \end{cases}$$

2. Pour les polynômes $P_n(x) = n!x^n$, de fonction génératrice $F(x,z) = (1-zx)^{-1}$, on trouve $\partial_x^k F(x,z) = k!z^k(1-zx)^{-k-1}$ (pour $k \geqslant 0$). La relation $(*)$ devient

$$\sum_{k\geqslant 0} d_k(x)(k!)^2(yz)^k[1-x(y+z)+x^2yz]^{-k-1} = (1-x(y+z))^{-1}.$$

En considérant ici les polynômes $d_k(x) = (x^k/k!)^2$, on obtient

$$\det((i+j)!x^{i+j})_{0\leqslant i,j\leqslant n} = \prod_{k=0}^{n}(x^k/k!)^2(k!)^4 = \prod_{k=0}^{n}(k!x^k)^2 = \Big(\prod_{k=0}^{n} k!\Big)^2 x^{n(n+1)}.$$

3. Les polynômes $D_n(x) = \sum_{k=0}^{n}(n)_k(-1)^{n-k}x^k$ engendrent les mêmes déterminants : la fonction génératrice exponentielle est donnée par $F(x,z) = e^{-z}(1-xz)^{-1}$ et la relation $(*)$ se réécrit exactement comme ci-dessus. De manière plus générale, on a vu (proposition 1) que les déterminants de Hankel engendrés par une suite

$$P_{a,n}(x) = \sum_{k=0}^{n}\binom{n}{k}(-a)^{n-k}P_k(x)$$

ne dépendent pas de $a \in \mathcal{A}$ et coïncident donc avec ceux de la suite $P_{0,n}(x) = P_n(x)$. Les polynômes $D_n(x)$ s'obtiennent à partir de $P_n(x) = n!x^n$ et $a = 1$. Leur étude est

intéressante puisque $D_n(1)$ est le nombre de *dérangements* (i.e. de permutations sans point fixe) d'un ensemble à n éléments.

4. Soit I_n le nombre d'*involutions* sur un ensemble à n éléments, c'est-à-dire le nombre de permutations $\sigma \in Sym(n)$ d'ordre 2. Nous avons $I_0 = I_1 = 1$ et la relation de récurrence $I_{n+1} = I_n + nI_{n-1}$ conduit à la fonction génératrice $\sum I_n \frac{z^n}{n!} = e^{z+z^2/2}$. Pour utiliser la méthode présentée ci-dessus, il faut construire des polynômes $I_n(x)$ dont I_n serait une valeur particulière et il semble naturel de considérer $\sum I_n(x)\frac{z^n}{n!} = e^{xz+z^2/2} =: F(x,z)$. On a $I_n(1) = I_n$ et en dérivant $F(x,z)$ par rapport à z, on trouve $I_{n+1}(x) = xI_n(x) + nI_{n-1}(x)$, ce qui montre du même coup que les polynômes $I_n(x)$ sont unitaires avec $\deg I_n(x) = n$. La relation $(*)$ devient

$$\sum_{k\geqslant 0} d_k(x)(yz)^k = e^{yz},$$

et avec $d_k(x) = 1/k!$, la proposition donne

$$\det(I_{i+j}(x))_{0\leqslant i,j\leqslant n} = \prod_{k=0}^{n}(1/k!)(k!)^2 = \prod_{k=0}^{n} k! = \det(I_{i+j})_{0\leqslant i,j\leqslant n}.$$

5. Les *polynômes d'Hermite* $H_n(x)$ admettent la fonction génératrice $F(x,z) = e^{2xz-z^2}$ et satisfont la relation de récurrence $H_{n+1}(x) = 2xH_n(x) - 2nH_{n-1}(x)$. La relation $(*)$ devient

$$\sum_{k\geqslant 0} d_k(x)(4yz)^k = e^{-2yz}.$$

Elle est vérifiée pour les polynômes constants $d_k(x) = 1/((-2)^k k!)$ et comme le coefficient dominant de $H_k(x)$ est 2^k, on trouve

$$\det(H_{i+j}(x))_{0\leqslant i,j\leqslant n} = \prod_{k=0}^{n}\frac{1}{(-2)^k k!}(2^k k!)^2 = \prod_{k=0}^{n} k!(-2)^k = \Big(\prod_{k=0}^{n} k!\Big)(-2)^{n(n+1)/2}.$$

6. Considérons maintenant les *polynômes de Bell* $B_n(x)$ étudiés au chapitre 2. On a $F(x,z) = e^{xg(z)}$ avec $g(z) = e^z - 1$ et $(*)$ devient

$$\sum_{k\geqslant 0} d_k(x)(e^{y+z} - e^y - e^z + 1)^k = e^{x(e^{y+z}-e^y-e^z+1)}.$$

Ceci est vérifié pour $d_k(x) = x^k/k!$, et on obtient

$$\det(B_{i+j}(x))_{0\leqslant i,j\leqslant n} = \prod_{k=0}^{n}(x^k/k!)(k!)^2 = \prod_{k=0}^{n} k!x^k = \Big(\prod_{k=0}^{n} k!\Big)x^{n(n+1)/2}.$$

En revoyant la preuve de la proposition 2, on retrouve l'identité de Radoux (voir §2.4).

7. Les *nombres d'Euler* E_n ($n \geqslant 0$) peuvent être définis par $F(z) = \sum E_n \frac{z^n}{n!} = 1/\cos z$. Cette fonction génératrice exponentielle vérifie

$$F(y+z) = \frac{1}{\cos(y+z)} = \frac{\cos y \cos z}{\cos y \cos z - \sin y \sin z} \; \frac{1}{\cos y \cos z} = \frac{(1-\tan y \tan z)^{-1}}{\cos y \cos z}$$

ce qui, à l'aide d'une série géométrique, peut s'exprimer formellement

$$F(y+z) = \frac{1}{\cos y \cos z} \sum_{k\geqslant 0} (\tan y)^k (\tan z)^k = \sum_{k\geqslant 0} \frac{(\tan y)^k}{\cos y} \frac{(\tan z)^k}{\cos z}.$$

La deuxième condition de la proposition est donc vérifiée si l'on considère les constantes $d_k(z) = 1$ et les fonctions $F_k(z) = (\tan z)^k/\cos z$. La première condition l'est également :

$$E_{n,k} := \big[\partial^n F_k(z)\big]_{z=0} = \Big[\partial^n \frac{(\tan z)^k}{\cos z}\Big]_{z=0} \quad \text{est nul lorsque } k > n \text{ et vaut } n! \text{ si } k = n.$$

Ceci est évident pour $n = 0$ et persiste par induction grâce à la relation de récurrence $E_{n+1,k} = kE_{n,k-1} + (k-1)E_{n,k+1}$. En fin de compte, la proposition 2 fournit

$$\det(E_{i+j})_{0\leqslant i,j\leqslant n} = \Big(\prod_{k=0}^{n} k!\Big)^2.$$

Avec cette définition, les nombres d'Euler d'indices impairs sont nuls et certaines personnes préfèrent travailler avec $\widetilde{E}_n = E_{2n}$. On trouverait alors

$$\det(\widetilde{E}_{i+j})_{0\leqslant i,j\leqslant n} = \det(E_{2(i+j)})_{0\leqslant i,j\leqslant n} = \Big(\prod_{k=0}^{n} (2k)!\Big)^2$$

en modifiant légèrement la fin de preuve de la proposition.

3.2 Fonction génératrice exponentielle

Dans l'exemple des nombres d'Euler (de fonction génératrice $F(z) = 1/\cos z$), nous avons introduit les fonctions $F_k(z) = g(z)^k F(z)$ où $g(z) = \tan z$ vérifie l'équation différentielle $g'(z) = 1 + g(z)^2$ avec la condition initiale $g(0) = 0$. Cette situation peut être généralisée comme suit.

Théorème 3. *On considère une fonction génératrice exponentielle $F(z) = \exp G(z)$ avec $G(0) = 0$ et on suppose que $g(z) = G'(z) - G'(0)$ vérifie $g'(z) = \alpha + \beta g(z) + \gamma g(z)^2$ pour certains paramètres $\alpha \neq 0$, β et γ dans $\mathcal{A}$. Alors*

$$F(y+z) = \sum_{k\geqslant 0} \frac{1\cdot(1+\gamma)\cdots(1+(k-1)\gamma)}{k!\alpha^k} \; g(y)^k F(y) \; g(z)^k F(z).$$

Les déterminants de Hankel correspondants sont donnés par

$$\det H_n = \alpha^{n(n+1)/2} \prod_{k=0}^{n} \Big(k!(1+\gamma)\cdots(1+(k-1)\gamma) \Big).$$

PREUVE. Pour $k \geqslant 0$, on considère les fonctions $F_k(z) = g(z)^k F(z)$. On peut écrire

$$\begin{aligned} \partial F_k &= k g^{k-1} g' F + g^k F' \\ &= k g^{k-1}(\alpha + \beta g + \gamma g^2) F + g^k G' F \\ &= \big(k\alpha g^{k-1} + (G'(0) + k\beta) g^k + (1+k\gamma) g^{k+1} \big) F \\ &= k\alpha F_{k-1} + (G'(0) + k\beta) F_k + (1+k\gamma) F_{k+1} \end{aligned}$$

(par convention, $F_k(z) = 0$ pour $k < 0$), c'est-à-dire

$$\partial^{n+1} F_k(z) = \partial^n \big[k\alpha F_{k-1}(z) + (G'(0) + k\beta) F_k(z) + (1+k\gamma) F_{k+1}(z) \big] \quad \text{pour } n \geqslant 0.$$

Cette relation nous permet d'établir inductivement les faits suivants (évidents pour $n = 0$) :

- $\big[\partial^n F_k(z)\big]_{z=0} = 0$ chaque fois que $k > n$,
- $\big[\partial^n F_n(z)\big]_{z=0} = n\alpha \big[\partial^{n-1} F_{n-1}(z)\big]_{x=0} = \cdots = n!\alpha^n$.

Un calcul direct montre d'autre part que

$$\partial^{n+1} F_k(z)\ \partial^m F_k(z) - \partial^n F_k(z)\ \partial^{m+1} F_k(z) = k\alpha H_{k-1}(z) - (1+k\gamma) H_k(z)$$

avec $H_k(z) = \partial^m F_{k+1}(z)\ \partial^n F_k(z) - \partial^m F_k(z)\ \partial^n F_{k+1}(z)$ ($= 0$ si $k < 0$).

Considérons alors les éléments (dans $\operatorname{Frac} \mathcal{A}$, corps des fractions de $\mathcal{A}$)

$$d_k = \frac{(1+\gamma)\cdots(1+(k-1)\gamma)}{k!\alpha^k} \quad (= 1 \text{ si } k = 0).$$

Ils vérifient $d_{k+1}(k+1)\alpha = d_k(1+k\gamma)$, de sorte que tous les termes de la somme

$$\sum_{k \geqslant 0} d_k \big[\partial^{n+1} F_k(z)\ \partial^m F_k(z) - \partial^n F_k(z)\ \partial^{m+1} F_k(z) \big] = \sum_{k \geqslant 0} d_k [k\alpha H_{k-1}(z) - (1+k\gamma) H_k(z)]$$

se compensent : il s'agit d'une somme téléscopique nulle. Pour tous les entiers $m, n \geqslant 0$, on a donc

$$\sum d_k \partial^n F_k(z)\ \partial^m F_k(z) = \sum d_k \partial^{n-1} F_k(z)\ \partial^{m+1} F_k(z) = \cdots = \sum d_k F_k(z)\ \partial^{m+n} F_k(z)$$

et en évaluant cette expression en $z = 0$, il vient

$$\sum d_k \big[\partial^n F_k(z)\ \partial^m F_k(z) \big]_{z=0} = \sum d_k F_k(0) \big[\partial^{m+n} F_k(z) \big]_{z=0} = \big[\partial^{m+n} F(z) \big]_{z=0}.$$

Cela montre que pour la suite qui admet la fonction génératrice $F(z)$, on peut utiliser la proposition 2 avec les éléments d_k et les fonctions $F_k(z)$ définis ci-dessus. □

Voici les données correspondant aux exemples (1-7) déjà traités :

	$F(z)$	$G(z)$	$g(z)$	α	β	γ
Base canonique	e^{xz}	xz	x	0	0	0
$P_n(x) = n!x^n$	$(1-xz)^{-1}$	$-\log(1-xz)$	$\frac{x}{1-xz} - x$	x^2	$2x$	1
Polynômes de dérangement	$e^{-z}(1-xz)^{-1}$	$-z-\log(1-xz)$	$\frac{x}{1-xz} - x$	x^2	$2x$	1
Polynômes d'involution	$e^{xz+z^2/2}$	$xz + \frac{z^2}{2}$	z	1	0	0
Polynômes d'Hermite	e^{2xz-z^2}	$2xz - z^2$	$-2z$	-2	0	0
Polynômes de Bell	$e^{x(e^z-1)}$	$x(e^z-1)$	$x(e^z-1)$	x	1	0
Nombres d'Euler	$1/\cos z$	$-\log(\cos z)$	$\tan z$	1	0	1

Nous pouvons ajouter les exemples suivants :

8. La suite décalée des polynômes de Bell $(B_{n+1}(x))_{n\geqslant 0}$ admet la fonction génératrice $F(x,z) = xe^z e^{x(e^z-1)}$. Elle mène à $g(z) = x(e^z-1)$ comme pour la suite $(B_n(x))$ et donc

$$\det(B_{i+j+1}(x))_{0\leqslant i,j\leqslant n} = \det(B_{i+j}(x))_{0\leqslant i,j\leqslant n} = \Big(\prod_{k=0}^{n} k!\Big) x^{n(n+1)/2}$$

pour tout $n \geqslant 0$. Cette propriété caractérise d'ailleurs la suite des polynômes de Bell.

