

CONGRUENCES POUR QUELQUES  
SUITES CLASSIQUES DE NOMBRES;  
SOMMES DE FACTORIELLES ET  
CALCUL OMBRAL

THESE

présentée à la faculté des sciences, pour obtenir  
le grade de docteur ès sciences, par

Anne Gertsch Hamadene

UNIVERSITE DE NEUCHATEL  
Institut de mathématiques  
Rue Emile-Argand 11  
Case postale 2  
CH-2007 NEUCHATEL (Suisse)

# IMPRIMATUR POUR LA THÈSE

**Congruences pour quelques suites classiques de  
nombres; sommes de factorielles et calcul ombra**

de Mme Anne Gertsch Hamadene

---

UNIVERSITÉ DE NEUCHÂTEL

FACULTÉ DES SCIENCES

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

MM. A. Robert (directeur de thèse), U. Suter,  
et L. van Hamme (Vrije Uni. Bruxelles)

autorise l'impression de la présente thèse.

Neuchâtel, le 18 février 1999

Le doyen:



F. Stoeckli

## Avant-propos

Le présent travail de thèse est constitué du texte ci-après ainsi que des deux articles [7] et [8]. Dans l'article [7], nous avons démontré de nouvelles propriétés de congruence pour les nombres et les polynômes de Bell, et ce en utilisant des méthodes originales de calcul ombral. Dans l'article [8], il est démontré plusieurs propriétés de divisibilité des nombres harmoniques généralisés conjecturées par Y. Matiyasevich.

Les 6 premiers paragraphes du texte ci-après constituent une étude diversifiée de problèmes liés à des sommes de factorielles.

Le paragraphe 1 énonce les deux conjectures qui ont motivé ce travail, à savoir l'irrationalité de la somme (infinie) des factorielles en analyse  $p$ -adique et l'hypothèse de Kurepa concernant les sommes finies de factorielles. On rappelle ensuite quelques définitions et propriétés du système des polynômes de Pochhammer ainsi que des nombres de Stirling de première et de deuxième espèce.

Le paragraphe 2 introduit une fonction génératrice qui, tantôt sous la forme d'une série de Mahler, tantôt sous celle d'une série de puissances, permet d'exprimer les problèmes de sommes de factorielles liés aux deux conjectures du paragraphe 1. D'autre part, l'hypothèse de Kurepa est mise en relation avec l'analyse combinatoire : le nombre de permutations sans point fixe des éléments d'un ensemble fournit un énoncé équivalent à l'hypothèse de Kurepa.

Dans le paragraphe 3, on démontre des congruences fortes mettant en relation les nombres de Stirling de première espèce avec ceux de deuxième espèce.

Les congruences du paragraphe 3 permettent de construire un lien entre des sommes partielles (finies) de factorielles et les polynômes de Bell ; en particulier, un énoncé reliant l'hypothèse de Kurepa aux nombres de Bell constitue le point fort du paragraphe 4.

Le paragraphe 5 reprend, éclaire et améliore certains résultats de B. Dragovich ([5], [6]) à propos de formules qui font intervenir des sommes, finies ou infinies, de factorielles.

Au paragraphe 6, des méthodes de calcul ombral permettent en particulier d'améliorer un résultat de B. Dragovich.

Enfin, le paragraphe 7 consiste en une généralisation des congruences fortes pour les nombres de Bell qui se trouvent dans [7]. Cette généralisation

s'applique aux polynômes de Bell-Carlitz, à savoir à la généralisation de L. Carlitz des nombres de Bell. Les méthodes utilisées sont analogues à celles de [7].

Je tiens à remercier chaleureusement toutes les personnes qui m'ont aidée à mener à bien ce travail.

Mes remerciements vont en priorité à mon directeur de thèse, Monsieur Alain Robert, qui m'a sans cesse encouragée au cours de ces quatre années. A de nombreuses reprises, j'ai bénéficié de ses exposés, tous plus intéressants les uns que les autres. Il m'a en outre fait partager son goût pour les raisonnements mathématiques clairs et astucieux. Son enthousiasme et sa disponibilité de chaque instant m'ont permis de travailler dans des conditions optimales.

Je remercie sincèrement Messieurs Ulrich Suter et Lucien van Hamme qui ont accepté de faire partie de mon jury de thèse.

Je remercie aussi Messieurs Maxime Zuber et Christian Vonlanthen qui m'ont beaucoup encouragée et orientée au début de mon travail, ainsi que les collègues - et néanmoins amis - qui se sont succédés dans mon bureau, à savoir Paul-André Garessus, Valérie Schürch, Eva Schlaepfer et Alexandre Junod. Ils m'ont été d'un grand soutien, aussi bien mathématique que psychologique.

Mes remerciements vont également à mon mari Slimane Hamadene ainsi qu'à toute ma famille, qui, toujours présents, m'ont encouragée lors des bons et des mauvais moments de ces quatre années. . .

Pour terminer, je remercie tous les professeurs et les assistants de l'institut de mathématiques qui, à plusieurs reprises, m'ont soutenue et conseillée dans mon travail. Ils m'ont habituée à une ambiance de travail chaleureuse et sympathique.