Les polynômes $\widehat{B}_n(x)$ de fonction génératrice exponentielle $F(x,z) = \exp\big(\frac{e^{xz}-1}{x}\big)$ donnent également lieu aux mêmes déterminants de Hankel que les polynômes de Bell $B_n(x)$.

9. Les *polynômes d'Euler* $(E_n^m(x))$ *d'ordre* $m \geqslant 1$ sont définis par la fonction génératrice $F(x,z) = \big(\frac{2}{e^z+1}\big)^m e^{xz}$. Par la proposition 1, on peut simplement considérer la fonction génératrice $F(z) = F(0,z)$ pour évaluer les déterminants de Hankel associés. On trouve $g(z) = m\big(\frac{1}{e^z+1} - \frac{1}{2}\big)$ et on peut appliquer le théorème avec $\alpha = -\frac{m}{4}$, $\beta = 0$ et $\gamma = \frac{1}{m}$:

$$\det H_n(x) = \Big(-\frac{1}{4}\Big)^{n(n+1)/2} \prod_{k=0}^{n} k!\; m(m+1)\cdots(m+k-1) = \det H_n(0).$$

Le lecteur pourra retrouver les déterminants de Hankel associés aux nombres d'Euler ordinaires E_n (exemple 7) en remarquant que $E_n = (-2)^n E_n^1(\frac{1}{2})$. De nombreux résultats de [1], [6], [7], [27] et [28] peuvent également être retrouvés.

3.3 Fonctions génératrices ordinaires

Le théorème précédent, concernant des fonctions génératrices exponentielles (ou "séries de Hurwitz"), peut être transcrit pour des fonctions génératrices ordinaires $F(z) = \sum \alpha_k z^k$. Ayant considéré des séries de Hurwitz $F(z) = \exp G(z) = \sum \frac{G(z)^k}{k!}$ avec $G(0) = 0$, nous pouvons, par analogie, nous intéresser à des fonction génératrices ordinaires de la forme

$$F(z) = \sum G(z)^k = \frac{1}{1 - G(z)} \text{ avec } G(0) = 0.$$

L'opérateur de dérivation ∂ tirait son importance du fait qu'il est *"associé"* à la base polynomiale ($f_n(z) = z^n/n!$), dans le sens où $\partial f_0(z) = 0$ et $\partial f_n(z) = f_{n-1}(z)$ pour $n \geqslant 1$. Son analogue dans notre nouveau contexte est donné par $\nabla : f(z) \longmapsto \frac{f(z)-f(0)}{z}$, opérateur associé à la base canonique (z^n).

Théorème 4. *Considérons une fonction génératrice ordinaire $F(z) = \frac{1}{1-G(z)}$ avec $G(0) = 0$ et supposons que $g(z) = \nabla G(z) - \nabla G(0) = \frac{G(z)}{z} - G'(0)$ vérifie une relation $g(z) = z(\alpha + \beta g(z) + \gamma g(z)^2)$ pour certains paramètres $\alpha \neq 0$, β et γ dans $\mathcal{A}$. Alors les déterminants de Hankel sont donnés par*

$$\det H_n = \alpha^{n(n+1)/2} \gamma^{n(n-1)/2}.$$

PREUVE. Les fonctions $F_k(z) = g(z)^k F(z)$ vérifient $\nabla F_0(z) = G'(0)F_0(z) + F_1(z)$ et

$$\nabla F_k(z) = \alpha F_{k-1}(z) + \beta F_k(z) + \gamma F_{k+1}(z) \quad \text{pour tout } k \geqslant 1.$$

Par induction, on établit

$$\big[\nabla^n F_k(z)\big]_{z=0} = 0 \text{ si } k > n \quad , \quad \big[\nabla^n F_n(z)\big]_{z=0} = \alpha^n.$$

D'autre part, on montre directement que

$$\nabla^{n+1} F_k(z)\ \nabla^m F_k(z) - \nabla^n F_k(z)\ \nabla^{m+1} F_k(z) = \begin{cases} -H_0(z) & \text{si } k = 0 \\ \alpha H_{k-1}(z) - \gamma H_k(z) & \text{si } k \geqslant 1 \end{cases}$$

avec $H_k(z) = \nabla^m F_{k+1}(z) \nabla^n F_k(z) - \nabla^m F_k(z) \nabla^n F_{k+1}(z)$. En considérant les éléments $d_0 = 1$ et $d_k = \gamma^{k-1}/\alpha^k$ pour $k \geqslant 1$, on voit que

$$\sum_{k \geqslant 0} d_k \big[\nabla^{n+1} F_k(z)\ \nabla^m F_k(z) - \nabla^n F_k(z)\ \nabla^{m+1} F_k(z)\big]$$

est une somme téléscopique nulle. Pour tous les entiers $m, n \geqslant 0$, on peut écrire

$$\sum d_k \nabla^n F_k(z)\ \nabla^m F_k(z) = \sum d_k \nabla^{n-1} F_k(z)\ \nabla^{m+1} F_k(z) = \cdots = \sum d_k F_k(z)\ \nabla^{m+n} F_k(z)$$

et une évaluation en $z = 0$ donne $\sum d_k \big[\nabla^n F_k(z)\ \nabla^m F_k(z)\big]_{z=0} = \big[\nabla^{m+n} F(z)\big]_{z=0}$. On conclut comme dans la preuve de la proposition 2. □

Remarque

Comme $\frac{G(z)}{z} = \frac{1}{z}\big(1 - \frac{1}{F(z)}\big) = \frac{F(z)-1}{zF(z)} \underset{z\to 0}{\longrightarrow} F'(0)$, on peut expliciter $g(z) = \frac{F(z)-1}{zF(z)} - F'(0)$, donc $F(z) = (1 - F'(0)z - zg(z))^{-1}$. De plus, la condition initiale $g(0) = 0$ et la relation quadratique $g(z) = z(\alpha + \beta g(z) + \gamma g(z)^2)$ montrent que

$$g(z) = \frac{1 - \beta z - \sqrt{(1-\beta z)^2 - 4\gamma\alpha z^2}}{2\gamma z} \qquad (\text{si } \gamma \neq 0).$$

Exemples

1. Pour les *nombres de Catalan* $C_n = \frac{1}{n+1}\binom{2n}{n}$, on a $F(z) = \frac{1-\sqrt{1-4z}}{2z}$ et donc

$$g(z) = \frac{1 - \sqrt{1-4z} - 2z}{z(1-\sqrt{1-4z})} - 1 = \frac{4z - 2z(1+\sqrt{1-4z})}{4z^2} - 1 = \frac{1 - 2z - \sqrt{1-4z}}{2z}.$$

On peut utiliser le théorème avec $\gamma = 1$, $\beta = 2$ et $\alpha = 1$: on obtient $\det H_n = 1$ pour tout entier $n \geqslant 0$.

Les *nombres de Motzkin*, définis par la fonction génératrice $F(z) = \frac{1-z-\sqrt{1-2z-3z^2}}{2z^2}$, engendrent les mêmes déterminants (avec $\gamma = \beta = \alpha = 1$).

2. Les *polynômes de Legendre* sont définis par $F(x,z) = (1 - 2xz + z^2)^{-1/2}$ et le théorème peut être utilisé avec $\alpha = \frac{x^2-1}{2}$, $\beta = x$ et $\gamma = \frac{1}{2}$. On trouve alors

$$\det H_n(x) = \frac{(x^2-1)^{n(n+1)/2}}{2^{n^2}}.$$

3.4 Polynômes orthogonaux

Nous supposons dans ce paragraphe que $\mathcal{A}$ est un sous-anneau de $\mathbb{R}$ et nous nous plaçons dans le contexte du calcul symbolique : pour une suite donnée $\alpha \in \mathcal{F}(\mathbb{N}, \mathcal{A})$, on considère l'application $\mathcal{A}$-linéaire

$$\Phi : \mathcal{A}[x] \longrightarrow \mathcal{A},\ x^n \longmapsto \alpha_n.$$

Nous supposerons de plus que les déterminants de Hankel sont tous positifs. Cela signifie que pour un entier n fixé, la matice symétrique H_n est définie positive et que l'application bilinéaire

$$(f, g) \longmapsto (f \mid g) := \Phi(f(x)g(x))$$

est un produit scalaire sur $V_n[x] := \{P(x) \in \mathcal{A}[x]\ :\ \deg P \leqslant n\}$ (la matrice de Gram dans la base canonique étant donnée par la matrice de Hankel H_n). Comme ceci est valable pour tout entier $n \geqslant 0$, cette application définit un produit scalaire sur $\mathcal{A}[x] = \bigcup V_n[x]$. Une

famille orthogonale de polynômes unitaires est alors obtenue par le procédé d'orthogonalisation de Gram-Schmidt :

$$P_0(x) = 1 \quad , \quad P_n(x) = \frac{1}{\det H_{n-1}} \begin{vmatrix} \alpha_0 & \cdots & \alpha_{n-1} & 1 \\ \alpha_1 & \cdots & \alpha_n & x \\ \vdots & & \vdots & \vdots \\ \alpha_n & \cdots & \alpha_{2n-1} & x^n \end{vmatrix} \quad \text{pour } n \geqslant 1$$

et on notera $P_n(x) = p_{n,0} + p_{n,1}x + p_{n,2}x^2 + \cdots + p_{n,n-1}x^{n-1} + x^n$ ($p_{n,n} = 1$). Ces polynômes unitaires admettent des coefficients dans $\operatorname{Frac}\mathcal{A}$ et vérifient une relation de récurrence à trois termes [34]

$$P_{n+1}(x) = (x - \lambda_n)P_n(x) - \mu_n P_{n-1}(x) \qquad (\text{pour } n \geqslant 1)$$

avec $\lambda_n = p_{n,n-1} - p_{n+1,n}$ et $\mu_n = \|P_n(x)\|^2 / \|P_{n-1}(x)\|^2$.

Comme la matrice de Hankel (d'un certain ordre n) est symétrique définie positive, elle admet une unique décomposition de la forme $H = LDL^t$ où L est une matrice triangulaire inférieure avec des 1 sur la diagonale et $D = \operatorname{Diag}(d_0, d_1, \ldots, d_n)$ est une matrice diagonale. La relation $L^{-1}H(L^{-1})^t = D$ montre alors que

$$L^{-1} = \begin{pmatrix} p_{0,0} & 0 & \cdots & 0 \\ p_{1,0} & p_{1,1} & \ddots & \vdots \\ \vdots & & \ddots & 0 \\ p_{n,0} & p_{n,1} & \cdots & p_{n,n} \end{pmatrix}.$$

La k-ième ligne de L^{-1} est formée avec les coefficients de $P_k(x)$ et on a $\|P_k(x)\|^2 = d_k$. On en déduit ainsi que $\mu_k = d_k/d_{k-1}$ et que $\det H_n = \|P_0(x)\|^2 \cdot \|P_1(x)\|^2 \cdots \|P_n(x)\|^2$.

D'autre part, la matrice $M = L^{-1}$ admet le polynôme caractéristique $P_M(x) = (1-x)^{n+1}$ et le théorème de Cayley-Hamilton permet d'exprimer formellement (avec l'opérateur ∇ défini précédemment)

$$L = M^{-1} = -\frac{1}{\det M}\big[\nabla P_M(x)\big]_{x=M} = \sum_{l=1}^{n+1} \binom{n+1}{l} (-1)^{l-1} M^{l-1}.$$

En considérant les éléments situés juste au-dessous de la diagonale de $M, M^2, ..., M^n$, on voit que $L_{k+1,k} = -p_{k+1,k}$, de sorte que $\lambda_k = L_{k+1,k} - L_{k,k-1}$.

Théorème 5. *Si les déterminants de Hankel sont tous positifs et ont pu être déterminés par la fonction génératrice exponentielle (théorème 3) (resp. ordinaire, théorème 4), alors*

$$\lambda_n = G'(0) + n\beta \quad \textit{et} \quad \mu_n = n\alpha(1 + (n-1)\gamma) \quad \textit{pour tout } n \geqslant 1$$
$$(\textit{resp.} \quad \lambda_1 = \beta,\ \mu_1 = \alpha \ \textit{et} \ \ \lambda_n = \beta,\ \mu_n = \alpha\gamma \quad \textit{pour tout } n \geqslant 2)$$

PREUVE. Avec les notations précédentes et la normalisation désirée, on a

$$\mu_n = \frac{d_n\big[\partial^n F_n(z)\big]^2_{z=0}}{d_{n-1}\big[\partial^{n-1} F_{n-1}(z)\big]^2_{z=0}} = n\alpha(1+(n-1)\gamma)$$

$$\lambda_n = \Big[\frac{\partial^{n+1}F_n(z)}{\partial^n F_n(z)} - \frac{\partial^n F_{n-1}(z)}{\partial^{n-1}F_{n-1}(z)}\Big]_{z=0} = \frac{1}{n!\alpha^n}\Big[\partial^{n+1}F_n(z) - n\alpha\partial^n F_{n-1}(z)\Big]_{z=0}.$$

Par la relation de récurrence établie dans la preuve du théorème 1, on obtient tout simplement $\lambda_n = G'(0) + n\beta$. L'autre cas est similaire. □

Remarque

Soit $\alpha \in \mathcal{F}(\mathbb{N}, \mathcal{A})$ une suite dont la fonction génératrice exponentielle (resp. ordinaire) vérifie les hypothèses du théorème 3 (resp. du théorème 4). On a alors de manière plus explicite $P_0(x) = \alpha_0 = 1$, $P_1(x) = x - \alpha_1$ et la relation de récurrence

$$P_{n+1}(x) = (x - \alpha_1 - n\beta)P_n(x) - n\alpha(1+(n-1)\gamma)P_{n-1}(x) \quad (\text{pour } n \geqslant 1)$$

dans le "cas exponentiel" (car $G'(0) = F'(0) = \alpha_1$), respectivement

$$P_2(x) = (x-\beta)P_1(x) - \alpha P_0(x),$$

$$P_{n+1}(x) = (x-\beta)P_n(x) - \alpha\gamma P_{n-1}(x) \quad (\text{pour } n \geqslant 2)$$

dans le "cas ordinaire". (On ne confondra pas le coefficient α avec la désignation générique de la suite $(\alpha_n)_{n\geqslant 0}$ ou avec l'un de ses éléments α_n ...)

Exemples

1. Considérons l'application linéaire $\Phi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}[x]$ qui envoie le polynôme de Pochhammer $(x)_n = x(x-1)\cdots(x-(n-1))$ sur x^n et définissons les polynômes de Bell par $B_n(x) = \Phi(x^n)$. Soit $a > 0$ un entier positif. Nous avons vu que les déterminants de Hankel associés à la suite $(B_n(a))_{n\geqslant 0}$ sont tous positifs, de sorte que cette suite engendre un produit scalaire $(f \mid g)_a = \Phi_a(fg) := \Phi(fg)\big|_{x=a}$ sur $\mathbb{Z}[x]$. Les polynômes unitaires définis récursivement par $P_{a,0}(x) = 1$, $P_{a,1}(x) = x - a$ et la relation

$$P_{a,n+1}(x) = (x - a - n)P_{a,n}(x) - naP_{a,n-1}(x) \quad (n \geqslant 1)$$

en constituent un système orthogonal dans $\mathbb{Z}[x]$ (utiliser le théorème 5 avec $\alpha = a$, $\beta = 1$ et $\gamma = 0$). Ces polynômes, appelés *polynômes de Charlier* sont

$$P_{a,n}(x) = \Phi^{-1}((x-a)^n) = \sum_{k=0}^{n} \binom{n}{k}(-a)^{n-k}(x)_k$$

On peut revoir le paragraphe 4 de la deuxième partie pour se raffraîchir la mémoire.

2. Les nombres d'Euler, définis par la fonction génératrice exponentielle $F(z) = 1/\cos z$, fournissent également un produit scalaire sur $\mathbb{Z}[x]$ et les polynômes unitaires

$$Q_0(x) = 1,\ Q_1(x) = x \ \text{ et } \ Q_{n+1}(x) = xQ_n(x) - n^2Q_{n-1}(x) \quad (n \geqslant 1),$$

appelés *polynômes de Meixner*, constituent une famille orthogonale dans $\mathbb{Z}[x]$ (utiliser le dernier théorème avec $\alpha = \gamma = 1$ et $\beta = 0$).

3. Les polynômes unitaires qui forment un système orthogonal pour le produit scalaire associé à la suite $n! = [n!x^n]_{x=1}$ sont donnés par $L_0(x) = 1$, $L_1(x) = x - 1$ et

$$L_{n+1}(x) = (x - (2n+1))L_n(x) - n^2L_{n-1}(x) \quad (n \geqslant 1)$$

(prendre $\alpha = \gamma = 1$ et $\beta = 2$ dans le dernier théorème). Ce sont les *polynômes normalisés de Laguerre*

$$L_n(x) = \sum_{k=0}^{n} \binom{n}{k} (n)_k (-1)^k x^{n-k}.$$

4. Si une suite $\alpha \in \mathcal{F}(\mathbb{N}, \mathcal{A})$ engendre un produit scalaire, alors il en est de même pour $T^a\alpha \in \mathcal{F}(\mathbb{N}, \mathcal{A})$ car les déterminants de Hankel associés aux deux suites coïncident. On peut relier les bases orthogonales respectives de la manière suivante.

Proposition 6. *Si une base polynomiale $(P_n(x))_{n\geqslant 0}$ est orthogonale pour le produit scalaire issu de $\alpha \in \mathcal{F}(\mathbb{N}, \mathcal{A})$, alors la famille $(P_n(x-a))_{n\geqslant 0}$ est une base orthogonale pour le produit scalaire issu de $T^a\alpha \in \mathcal{F}(\mathbb{N}, \mathcal{A})$.*

PREUVE. Notons H_n (resp. $H_{a,n}$) les matrices de Hankel (d'ordre n) asssociées à la suite α (resp. $T^a\alpha$) et considérons la matrice $P = (p_{i,j})_{0\leqslant i,j\leqslant n}$ dont la m-ième ligne est formée avec les coefficients de $P_m(x) = p_{m,0} + p_{m,1}x + \cdots + p_{m,m}x^m$. Par construction, la matrice $D = PH_nP^t$ est diagonale et en reprenant les notations de la proposition 1, on a

$$D = PH_nP^t = PS_n(a)^{-1}H_{a,n}(S_n(a)^{-1})^tP^t = (PS_n(-a))H_{a,n}(PS_n(-a))^t.$$

La matrice $PS_n(-a)$ est donc formée avec les coefficients d'une base polynomiale orthogonale associée au produit scalaire issu de $T^a\alpha$. Ces polynômes sont donnés (pour $m \leqslant n$) par

$$\widehat{P}_m(x) = \sum_{l=0}^{n} (PS_n(-a))_{m,l}x^l = \sum_{l=0}^{n} \left(\sum_{k=0}^{n} \binom{k}{l} (-a)^{k-l} p_{m,k} \right) x^l.$$

En échangeant les deux sommes, il vient

$$\widehat{P}_m(x) = \sum_{k=0}^{n} p_{m,k} \sum_{l=0}^{n} \binom{k}{l} (-a)^{k-l}x^l = \sum_{k=0}^{n} p_{m,k}(x-a)^k = P_m(x-a)$$

et la proposition est ainsi démontrée. □

3.5 Congruences

Lorsque $\mathcal{A}$ est un anneau unitaire commutatif et intègre, nous pouvons généraliser l'existence d'un produit scalaire supposé dans le paragraphe précédent au travers d'un système orthogonal de polynômes unitaires. On dira donc qu'une application $\mathcal{A}$-linéaire

$$\Phi : \mathcal{A}[x] \longrightarrow \mathcal{A},\ x^n \longmapsto \alpha_n$$

est un *produit scalaire généralisé* lorsqu'il existe dans $\mathcal{A}[x]$ des polynômes unitaires $P_n(x)$ ($n \geqslant 0$) avec $\deg P_n(x) = n$, tels que

$$\Phi(P_n(x)P_m(x)) = 0 \quad \text{chaque fois que } m \neq n.$$

La famille $(P_n(x))_{n\geqslant 0}$ est alors appelée *système orthogonal (généralisé) associé.* Tous les produits scalaires qui entrent dans le contexte du paragraphe précédent ($\mathcal{A} \subset \mathbb{R}$) sont des produits scalaires généralisés.

Fixons un entier $m \geqslant 0$. Comme les polynômes $P_n(x)$ sont unitaires, on peut alors trouver une décomposition

$$x^m = \sum_{k=0}^{m} \left\langle {m \atop k} \right\rangle P_k(x) \quad \text{avec} \quad \left\langle {m \atop k} \right\rangle \in \mathcal{A}$$

(on a évidemment $\left\langle {m \atop m} \right\rangle = 1$ et on peut poser $\left\langle {m \atop k} \right\rangle = 0$ si $k > m$). Cela montre que

$$\Phi(x^m P_n(x)) = \sum_{k=0}^{m} \left\langle {m \atop k} \right\rangle \Phi(P_k(x)P_n(x)) = \left\langle {m \atop n} \right\rangle \Phi(P_n(x)^2)$$

et par linéarité, on obtient

Proposition 7. *Un système orthogonal $(P_n(x))_{n\geqslant 0}$ associé à un produit scalaire généralisé Φ fournit des congruences pour la "suite des moments" $\alpha_n = \Phi(x^n)$: on a*

$$\Phi(f(x)P_n(x)) \equiv 0 \bmod \Phi(P_n(x)^2)\mathcal{A}$$

pour tout polynôme $f(x) \in \mathcal{A}[x]$.

Remarque

Lorsque $\mathcal{A}$ est un sous-anneau de $\mathbb{R}$ et les déterminants de Hankel vérifient la condition du théorème 5, l'application Φ engendre un produit scalaire (ordinaire) qui admet une base orthogonale de polynômes unitaires $P_n(x)$ dans $\mathcal{A}[x]$. On a alors

$$\Phi(x^m P_n(x)) = \frac{1}{\det H_{n-1}} \begin{vmatrix} \alpha_0 & \cdots & \alpha_{n-1} & \alpha_m \\ \alpha_1 & \cdots & \alpha_n & \alpha_{m+1} \\ \vdots & & \vdots & \vdots \\ \alpha_n & \cdots & \alpha_{2n-1} & \alpha_{m+n} \end{vmatrix}$$

et $\Phi(P_n(x)^2) = \|P_n(x)\|^2 = \Phi(x^n P_n(x)) = \det H_n / \det H_{n-1}$ (pour $n \geqslant 1$).

3.5.1 Polynômes de Bell

Nous avons vu que pour tout entier $a > 0$, l'application linéaire

$$\Phi_a : \mathbb{Z}[x] \longrightarrow \mathbb{Z},\ x^n \longmapsto B_n(a)$$

engendre un produit scalaire sur $\mathbb{Z}[x]$ pour lequel un système orthogonal est donné par les polynômes (unitaires) de Charlier

$$P_{a,n}(x) = \Phi^{-1}((x-a)^n) = \sum_{k=0}^{n} \binom{n}{k}(-a)^{n-k}(x)_k$$

où $\Phi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}[x], x^n \longmapsto B_n(x)$. Pour tout $n \geqslant 1$, la proposition fournit une congruence modulo $n!a^n$. Par exemple, les nombres de Bell ($a = 1$) vérifient

$$\begin{aligned}
n = 2 \quad &: \quad B_{m+2} \equiv B_m + B_{m+1} \bmod 2 \\
n = 3 \quad &: \quad B_{m+3} \equiv B_m + 4B_{m+1} \bmod 6 \\
n = 4 \quad &: \quad B_{m+4} \equiv 23B_m + 19B_{m+2} + 10B_{m+3} \bmod 24 \\
n = 5 \quad &: \quad B_{m+5} \equiv B_m + 31B_{m+1} + 25B_{m+2} + 45B_{m+3} + 15B_{m+4} \bmod 120
\end{aligned}$$

Pour généraliser, on peut remplacer les entiers $a > 0$ par une variable z et considérer pour $\mathcal{A} = \mathbb{Z}[z]$ l'application $\mathcal{A}$-linéaire $\Phi_z : \mathcal{A}[x] \longrightarrow \mathcal{A},\ x^n \longmapsto B_n(z)$. Les polynômes $P_{z,n}(x) \in \mathcal{A}[x]$ sont unitaires et pour $m \neq n$, le polynôme $\Phi_z(P_{z,n}(x)P_{z,m}(x))$ (dans $\mathbb{Z}[z]$) est identiquement nul puisqu'il s'annule pour tout entier $z = a > 0$. Ainsi la famille $(P_{z,n}(x))_{n\geqslant 0}$ est un système orthogonal et Φ_z est un produit scalaire généralisé (voir §2.4). Nous allons donc pouvoir établir des congruences pour les polynômes de Bell.

Etant donné un nombre premier p quelconque, on peut plonger la situation dans l'anneau $\mathbb{Z}_p$ des entiers p-adiques et considérer $\mathcal{A} = \mathbb{Z}_p[z]$ au lieu de $\mathbb{Z}[z]$ dans ce qui précède. En rappelant que

$$\binom{np}{kp} \equiv \binom{n}{k} \bmod np\mathbb{Z}_p \ \text{ et } \ \binom{np}{k} \equiv 0 \bmod np\mathbb{Z}_p \ \text{ si } p \nmid k$$

d'une part (la relation $(x+1)^{np} \equiv (x^p+1)^n \bmod np\mathbb{Z}_p[x]$ découle du TAF (voir §1.2) ou directement du fait qu'elle est valable pour $n = 1$ (avec la proposition 1 de §2.2)) et que

$$(x)_{kp} \equiv (x^p - x)^k \bmod \frac{kp}{2}\mathbb{Z}_p[x]$$

(voir §2.6, proposition 3) d'autre part, on peut écrire modulo $(np/2)\mathbb{Z}_p[z][x]$

$$P_{z,np}(x) = \sum_{k=0}^{np} \binom{np}{k}(-z)^{np-k}(x)_k \equiv \sum_{k=0}^{n} \binom{n}{k}(-z^p)^{n-k}(x)_{kp} \equiv (x^p - x - z^p)^n.$$

Pour tout entier $n \geqslant 0$ et tout polynôme $f(x) \in \mathbb{Z}_p[x]$, on a donc

$$\Phi_z((x^p - x - z^p)^n f(x)) \equiv \Phi_z(P_{z,np}(x) f(x)) \equiv 0 \bmod \frac{np}{2}\mathbb{Z}_p[z]$$

(la première congruence a lieu modulo $(np/2)\mathbb{Z}_p[z]$ alors que la deuxième est valable modulo $(np)!z^{np}\mathbb{Z}_p[z]$). Ceci nous permet d'établir (toujours modulo $(np/2)\mathbb{Z}_p[z]$)

$$\Phi_z(x^{np} f(x)) = \Phi_z\left(\sum_{k=0}^{n} \binom{n}{k} (x^p - x - z^p)^k (x + z^p)^{n-k} f(x)\right) \equiv \Phi_z((x + z^p)^n f(x)).$$

Par induction, nous retrouvons alors la congruence générale de §2.7 :

$$\begin{aligned} \Phi_z(x^{np^\nu} f(x)) &\equiv \Phi_z((x + z^p)^{np^{\nu-1}} f(x)) \equiv \Phi_z((x + z^p + z^{p^2})^{np^{\nu-2}} f(x)) \\ &\equiv \cdots \equiv \Phi_z((x + z^p + z^{p^2} + \cdots + z^{p^\nu})^n f(x)) \bmod \frac{np}{2}\mathbb{Z}_p[z]. \end{aligned}$$

Remarque

En appliquant l'opérateur Φ^{-1} à la relation

$$B_m(x) = \sum_{l=0}^{m} \left\{ {m \atop l} \right\} x^l = \sum_{l=0}^{m} \left\{ {m \atop l} \right\} \sum_{k=0}^{l} \binom{l}{k} (x - z)^k z^{l-k}$$

et en échangeant les deux sommes, on obtient

$$x^m = \sum_{k=0}^{m} \left\langle {m \atop k} \right\rangle P_{z,k}(x) \quad \text{avec} \quad \left\langle {m \atop k} \right\rangle = \sum_{l=k}^{m} \left\{ {m \atop l} \right\} \binom{l}{k} z^{l-k}$$

3.5.2 Nombres d'Euler

Les nombres d'Euler (avec série de Hurwitz $F(z) = 1/\cos z$) engendrent un produit scalaire sur $\mathbb{Z}[x]$ pour lequel une base orthogonale est donnée par les polynômes de Meixner

$$Q_0(x) = 1,\ Q_1(x) = x \ \text{ et } \ Q_{n+1}(x) = xQ_n(x) - n^2 Q_{n-1}(x) \quad (n \geqslant 1).$$

Pour chaque entier $n \geqslant 1$, ils permettent de trouver une congruence modulo $(n!)^2$:

$$\begin{aligned} n = 2 &: E_{m+2} \equiv E_m \bmod 4 \\ n = 3 &: E_{m+3} \equiv 5E_{m+1} \bmod 36 \\ n = 4 &: E_{m+4} \equiv 14E_{m+2} - 9E_m \bmod 576 \\ n = 5 &: E_{m+5} \equiv 30E_{m+3} - 89E_{m+1} \bmod 14400 \end{aligned}$$

Comme les nombres d'indices impairs sont nuls, les congruences intéressantes sont celles où m et n ont même parité. En travaillant avec $\widetilde{E}_n = E_{2n}$, on obtiendrait par exemple

$$\begin{aligned} n=2 \quad &: \quad \widetilde{E}_{m+1} \equiv \widetilde{E}_m \equiv \cdots \equiv \widetilde{E}_0 = 1 \bmod 4 \\ n=3 \quad &: \quad \widetilde{E}_{m+2} \equiv 5\widetilde{E}_{m+1} \equiv \cdots \equiv 5^m \widetilde{E}_2 = 5^{m+1} \bmod 36 \\ n=5 \quad &: \quad \widetilde{E}_{m+3} \equiv \widetilde{E}_{m+1} \equiv \cdots \equiv \begin{cases} \widetilde{E}_1 = 1 & \text{si } m \text{ est pair} \\ \widetilde{E}_2 = 5 & \text{sinon} \end{cases} \bmod 30 \end{aligned}$$

Pour établir des congruences pour les nombres d'Euler E_n (ou $\widetilde{E}_n$), il nous faut tout d'abord en trouver pour les polynômes de Meixner.

Proposition 8. *Pour tout nombre premier $p \neq 2$, nous avons la congruence polynomiale*

$$Q_p(x) \equiv x^p - (-1)^{(p-1)/2} x \bmod p\mathbb{Z}_p[x].$$

PREUVE. Nous pouvons expliciter $Q_n(x) = \big[\partial^n \big((1+z^2)^{-1/2} \exp(x \arctan z)\big)\big]_{z=0}$ où ∂ est l'opérateur de dérivation par rapport à z. Une première astuce consiste à remarquer que $g(z) = (1+z^2)^{1/2}$ est un élément de $\mathbb{Z}_p[[z^2]]$ qui vérifie

$$\big[\partial^{2m} g(z)\big]_{z=0} = \binom{1/2}{m} (2m)! = \frac{1}{2}\Big(\frac{1}{2} - 1\Big) \cdots \Big(\frac{1}{2} - (m-1)\Big) \frac{(2m)!}{m!}.$$

Ainsi, puisque p est impair, on a $\big[\partial^k g(z)\big]_{z=0} \in k\mathbb{Z}_p$ pour tout $k \geqslant 0$. On en déduit que

$$\big[\partial^{np} \exp(x \arctan z)\big]_{z=0} = \sum_{k=0}^{np} \binom{np}{k} \big[\partial^k g(z)\big]_{z=0} Q_{np-k}(x)$$

est congru, modulo $np\mathbb{Z}_p[x]$, à $\displaystyle\sum_{k=0}^{n} \binom{n}{k} \big[\partial^{kp} g(z)\big]_{z=0} Q_{(n-k)p}(x) \equiv Q_{np}(x)$.

Pour le problème qui nous intéresse, nous pouvons donc remplacer les polynômes $Q_n(x)$ par $\widehat{Q}_n(x) = \big[\partial^n \exp(x \arctan z)\big]_{z=0}$. Cette nouvelle suite, qui a été étudiée notamment par L. Carlitz, peut être définie recursivement par

$$\widehat{Q}_0(x) = 1, \ \widehat{Q}_1(x) = x \ \text{ et } \ \widehat{Q}_{n+1}(x) = x\widehat{Q}_n(x) - n(n-1)\widehat{Q}_{n-1}(x) \quad (n \geqslant 1).$$

La *formule de Faà di Bruno* [14] affirme que si f et g sont des fonctions possèdant un nombre suffisant de dérivées, alors

$$\partial^n g(f(z)) = \sum{}' \frac{n!}{m_1! m_2! \cdots m_n!} \, g^{(m_1+\cdots+m_n)}(f(z)) \, \Big(\frac{f'(z)}{1!}\Big)^{m_1} \Big(\frac{f''(z)}{2!}\Big)^{m_2} \cdots \Big(\frac{f^{(n)}(z)}{n!}\Big)^{m_n}$$

où $\sum'$ indique que la somme porte sur tous les n-uplets $(m_1, m_2, ..., m_n) \in \mathbb{N}^n$ vérifiant $m_1 + 2m_2 + \cdots + nm_n = n$.

En particulier, pour $n = p$ premier et $f(z) = \sum_{n\geqslant 1} a_n \frac{z^n}{n}$, on obtient

$$[\partial^p \exp(f(z))]_{z=0} = \sum{}' \frac{p!}{m_1!m_2!\cdots m_p!}\Big(\frac{a_1}{1}\Big)^{m_1}\Big(\frac{a_2}{2}\Big)^{m_2}\cdots\Big(\frac{a_p}{p}\Big)^{m_p}.$$

On remarque que si un anneau $\mathcal{A}$ contient les coefficients $a_1, \dots, a_p$, alors la somme ci-dessus est congrue à $a_1^p - a_p$ modulo $p\mathcal{A}$. La proposition provient alors simplement du fait que pour $f(z) = x \arctan z$, on a $a_{2k} = 0$ et $a_{2k+1} = (-1)^k x$ $(k \geqslant 0)$ dans $\mathcal{A} = \mathbb{Z}_p[x]$.

Cette remarque permet également de retrouver la congruence $B_p(x) \equiv x^p + x \bmod p\mathbb{Z}_p[x]$ pour les polynômes de Bell définis par la série de Hurwitz $F(z) = \exp(x(e^z - 1))$: les éléments $a_k = x/(k-1)!$ sont dans $\mathbb{Z}_p[x]$ pour tout $k = 1, \dots, p$. □

De nombreux essais numériques laissent à penser que la proposition peut être généralisée :

Conjecture. $Q_{np}(x) \equiv Q_p^n(x) \equiv (x^p - (-1)^{(p-1)/2}x)^n \bmod np\mathbb{Z}_p[x]$ *(pour $p \neq 2$).*

Cette conjecture impliquerait alors

$$E_{m+np} \equiv (-1)^{n(p-1)/2} E_{m+n} \bmod np\mathbb{Z}_p \quad \text{et} \quad \widetilde{E}_{m+np} \equiv \widetilde{E}_{m+n} \bmod np\mathbb{Z}_p.$$

En effet, si on pose $s = (-1)^{(p-1)/2}$ et on considère l'opérateur linéaire $\Phi : x^n \longmapsto E_n$, on voit que la différence

$$E_{m+np} - s^n E_{m+n} = \Phi\Big(x^m\big(x^{np} - (sx)^n\big)\Big) = \Phi\Big(x^m \sum_{k=1}^{n} \binom{n}{k} (sx)^{n-k}(x^p - sx)^k\Big)$$

serait congrue modulo $np\mathbb{Z}_p$, à $\displaystyle\sum_{k=1}^{n}\binom{n}{k}\Phi\Big(x^m(sx)^{n-k}Q_{kp}(x)\Big)$, mais cette somme est nulle (modulo $np\mathbb{Z}_p$) par la proposition 7. La preuve (ou une réfutation) de la conjecture est laissée en suspens mais quoi qu'il en soit, la proposition 8 montre qu'elle est valable (de même que les congruences dérivées ci-dessus) pour $n = 1$.

Remarque

Certaines congruences peuvent être obtenues directement à l'aide des déterminants de Hankel, sans avoir recours à un système orthogonal. Cela a été le cas pour la congruence de Radoux (§2.11) et dans le même ordre d'idée, pour p premier, on a (modulo $p\mathbb{Z}$)

$$\Big(\prod_{k=0}^{p-1} k!\Big)^2 = \begin{vmatrix} 0! & 1! & \cdots & (p-1)! \\ 1! & 2! & \cdots & p! \\ \vdots & \vdots & & \vdots \\ (p-1)! & p! & \cdots & (2(p-1))! \end{vmatrix} \equiv \begin{vmatrix} 0! & 1! & \cdots & (p-1)! \\ 1! & & \iddots & 0 \\ \vdots & \iddots & \iddots & \vdots \\ (p-1)! & 0 & \cdots & 0 \end{vmatrix}$$

donc $\Big(\prod_{k=0}^{p-1} k!\Big)^2 \equiv (-1)^{(p-1)p/2}((p-1)!)^p \equiv -(-1)^{(p-1)p/2} \bmod p\mathbb{Z}$.

3.6 Critère de rationalité

Les déterminants de Hankel sont fort utiles pour établir certaines congruences mais leur importance ne s'arrête pas là, ils fournissent également un critère de rationalité très élégant [2], dont nous nous permettons de rappeler l'énoncé ainsi que la preuve.

Théorème 9. *Soit $(a_n)_{n\geqslant 0}$ une suite dans un anneau commutatif unitaire intègre $\mathcal{A}$ et notons*

$$H_n^{[k]} = \begin{pmatrix} a_k & a_{k+1} & \cdots & a_{k+n} \\ a_{k+1} & a_{k+2} & \cdots & a_{k+n+1} \\ \vdots & \vdots & & \vdots \\ a_{k+n} & a_{k+n+1} & \cdots & a_{k+2n} \end{pmatrix} \qquad (k, n \in \mathbb{N})$$

le déterminant de Hankel d'ordre n associé à la sous-suite $(a_{k+n})_{n\geqslant 0}$. Alors les assertions suivantes sont équivalentes

1. *la série formelle $f(X) = \sum_{n\geqslant 0} a_n X^n \in \mathcal{A}[[X]]$ décrit une fonction rationnelle,*
2. *il existe deux entiers N et K tels que $\det H_N^{[k]} = 0$ pour tout $k \geqslant K$,*
3. *il existe un entier N tel que $\det H_n = 0$ pour tout $n \geqslant N$.*

PREUVE. Notons que comme $\mathcal{A}$ est commutatif unitaire et intègre, il en est de même pour $\mathcal{A}[X]$ et ces anneaux admettent chacun un corps des fractions. Nous pouvons ainsi plonger $\mathcal{A}$ dans $\operatorname{Frac}\mathcal{A}$ et la première assertion a bien un sens dans $\operatorname{Frac}\mathcal{A}[X]$.

1) $\Longrightarrow$ 3) Supposons que $f(X) = P(X)/Q(X)$ soit une fonction rationnelle et écrivons $Q(X) = q_0 + q_1 X + \cdots + q_k X^k \in \mathcal{A}[X]$ avec $q_k \neq 0$ (i.e. $k = \deg Q$). Pour tout entier $n > \max(\deg P, \deg Q)$, le coefficient devant X^n dans la relation $Q(X)f(X) = P(X)$ est $\sum_{i=0}^{k} q_i a_{n-i} = 0$. Vectoriellement, on obtient la dépendance linéaire

$$q_0 \begin{pmatrix} a_n \\ a_{n+1} \\ \vdots \\ a_{2n} \end{pmatrix} + q_1 \begin{pmatrix} a_{n-1} \\ a_n \\ \vdots \\ a_{2n-1} \end{pmatrix} + \cdots + q_k \begin{pmatrix} a_{n-k} \\ a_{n+1-k} \\ \vdots \\ a_{2n-k} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

et donc $\det H_n = 0$ (pour tout n comme ci-dessus).

3) $\Longrightarrow$ 2) On montre que si $\det H_n = 0$ pour tout $n \geqslant N$, alors $\det H_n^{[k]} = 0$ pour tout $n \geqslant N$ et tout $k \geqslant 0$. Ceci découle par induction sur $k \geqslant 0$ de l'implication

$$\det H_n^{[k]} = \det H_{n+1}^{[k]} = 0 \implies \det H_n^{[k+1]} = 0.$$

En effet, si $\det H_n^{[k]}$ est nul, on a une dépendance linéaire non triviale entre les colonnes de $H_n^{[k]}$, disons $\alpha_0 C_k + \alpha_1 C_{k+1} + \cdots + \alpha_n C_{k+n} = 0$. Si $\alpha_0 = 0$, on a une dépendance

linéaire $\alpha_1 C_{k+1} + \cdots + \alpha_n C_{k+n} = 0$ entre les colonnes de $H_n^{[k+1]}$ et donc $\det H_n^{[k+1]} = 0$. Dans le cas contraire, on peut remplacer dans la matrice $H_{n+1}^{[k]}$ la première colonne C'_k par $C'_k - (\alpha_1 C'_{k+1} + \cdots + \alpha_n C'_{k+n})/\alpha_0$:

$$H_{n+1}^{[k]} \sim \begin{pmatrix} 0 & a_{k+1} & \cdots & \cdots & a_{k+n} & a_{k+n+1} \\ 0 & a_{k+2} & \cdots & \cdots & a_{k+n+1} & a_{k+n+2} \\ \vdots & \vdots & & & \vdots & \vdots \\ 0 & a_{k+n+1} & \cdots & \cdots & a_{k+2n} & a_{k+2n+1} \\ \beta & a_{k+n+2} & \cdots & \cdots & a_{k+2n+1} & a_{k+2n+2} \end{pmatrix}$$

Cette transformation ne change pas le déterminant : $\det H_{n+1}^{[k]} = \beta \cdot \det H_n^{[k+1]}$ est nul (par hypothèse). On en déduit que $\det H_n^{[k+1]} = 0$ ou $\beta = 0$ mais ce deuxième cas implique le premier puisque la sous-matrice de taille $n \times n$ située en bas à gauche a le même déterminant que $H_n^{[k+1]}$ (en d'autres termes, on a $\det H_n^{[k+1]} = \beta \cdot \det H_{n-1}^{[k+2]}$).

2) $\Longrightarrow$ 1) Supposons que l'ensemble

$$\{n \in \mathbb{N} \ : \ \text{il existe } K \text{ tel que } \det H_n^{[k]} = 0 \text{ pour tout } k \geqslant K\}$$

soit non vide et considérons son élément minimal $N \in \mathbb{N}$. Le cas d'une suite $(a_n)_{n \geqslant 0}$ nulle à partir d'un certain rang étant trivial ($f(X)$ est simplement un polynôme), on peut supposer que $N \geqslant 1$. On remarque alors que, pour un entier fixé $k \geqslant K$, la matrice $H_N^{[k]}$ est de rang N car $\det H_{N-1}^{[k]}$ est non nul : dans le cas contraire, le résultat ci-dessus montrerait que $\det H_{N-1}^{[k+1]} = 0$ pour tout $k \in K$, contredisant la minimalité de N. L'équation $H_N^{[k]} Y = 0$ admet ainsi une solution (unique à multiple près) $Y = {}^t(y_0 \ \ldots \ y_{N-1} \ y_N) \in \mathcal{A}^{N+1}$ avec $y_N \neq 0$. Toute solution correspondant à $k = K$ correspond alors à tout entier $k \geqslant K$: comme la dernière ligne de $H_N^{[k+1]}$ est une combinaison linéaire des lignes précédentes, la condition $H_N^{[k]} Y = 0$ implique $H_N^{[k+1]} Y = 0$. On a ainsi

$$a_k y_0 + a_{k+1} y_1 + \cdots + a_{k+N} y_N = 0 \ \text{ pour tout } k \geqslant K$$

et $(y_N + y_{N-1} X + \cdots + y_1 X^{N-1} + y_0 X^N) f(X)$ est un polynôme de degré $< N + K$ puisque pour $k \geqslant K$, le coefficient devant x^{N+k} dans ce produit est $\sum_{i=0}^{N} y_i a_{k+i} = 0$. $\square$

Remarque

L'implication 3) $\Longrightarrow$ 2) s'obtient également avec l'*identité de Sylvester* [2]. Elle se traduit pour les matrices considérées ici par la relation

$$\big(\det H_n^{[k+1]}\big)^2 = \big(\det H_n^{[k+2]}\big)\big(\det H_n^{[k]}\big) - \big(\det H_{n+1}^{[k]}\big)\big(\det H_{n-1}^{[k+2]}\big),$$

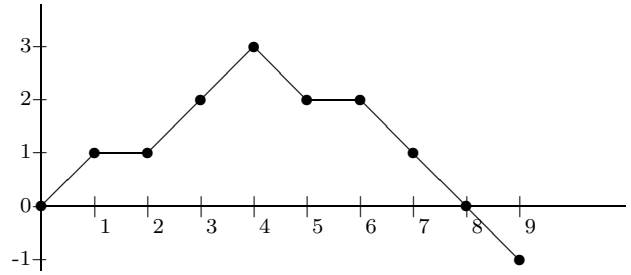
que l'on peut prolonger lorsque $n = 0$ en posant $\det H_{-1}^{[k]} = 1$.

3.7 Chaînes à accroissements pondérés

Dans ce paragraphe, nous donnons une interprétation combinatoire des coefficients α, β et γ qui interviennent dans les théorèmes 3 et 4, fournissant par la même occasion une certaine interprétation des suites rencontrées. Notre point de départ est la *combinatoire des chemins* [11].

Soit $n \geqslant 0$ un entier positif. On appelle *n-chaîne* la donnée de $n+1$ entiers $\sigma_0, \ldots, \sigma_n$ tels que les *accroissements* $\delta_k = \sigma_{k+1} - \sigma_k$ $(k = 0, \ldots, n-1)$ prennent leurs valeurs dans $\{-1, 0, 1\}$ et on note $\sigma = (\sigma_0 \to \sigma_1 \to \cdots \to \sigma_n)$. Une 1-chaîne est également appelée *maillon*. On peut visualiser σ par un chemin dans $\mathbb{N} \times \mathbb{Z}$ en reliant les points (k, σ_k) :

$$\sigma = (0 \to 1 \to 1 \to 2 \to 3 \to 2 \to 2 \to 1 \to 0 \to -1)$$



On compose deux chaînes $\mu = (\mu_0 \to \cdots \to \mu_m)$ et $\sigma = (\sigma_0 \to \cdots \to \sigma_n)$ en translatant la deuxième de manière à ce qu'elle puisse prolonger la première :

$$\sigma\mu = (\mu_0 \to \cdots \to \mu_{m-1} \to \mu_m \to \sigma_1 - \sigma_0 + \mu_m \to \cdots \to \sigma_n - \sigma_0 + \mu_m).$$

L'ensemble des chaînes (de longueur quelconque) est un monoïde $\mathcal{C}$ non commutatif et la fonction qui associe à une chaîne sa longueur est un homomorphisme de monoïdes $\mathcal{C} \longrightarrow \mathbb{N}$: la composition d'une m-chaîne avec une n-chaîne est une $(m+n)$-chaîne. Une 0-chaîne est un élément neutre pour la composition et une n-chaîne est simplement la composition de n maillons. On peut munir $\mathcal{C}$ d'une relation d'équivalence de manière naturelle : on dit que deux chaînes μ et σ sont *équivalentes* (et on note $\mu \sim \sigma$) si elles ont la même longueur et si les différences $\sigma_k - \mu_k$ sont indépendantes de k. La composition s'étend évidemment sur le monoïde quotient $\mathcal{C}/\!\sim$ avec la propriété d'être simplifiable :

$$\text{si } [\,\sigma_1\mu\,] = [\,\sigma_2\mu\,] \text{ ou } [\,\mu\sigma_1\,] = [\,\mu\sigma_2\,], \text{ alors } [\,\sigma_1\,] = [\,\sigma_2\,].$$

De plus, la fonction longueur reste un homomorphisme bien défini $(\mathcal{C}/\!\sim) \longrightarrow \mathbb{N}$.

On dit qu'une n-chaîne est *à accroissements pondérés* lorsque l'on fait correspondre à chaque $k = 0, 1, \ldots, n-1$ un entier $w_k \geqslant 1$. On note alors $\sigma = (\sigma_0 \xrightarrow{w_0} \sigma_1 \xrightarrow{w_1} \cdots \xrightarrow{w_{n-1}} \sigma_n)$.

On dira encore que ces accroissements sont *majorés par une fonction* $\psi : \mathbb{Z} \longrightarrow \mathbb{N}$ lorsque les poids $w_1, \ldots, w_{n-1}$ considérés vérifient $1 \leqslant w_k \leqslant \psi(\sigma_k)$. Cette fonction ψ peut dépendre

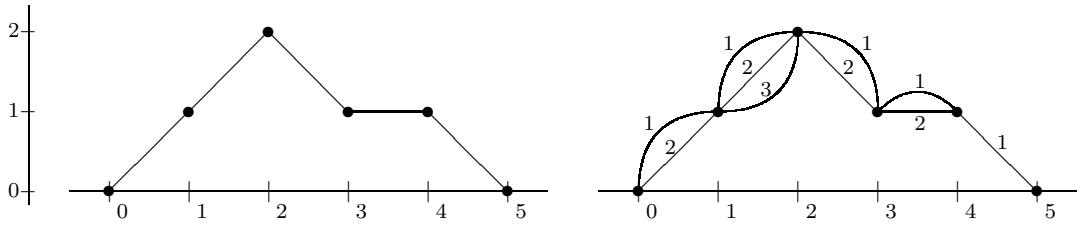
du type de l'accroissement, elle est alors définie par trois applications $\psi_-, \psi_0, \psi_+ : \mathbb{Z} \longrightarrow \mathbb{N}$ de la manière suivante :

$$\psi(\sigma_k) = \begin{cases} \psi_-(\sigma_k) & \text{si } \delta_k = -1 \\ \psi_0(\sigma_k) & \text{si } \delta_k = 0 \\ \psi_+(\sigma_k) & \text{si } \delta_k = +1 \end{cases}$$

(pour être un peu plus formel, on peut voir ψ comme application $\mathbb{Z} \times \{-1, 0, +1\} \longrightarrow \mathbb{N}$).

Notons $E_{i,j}^{[n]}(\psi)$ l'ensemble des n-chaînes $\sigma = (\sigma_0 \xrightarrow{w_0} \sigma_1 \xrightarrow{w_1} \cdots \xrightarrow{w_{n-1}} \sigma_n)$ d'extrêmités $\sigma_0 = i$, $\sigma_n = j$, avec $\sigma_k \geqslant \min\{i, j\}$ pour tout k et dont les accroissements sont majorés par $\psi = \{\psi_-, \psi_0, \psi_+\}$. Nous nous proposons de calculer les déterminants de Hankel associés à la suite $N_{i,j}^{[n]}(\psi) = \#E_{i,j}^{[n]}(\psi)$ pour certains entiers i et j fixés.

Illustration : on considère une chaîne dans $E_{i,j}^{[n]}(\psi)$ en ignorant d'abord les pondérations puis on complète en ajoutant à chaque altitude autant de maillons que la fonction ψ le permet (quitte à exclure simplement la chaîne initiale lorsque la fonction ψ est nulle à une certaine altitude). Chaque choix de parcours fournit alors une chaîne à accroissements majorés par ψ. Dans l'exemple qui suit, nous complétons $\sigma = (0 \to 1 \to 2 \to 1 \to 1 \to 0)$ dans $E_{0,0}^{[5]}(\psi_-(k) = k,\ \psi_0(k) = k+1,\ \psi_+(k) = k+2)$, ce "squelette" donne lieu à $2 \cdot 3 \cdot 2 \cdot 2 = 24$ chaînes pondérées possibles selon la fonction de majoration ψ considérée :



Comme il faut considérer tous les "squelettes" possibles, nous voyons combien il est difficile d'identifier une suite $N_{i,j}^{[n]}(\psi)$ $(n \geqslant 0)$, mais nous allons donner une méthode permettant de le faire dans certains cas.

Nous pouvons déjà supposer que $i \leqslant j$ grâce à la relation

$$N_{i,j}^{[n]}(\psi_-(k),\ \psi_0(k),\ \psi_+(k)) = N_{j,i}^{[n]}(\psi_+(k-1),\ \psi_0(k),\ \psi_-(k+1))$$

et par translation, nous nous ramenons au cas où $i = 0$:

$$N_{i,j}^{[n]}(\psi_-(k),\ \psi_0(k),\ \psi_+(k)) = N_{0,j-i}^{[n]}(\psi_-(k+i),\ \psi_0(k+i),\ \psi_+(k+i)).$$

De manière générale, la composition de deux chaînes à accroissements majorés par ψ n'est permise que si elle s'effectue sans translation (c'est-à-dire lorsque la deuxième chaîne commence à l'altitude finalement atteinte par la première) afin qu'elle puisse respecter la fonction de majoration ψ. S'étant ramené au cas $i = 0$, il nous faut donc considérer également

$j = 0$. Les éléments de $E_{0,0}^{[n]} = E_{0,0}^{[n]}(\psi)$ sont parfois [30] appelés *chemins de Motzkin valués*, ou *chemin de Dyck* lorsque $\psi_0 = 0$, c'est-à-dire lorsque les chaînes considérées n'ont aucun accroissement nul.

Dans un premier temps, nous pouvons écrire

$$E_{0,0}^{[m+n]} = \coprod_{k\geqslant 0} E_{0,k}^{[m]} E_{k,0}^{[n]} \quad \text{donc} \quad N_{0,0}^{[m+n]} = \sum_{k\geqslant 0} N_{0,k}^{[m]} N_{k,0}^{[n]}.$$

La réunion disjointe et la somme sont finies puisqu'elles portent sur $k = 0, 1, \dots, \min(m, n)$. Pour de tels indices k, nous avons également les décompositions

$$E_{0,k}^{[m]} = \coprod_{M} E_{0,0}^{[m_0]}(0 \xrightarrow{*} 1) E_{1,1}^{[m_1]}(1 \xrightarrow{*} 2) \cdots (k-1 \xrightarrow{*} k) E_{k,k}^{[m_k]}$$

$$E_{k,0}^{[m]} = \coprod_{M} E_{k,k}^{[m_k]}(k \xrightarrow{*} k-1) E_{k-1,k-1}^{[m_{k-1}]}(k-1 \xrightarrow{*} k-2) \cdots (1 \xrightarrow{*} 0) E_{0,0}^{[m_0]}$$

où les réunions disjointes portent sur $M = \{(m_0, m_1, \dots, m_k) \in \mathbb{N}^{k+1} : \sum m_i = m - k\}$. En prenant le cardinal, il suit

$$N_{0,k}^{[m]} = \psi_+(0)\psi_+(1)\cdots\psi_+(k-1) \sum_{M} N_{0,0}^{[m_0]} N_{1,1}^{[m_1]} \cdots N_{k,k}^{[m_k]},$$

$$N_{k,0}^{[m]} = \psi_-(k)\psi_-(k-1)\cdots\psi_-(1) \sum_{M} N_{k,k}^{[m_k]} N_{k-1,k-1}^{[m_{k-1}]} \cdots N_{0,0}^{[m_0]}.$$

Si ψ_- est positive sur $\mathbb{N} \setminus \{0\}$, nous pouvons ainsi écrire

$$N_{0,0}^{[m+n]} = \sum_{k\geqslant 0} N_{0,k}^{[m]} N_{k,0}^{[n]} = N_{0,0}^{[m]} N_{0,0}^{[n]} + \sum_{k\geqslant 1} \frac{\psi_+(0)\psi_+(1)\cdots\psi_+(k-1)}{\psi_-(1)\psi_-(2)\cdots\psi_-(k)} N_{k,0}^{[m]} N_{k,0}^{[n]}.$$

On remarque encore que $N_{k,0}^{[n]} = 0$ si $k > n$ et que $N_{n,0}^{[n]} = \psi_-(n)\psi_-(n-1)\cdots\psi_-(1)$ (car $E_{n,0}^{[n]}$ ne contient que les chaînes $(n \xrightarrow{*} n-1 \xrightarrow{*} \cdots \xrightarrow{*} 0)$). On peut donc conclure comme dans la proposition 2 en considérant les éléments

$$d_k = \frac{\psi_+(0)\psi_+(1)\cdots\psi_+(k-1)}{\psi_-(1)\psi_-(2)\cdots\psi_-(k)} \quad (= 1 \text{ si } k = 0).$$

Théorème 10. *Les déterminants de Hankel associés aux entiers $N_{0,0}^{[n]}(\psi_-, \psi_0, \psi_+)$ sont*

$$\begin{aligned} \det H_n(\psi) &= \prod_{k=0}^{n} d_k \big[N_{k,0}^{[k]}\big]^2 = \prod_{k=0}^{n} \psi_+(0)\psi_+(1)\cdots\psi_+(k-1)\psi_-(1)\psi_-(2)\cdots\psi_-(k) \\ &= \big(\psi_+(0)\psi_-(1)\big)^n \big(\psi_+(1)\psi_-(2)\big)^{n-1} \cdots \big(\psi_+(n-1)\psi_-(n)\big)^1, \end{aligned}$$

et ne dépendent donc pas de la fonction ψ_0.

La dernière formulation rappelle que $\psi_+(k)$ et $\psi_-(k+1)$ vont toujours de pair : à un accroissement positif depuis une altitude k correspond forcément un accroissement négatif depuis l'altitude $k+1$. En fait, $\psi_+(k)\psi_-(k+1)$ décrit le nombre de "pics" que l'on peut choisir depuis l'altitude k selon la fonction de majoration ψ. Ces quantités sont très importantes et ne cesseront d'apparaître par la suite. Lorsqu'elles sont strictement positives (pour tout $k \geqslant 0$), tous les déterminants de Hankel le sont également, et l'application linéaire définie par $\Phi : x^n \longmapsto N_{0,0}^{[n]}(\psi_-, \psi_0, \psi_+)$ s'étend en un produit scalaire sur $\mathbb{Z}[x]$. Les polynômes unitaires orthogonaux associés vérifient une relation de récurrence (voir §3.4)

$$P_{n+1}(x) = (x - \lambda_n)P_n(x) - \mu_n P_{n-1}(x) \quad (n \geqslant 1)$$

avec $\mu_n = \|P_n(x)\|^2/\|P_{n-1}(x)\|^2$ et $\lambda_n = \big(N_{n,0}^{[n+1]}/N_{n,0}^{[n]}\big) - \big(N_{n-1,0}^{[n]}/N_{n-1,0}^{[n-1]}\big)$.

On remarque que $N_{n,0}^{[n+1]} = (\psi_0(n) + \psi_0(n-1) + \cdots + \psi_0(0))N_{n,0}^{[n]}$ car $E_{n,0}^{[n+1]}$ est constitué des chaînes qui admettent un accroissement négatif à chaque altitude $n, \ldots, 1$ et un seul accroissement constant à une altitude $n, \ldots, 0$. D'autre part, on a

$$\|P_n(x)\|^2 = \det H_n / \det H_{n-1} = \psi_+(0)\psi_+(1)\cdots\psi_+(n-1)\psi_-(1)\psi_-(2)\cdots\psi_-(n).$$

Tout ceci montre

Théorème 11. *Les polynômes unitaires orthogonaux associés à la suite $N_{0,0}^{[n]}(\psi_-, \psi_0, \psi_+)$ vérifient la relation de récurrence*

$$P_{n+1}(x) = (x - \psi_0(n))P_n(x) - \psi_+(n-1)\psi_-(n)P_{n-1}(x) \quad (n \geqslant 1)$$

avec les conditions initiales $P_0(x) = 1$ et $P_1(x) = x - N_{0,0}^{[1]} = x - \psi_0(0)$.

Le résultat suivant est le bienvenu pour comparer deux suites.

Proposition 12. *Des suites $(\alpha_n)_{n\geqslant 0}$ et $(\beta_n)_{n\geqslant 0}$ qui vérifient $\alpha_0 = \beta_0$ et qui engendrent un même système orthogonal de polynômes unitaires (dans le cas où elles engendrent des déterminants de Hankel strictement positifs) coïncident : $\alpha_n = \beta_n$ pour tout $n \geqslant 0$.*

PREUVE. Les applications linéaires définies sur la base canonique par $\Phi_1 : x^n \longmapsto \alpha_n$ et $\Phi_2 : x^n \longmapsto \beta_n$ peuvent s'étendre en un produit scalaire sur $\mathcal{A}[x]$ par $(f \mid g)_i = \Phi_i(f(x)g(x))$ $(i = 1, 2)$. Pour un entier $m \geqslant 0$ fixé, on peut décomposer $x^m = \sum \left\langle {m \atop k} \right\rangle P_k(x)$ où $(P_n(x))_{n\geqslant 0}$ est le système orthogonal commun à ces deux produits scalaires. On voit alors que

$$\Phi_i(x^m) = \sum \left\langle {m \atop k} \right\rangle \Phi_i P_k(x) = \sum \left\langle {m \atop k} \right\rangle (P_k(x) \mid P_0(x))_i = \left\langle {m \atop 0} \right\rangle \|P_0(x)\|_i^2 = \left\langle {m \atop 0} \right\rangle \Phi_i(x^0)$$

coïncide pour $i = 1$ et $i = 2$. □

Corollaires et exemples

1. $N_{0,0}^{[n]}(\psi_-(k),\ \psi_0(k),\ \psi_+(k)) = N_{0,0}^{[n]}(\psi_+(k-1),\ \psi_0(k),\ \psi_-(k+1))$,

2. $N_{0,0}^{[n]}(\psi_-(k),\ \psi_0(k),\ \psi_+(k)) = N_{0,0}^{[n]}(\psi_-(k)\psi_+(k-1),\ \psi_0(k),\ 1)$,

3. $N_{0,0}^{[n]}(\psi_-(k),\ \psi_0(k),\ \psi_+(k)) = N_{0,0}^{[n]}(1,\ \psi_0(k),\ \psi_-(k+1)\psi_+(k))$.

D'un point de vue combinatoire, ces trois propriétés découlent du fait qu'une chaîne dans $E_{0,0}^{[n]}(\psi_-, \psi_0, \psi_+)$ présente autant d'accroissements positifs à une altitude k que d'accroissements négatifs à l'altitude $k+1$. On peut donc faire porter les poids possibles des accroissements positifs sur les accroissements négatifs, et réciproquement.
Si les déterminants d'une suite $\alpha \in \mathcal{F}(\mathbb{N}, \mathcal{A})$ sont tous positifs et ont pu être déterminés par le théorème 3 (avec des coefficients α, β et γ), alors on a automatiquement $\alpha_0 = 1$ et

$$\alpha_n = N_{0,0}^{[n]}(k\alpha,\ \alpha_1 + \beta k,\ 1 + k\gamma) = N_{0,0}^{[n]}(k,\ \alpha_1 + \beta k,\ (1 + k\gamma)\alpha).$$

Par exemple, on trouve :

4. Nombres de Bell : pour tout entier $a > 0$, on a

$$B_n(a) = N_{0,0}^{[n]}(k,\ k + a,\ a) \quad \text{et} \quad B_{n+1}(a) = N_{0,0}^{[n]}(k,\ k + a(a+1),\ a)$$

5. Nombres d'Euler : $E_n = N_{0,0}^{[n]}(k,\ 0,\ k+1)$

6. Factorielles : $n! = N_{0,0}^{[n]}(k,\ 2k+1,\ k+1)$ et

$$(n+1)! = N_{0,0}^{[n]}(k,\ 2(k+2),\ k+2) = N_{0,0}^{[n]}(k+1,\ 2(k+1),\ k+1)$$

   Plus généralement : $(r-1+n)!/(r-1)! = N_{0,0}^{[n]}(k,\ 2k+r,\ k+r)$

7. Involutions : pour tout entier $a > 0$, on a $I_n(a) = N_{0,0}^{[n]}(k,\ a,\ 1)$

8. Dérangements : $D_n(a) = N_{0,0}^{[n]}(ka^2,\ a - 1 + 2ak,\ k+1)$ pour tout entier $a > 0$

Le cas "ordinaire" (i.e. les déterminants de $\alpha \in \mathcal{F}(\mathbb{N}, \mathcal{A})$ sont tous positifs et ont pu être déterminés par le théorème 4) est plus délicat. On a par exemple :

9. Nombres de Motzkin : $M_n = N_{0,0}^{[n]}(1, 1, 1)$

10. Nombres de Catalan : $C_n = N_{0,0}^{[n]}(1,\ 1 + \chi(k), 1)$ avec $\chi(0) = 0$ et $\chi(k) = 1$ si $k \geqslant 1$.

Remarque

S'il existe une fonction $\widehat{\psi}_- : \mathbb{N} \setminus \{0\} \longrightarrow \mathbb{N}$ (prolongée par $\widehat{\psi}_-(0) = 0$) vérifiant

$$\widehat{\psi}_-(2k+2)\widehat{\psi}_-(2k+1) = \psi_-(k+1) \text{ et } \widehat{\psi}_-(2k) + \widehat{\psi}_-(2k+1) = \psi_0(k)$$

pour tout $k \geqslant 0$, alors $N_{0,0}^{[n]}(\psi_-, \psi_0, 1) = N_{0,0}^{[2n]}(\widehat{\psi}_-, 0, 1)$: une bijection entre $E_{0,0}^{[n]}(\psi_-, \psi_0, 1)$ et $E_{0,0}^{[2n]}(\widehat{\psi}_-, 0, 1)$ est donnée par l'homomorphisme de monoïde défini sur un maillon en posant pour tout $k \geqslant 0$:

$$\begin{aligned} F(k \xrightarrow{1} k+1) &= (2k \xrightarrow{1} 2k+1 \xrightarrow{1} 2k+2) \\ F(k+1 \xrightarrow{\psi_-} k) &= (2k+2 \xrightarrow{\widehat{\psi}_-} 2k+1 \xrightarrow{\widehat{\psi}_-} 2k) \\ F(k \xrightarrow{\psi_0} k) &= (2k \xrightarrow{1} 2k+1 \xrightarrow{\widehat{\psi}_-} 2k) \quad \text{ou} \quad (2k \xrightarrow{\widehat{\psi}_-} 2k-1 \xrightarrow{1} 2k) \end{aligned}$$

(les flèches sont surmontées de leur pondération maximale possible). En termes plus imagés, on "double" chaque maillon en choisissant de remplacer un accroissement plat par un "pic" ou un "creux". On prolonge ensuite à toute chaîne par la propriété $F(\sigma\mu) = F(\sigma)F(\mu)$.

Ainsi les nombres de Catalan sont souvent définis par $C_n = N_{0,0}^{[2n]}(1, 0, 1)$, à la place de $C_n = N_{0,0}^{[n]}(1, 1 + \chi(k), 1)$ comme nous l'avons trouvé ci-dessus.

De même, on a vu que $n! = N_{0,0}^{[n]}(k,\ 2k+1,\ k+1) = N_{0,0}^{[n]}(k^2,\ 2k+1,\ 1)$ et on peut également écrire $n! = N_{0,0}^{[2n]}(\lceil k/2 \rceil, 0, 1)$. Une bijection entre $Sym(n)$ et $E_{0,0}^{[2n]}(\lceil k/2 \rceil, 0, 1)$ est donnée dans [30] : il s'agit de la *bijection de Viennot-de Médicis* avec les "histoires de Laguerre subdivisées". Une bijection entre $Sym(n+1)$ et $E_{0,0}^{[n]}(k+1,\ 2(k+1),\ k+1)$ est donnée explicitement par la *décomposition de Françon-Viennot* [11].

3.8 Fractions continues

Pour $n \geqslant 0$, la décomposition

$$E_{i,i}^{[n+1]} = (i \xrightarrow{*} i)E_{i,i}^{[n]} \coprod \coprod_{k=0}^{n-1} (i \xrightarrow{*} i+1)E_{i+1,i+1}^{[k]}(i+1 \xrightarrow{*} i)E_{i,i}^{[n-1-k]}$$

montre que $N_{i,i}^{[n+1]} = \psi_0(i)N_{i,i}^{[n]} + \psi_+(i)\psi_-(i+1)\sum_{k=0}^{n-1} N_{i+1,i+1}^{[k]} N_{i,i}^{[n-1-k]}$.

Les fonctions génératrices ordinaires $F_i(z) = \sum N_{i,i}^{[n]} z^n$ sont donc reliées par

$$\frac{F_i(z) - 1}{z} = \psi_0(i)F_i(z) + z\psi_+(i)\psi_-(i+1)F_{i+1}(z)F_i(z).$$

En d'autres termes, on a $F_i(z) = (1-z\psi_0(i)-z^2\psi_+(i)\psi_-(i+1)F_{i+1}(z))^{-1}$ et en itérant cette relation, on aboutit formellement à une fraction continue de type "Jacobi" pour $F_0(z)$:

$$F_0(z) = \cfrac{1}{1 - z\psi_0(0) - z^2\cfrac{\psi_+(0)\psi_-(1)}{1 - z\psi_0(1) - z^2\cfrac{\psi_+(1)\psi_-(2)}{1 - z\psi_0(2) - z^2\cfrac{\psi_+(2)\psi_-(3)}{\ddots}}}}$$

Il est commode d'introduire la notation $F_0(z) = J_z\big[\psi_0(k),\ \psi_+(k)\psi_-(k+1) : k \geqslant 0\big]$ et de manière plus générale, on a $F_i(z) = J_z\big[\psi_0(k),\ \psi_+(k)\psi_-(k+1) : k \geqslant i\big]$ par translation. Le m-ième *convergent* de la fraction continue de $F_0(z)$ est

$$P_m(z)/Q_m(z) = J_z\big[\psi_0(k),\ \psi_+(k)\psi_-(k+1) : k = 0, 1, \dots, m\big].$$

Il s'agit de la fonction génératrice ordinaire associée aux nombres $N^{[n]}_{0,0}(\psi_-,\ \psi_0,\ \psi_+\chi)$ avec $\chi(k) = 1$ si $k \leqslant m$ et $\chi(k) = 0$ sinon.

Exemple : fraction continue de $\sum n!z^n$

La série $\sum n!z^n$ ayant fortement motivé cette thèse, il convient de conclure ce travail avec elle. Comme on a $n! = N^{[n]}_{0,0}(k,\ 2k+1,\ k+1)$, une fraction continue pour $\sum n!z^n$ est donnée par $J_z\big[2k+1,\ (k+1)^2 : k \geqslant 0\big]$. Nous pouvons en trouver une autre en considérant la fonction

$$F(a, b, z) = \sum_{n\geqslant 0} (a)_n (b)_n \frac{z^n}{n!}.$$

Elle offre l'avantage d'être symétrique par rapport aux variables a et b, et elle vérifie

$$F(-1, -1, z) = \sum_{n\geqslant 0} n!z^n.$$

On établit facilement la relation $F(a, b, z) - F(a, b-1, z) = azF(a-1, b-1, z)$, de laquelle on tire la fraction continue formelle

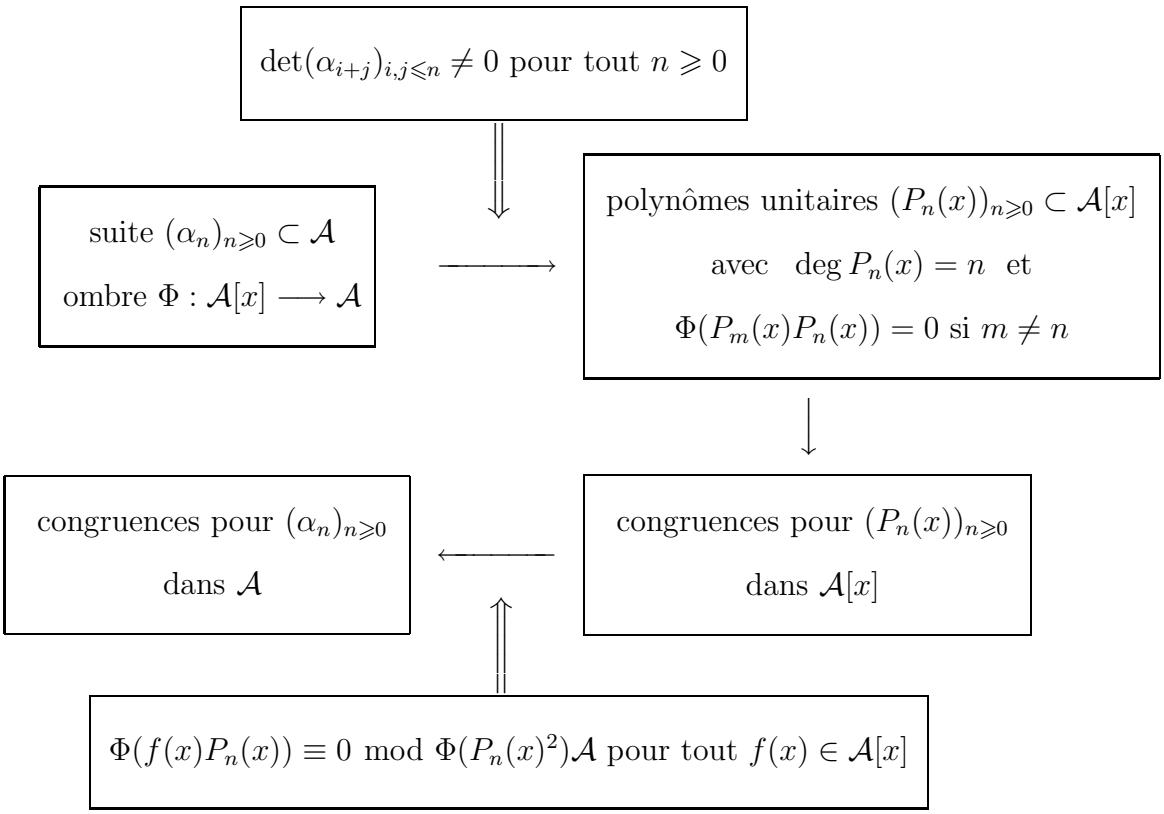
$$\frac{F(a, b-1, z)}{F(a, b, z)} = \frac{1}{1+}\ \frac{az}{1+}\ \frac{(b-1)z}{1+}\ \frac{(a-1)z}{1+}\ \frac{(b-2)z}{1+}\ \frac{(a-2)z}{1+}\ \frac{(b-3)z}{1+}\ \frac{(a-3)z}{1+}\ \cdots$$

En prenant $a = -1$ et $b = -1$ on trouve ainsi

$$\sum_{k\geqslant 0} k!z^k = \frac{1}{1-}\ \frac{z}{1-}\ \frac{z}{1-}\ \frac{2z}{1-}\ \frac{2z}{1-}\ \frac{3z}{1-}\ \frac{3z}{1-}\ \frac{4z}{1-}\ \cdots$$

3.9 Synthèse de la troisième partie

Philosophie générale



Théorème. *On considère une fonction génératrice ordinaire* $F(z) = \frac{1}{1-G(z)}$ *telle que* $G(0) = 0$ *et on suppose que* $g(z) = \nabla G(z) - \nabla G(0) = \frac{G(z)}{z} - G'(0)$ *vérifie une relation* $g(z) = z(\alpha + \beta g(z) + \gamma g(z)^2)$ *pour certains paramètres* $\alpha \neq 0$, β *et* γ *dans* $\mathcal{A}$. *Alors les déterminants de Hankel sont donnés par*

$$\det H_n = \alpha^{n(n+1)/2}\gamma^{n(n-1)/2}.$$

Les polynômes orthogonaux associés (si $\alpha\gamma \neq 0$*) sont*

$$P_0(x) = 1, \quad P_1(x) = x - F'(0), \quad P_2(x) = (x-\beta)P_1(x) - \alpha$$

$$P_{n+1}(x) = (x-\beta)P_n(x) - \alpha\gamma P_{n-1}(x) \quad (n \geqslant 2)$$

et vérifient $\|P_n(x)\|^2 = \alpha^n\gamma^{n-1}$.

Théorème. *On considère une fonction génératrice exponentielle* $F(z) = \exp G(z)$ *avec* $G(0) = 0$ *et on suppose que* $g(z) = G'(z) - G'(0)$ *vérifie* $g'(z) = \alpha + \beta g(z) + \gamma g(z)^2$ *pour certains paramètres* $\alpha \neq 0$, β *et* γ *dans* $\mathcal{A}$. *Alors*

$$F(y+z) = \sum_{k\geqslant 0} \frac{1\cdot(1+\gamma)\cdots(1+(k-1)\gamma)}{k!\alpha^k}\ g(y)^k F(y)\ g(z)^k F(z).$$

Les déterminants de Hankel correspondants sont donnés par

$$\det H_n = \alpha^{n(n+1)/2} \prod_{k=0}^{n} \Big(k!(1+\gamma)\cdots(1+(k-1)\gamma)\Big).$$

Les polynômes orthogonaux associés (si $\det H_n \neq 0$ *pour tout* $n \geqslant 0$*) sont*

$$P_0(x) = 1, \quad P_1(x) = x - F'(0)$$

$$P_{n+1}(x) = (x - F'(0) - n\beta)P_n(x) - n\alpha(1+(n-1)\gamma)P_{n-1}(x) \quad (n \geqslant 1)$$

et vérifient $\|P_n(x)\|^2 = n!\alpha^n(1+\gamma)(1+2\gamma)\cdots(1+(n-1)\gamma)$.

Théorème. *Soit* $\alpha_n = N_{0,0}^{[n]}(\psi_-, \psi_0, \psi_+)$ *le nombre de* n*-chaînes*

$$\sigma = (0 = \sigma_0 \xrightarrow{w_0} \sigma_1 \xrightarrow{w_1} \cdots \xrightarrow{w_{n-1}} \sigma_n = 0)$$

avec $\sigma_k \geqslant 0$ *pour tout* k *et dont les accroissements* $\delta_k = \sigma_{k+1} - \sigma_k \in \{-1, 0, +1\}$ *sont pondérés par*

$$1 \leqslant w_k \leqslant \begin{cases} \psi_-(\sigma_k) & si \quad \delta_k = -1 \\ \psi_0(\sigma_k) & si \quad \delta_k = 0 \\ \psi_+(\sigma_k) & si \quad \delta_k = +1 \end{cases}$$

Les déterminants de Hankel sont alors

$$\det H_n = (\psi_+(0)\psi_-(1))^n (\psi_+(1)\psi_-(2))^{n-1} \cdots (\psi_+(n-1)\psi_-(n))^1$$

Les polynômes orthogonaux associés (si ψ_- *et* ψ_+ *sont strictement positives) sont*

$$P_0(x) = 1, \quad P_1(x) = x - \psi_0(0)$$

$$P_{n+1}(x) = (x - \psi_0(n))P_n(x) - \psi_+(n-1)\psi_-(n)P_{n-1}(x)$$

et vérifient $\|P_n(x)\|^2 = (\psi_+(0)\psi_-(1)) \cdot (\psi_+(1)\psi_-(2)) \cdots (\psi_+(n-1)\psi_-(n))$.

Bibliographie

[1] M. Aigner, *A Characterization of the Bell Numbers,* Discrete Mathematics 205 (1999), p.207-210.

[2] Y. Amice, *Les Nombres p-adiques,* Presses univ. de France, coll. SUP, le Mathématicien (1975).

[3] D. Barsky, *Analyse p-adique et nombres de Bell,* Comptes Rendus Acad. Sciences 282 série A (1976), p.1257-1259.

[4] D. Barsky, B. Benzaghou, *Congruences pour les nombres de Bell,* Correspondance personnelle (2001).

[5] L. Carlitz, *A Note on Bernoulli Numbers of Higher Order,* Scripta Mathematica 22 (1956), p.217-221.

[6] P. Delsarte, *Nombres de Bell et polynômes de Charlier,* Comptes Rendus Acad. Sciences 287 série A (1978), p.271-273.

[7] R. Ehrenborg, *The Hankel Determinant of Exponential Polynomials,* American Math. Monthly 107 (2000), p.557-560.

[8] A. Gertsch, A. Robert, *Some Congruences concerning the Bell Numbers,* Bulletin de la Société Mathématique de Belgique 3 (1996), p.467-475.

[9] A. Gertsch, *Congruences pour quelques suites classiques de nombres, sommes de factorielles et calcul ombral,* Thèse de doctorat, Université de Neuchâtel (1999)

[10] R.L. Graham, D.E. Knuth, O. Patashnik, *Concrete Mathematics,* Addison - Wesley (1989).

[11] I.P Goulden, D.M. Jackson, *Combinatorial Enumeration,* Wiley - Interscience Series in Discrete Mathematics (1983).

[12] O. Hadas, *Congruences of Stirling numbers and Bell numbers via Weyl algebra,* Preprint.

[13] G. Hardy, E. Wright, *An Introduction to the Theory of Numbers,* 4th edition, Oxford, Clarendon Press (1971).

[14] W. B. Johnson, *The curious History of Faà di Bruno's Formula,* American Math. Monthly 109 (2002), p.217-234.

[15] A. Junod, *Congruences pour les polynômes et nombres de Bell,* Bulletin de la Société Mathématique de Belgique 9 (2002), p.503-509.

[16] A. Junod, *Congruences p-adiques pour une généralisation des polynômes d'Euler et de Bernoulli,* Bulletin de la Société Mathématique de Belgique, "p-adic numbers and number theory, analytic geometry and functional analysis" (2003), p.91-100.

[17] A. Junod, *Hankel Determinants and Orthogonal Polynomials,* Expositiones Mathematicae 21 (2003), p.63-74.

[18] N. Kahale, *New Modular Properties of Bell Numbers,* Journal of Combinatorial Theory, Series A 58 (1991), p.147-152.

[19] Đ. Kurepa, *Selected Papers,* Matematički Institut SANU (Beograd 1996).

[20] A. Mazouz, *Analyse p-adique et nombres de Bell à deux variables,* Bulletin de la Société Mathématique de Belgique 3 (1996), p.377-390.

[21] C. Radoux, *Nouvelles propriétés arithmétiques des Nombres de Bell,* Séminaire Delange-Pisot-Poitou, Univ. Paris VI, 16e année, exposé no 22 (1974-75).

[22] C. Radoux, *Nombres de Bell modulo p premier et extensions de degré p de* $\mathbf{F}_p$*,* Comptes Rendus Acad. Sciences, 281 série A (1975), p.879-882.

[23] C. Radoux, *Une Congruence pour les Polynômes* $P_n(x)$ *de fonction génératrice* $e^{x(e^z-1)}$*,* Comptes Rendus Acad. Sciences, 284 série A (1977), p.637-639.

[24] C. Radoux, *Arithmétique des nombres de Bell et analyse p-adique,* Bulletin de la Société Mathématique de Belgique, Vol. XXIX, fasc. 1, série B (1977), p.13-27.

[25] C. Radoux, *Densité asymptotique des nombres de Bell divisibles par un nombre premier p,* Annales de la Société Scientifique de Bruxelles, Vol. 91, fasc. IV (1977), p.207-214.

[26] C. Radoux, *Propriétés de distribution de la suite des nombres de Bell réduite modulo p premier,* Comptes Rendus Acad. Sciences, 285 série A (1977), p.653-655.

[27] C. Radoux, *Calcul effectif de certains déterminants de Hankel,* Bulletin de la Société Mathématique de Belgique, série B31 (1979), p.49-55.

[28] C. Radoux, *Addition Formulas and Hankel Determinants for some classical Sequences of Integers,* Journal of Comput. and Applied Math. 115 (2000), p.471-477.

[29] C. Radoux, *The Hankel Determinant of Exponential Polynomials : A very short Proof and a new Result concerning Euler Numbers,* American Math. Monthly 109 (2002), p.277-278.

[30] A. Randrianarivony, *Correspondances entre les différents types de bijections entre le groupe symétrique et les chemins de Motzkin valués,* Séminaire Lotharingien de Combinatoire, B35h (1995).

[31] A. Robert, *A Course in p-adic Analysis,* GTM 198, Springer-Verlag (2000).

[32] A. Robert, M. Zuber, *The Kazandzidis supercongruences - A simple proof and an application,* Rendiconti del Seminario Matematico della Università di Padova, Vol. 94 (1995), p.235-243.

[33] A. Robert, *A Note on the Numerators of the Bernoulli Numbers,* Expositiones Mathematicae 9 (1991), p.189-191.

[34] A. Robert, *Systèmes de Polynômes,* Queen's Papers in Pure and Applied Mathematics, no. 35 (1973).

[35] S. Roman, G.-C. Rota, *The Umbral Calculus,* Advances in Mathematics, Vol. 27, no. 2 (1978), p.95-188.

[36] G.-C. Rota, D. Kahaner, A. Odlyzko, *Finite Operator Calculus,* Journal of Mathematical Analysis and Applications, Vol. 42, no. 3 (1973), p.685-760.

[37] W.H. Schikhof, *Ultrametric Calculus, an Introduction to p-adic Analysis,* Cambridge University Press (1984).

[38] E.W. Weisstein, *Concise Encyclopedia of Mathematics,* CRC Press (1999).

[39] P.T. Young, *Congruences for Bernoulli, Euler, and Stirling Numbers,* Journal of Number Theory 78 (1999) p.204-227.

[40] M. Zuber, *Propriétés p-adiques de polynômes classiques,* Thèse de doctorat, Université de Neuchâtel (1992).

[41] M. Zuber, *Propriétés de congruence de certaines familles classiques de polynômes,* Comptes Rendus Acad. Sciences, 315 Série I (1992), p.869-872.

[42] M. Zuber, *Une suite récurrente remarquable,* Comptes Rendus Acad. Sciences, 318 Série I (1994), p.205-208.