## Table des matières

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	Deux conjectures . . . . .	3
1.2	Polynômes de Pochhammer et nombres de Stirling . . . . .	4
<b>2</b>	<b>Une fonction génératrice</b>	<b>4</b>
2.1	Série de Mahler . . . . .	4
2.2	Analyse combinatoire . . . . .	5
2.3	Série de puissances . . . . .	7
2.4	Tronquées de $f$ . . . . .	9
<b>3</b>	<b>Congruences fortes pour les nombres de Stirling</b>	<b>11</b>
<b>4</b>	<b>Polynômes et nombres de Bell</b>	<b>16</b>
<b>5</b>	<b>Sommes de factorielles selon B. Dragovich</b>	<b>18</b>
5.1	Sommes infinies . . . . .	18
5.2	Sommes finies . . . . .	23
<b>6</b>	<b>Calcul ombra</b>	<b>26</b>
6.1	Une autre application . . . . .	27
<b>7</b>	<b>Polynômes de Bell-Carlitz</b>	<b>29</b>
7.1	Quelques congruences polynomiales . . . . .	29
7.2	Calcul ombra . . . . .	30
7.3	Les polynômes de Bell-Carlitz . . . . .	33

# 1 Introduction

Pour un nombre premier  $p$ , on désigne par  $Z_p$  l'anneau des entiers  $p$ -adiques, par  $Q_p$  le corps des nombres  $p$ -adiques, complété de  $Q$  pour la valeur absolue  $p$ -adique usuelle  $|\cdot|_p$  (normalisée par  $|p|_p = 1/p$ ), et enfin par  $C_p$  le complété de la clôture algébrique de  $Q_p$ .

## 1.1 Deux conjectures

La motivation de ce travail est basée sur les conjectures ci-après.

CONJECTURE 1.1.- *La somme*

$$S = \sum_{n \geq 0} n!,$$

*convergente dans  $Q_p$ , est un nombre irrationnel (i.e.  $S \in Q_p \setminus Q$ ). Plus fort :  $S$  est un nombre transcendant.*

CONJECTURE 1.2 (HYPOTHÈSE DE KUREPA).- *Soit  $p$  un nombre premier impair; alors la somme*

$$\kappa_p = \sum_{0 \leq n \leq p-1} n!$$

*n'est jamais congrue à zéro modulo  $p$  (i.e.  $|\kappa_p|_p = 1$  pour tout  $p$  premier impair).*

REMARQUE.- Pour  $p$  premier impair,  $\kappa_p$  est pair et  $\kappa_p/2$  est impair dès que  $p > 3$ ; en d'autres termes,  $\kappa_p \equiv 2 \pmod{4}$  pour  $p > 3$ .

Exprimons quelques valeurs de  $\kappa_p$  modulo  $p$ .

$p$	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$\kappa_p \pmod{p}$	0	1	4	6	1	10	13	9	21	17	2	5	4	16	18

A priori il est étrange que l'on ne puisse rien dire de ces sommes alors que  $\sum_{n \geq 0} n \cdot n!$  est bien connue : elle vaut  $-1$  dans  $Z_p$ !

Une approche naïve du problème consiste à considérer un diviseur premier  $q > 2$  de  $\kappa_p$ . Si  $q = p$ , alors l'hypothèse de Kurepa est fausse. Si  $q < p$ , alors  $q$  divise  $n!$  pour  $n : q \leq n \leq p-1$ , donc  $q$  divise  $\sum_{0 \leq n \leq q-1} n! = \kappa_q$  et l'hypothèse de Kurepa est fausse.

Ainsi, l'hypothèse de Kurepa est équivalente à l'énoncé suivant.

“Soit  $q > 2$  un diviseur premier de  $\kappa_p$ ; alors  $q > p$ ”.

## 1.2 Polynômes de Pochhammer et nombres de Stirling

On considère le système de polynômes de Pochhammer  $\{(x)_n\}_{n \geq 0}$  défini par  $(x)_0 = 1$  et  $(x)_n = x(x-1)\dots(x-n+1) = n! \binom{x}{n}$  ( $n \geq 1$ ). Le degré de  $(x)_n$  vaut  $n$  et ces polynômes forment donc une base de  $\mathbb{Q}[x]$ .

**PROPOSITION 1.1.** - Pour  $\nu \geq 1$  et  $p$  un nombre premier impair, on a la congruence de Bauer généralisée [7]

$$(x)_{p^\nu} \equiv (x^p - x)^{p^{\nu-1}} \pmod{p^\nu \mathbb{Z}_p[x]} \quad (1).$$

Pour  $p = 2$ , la même congruence est valable modulo  $2^{\nu-1} \mathbb{Z}_2[x]$ .

Les nombres de Stirling de première espèce  $\left[ \begin{matrix} n \\ k \end{matrix} \right]$  ( $n, k \geq 0$ ) sont les entiers positifs définis par la formule

$$(x)_n = \sum_{0 \leq k \leq n} \left[ \begin{matrix} n \\ k \end{matrix} \right] (-1)^{n-k} x^k \quad (2).$$

Ils vérifient la relation de récurrence

$$\left[ \begin{matrix} n+1 \\ k \end{matrix} \right] = n \left[ \begin{matrix} n \\ k \end{matrix} \right] + \left[ \begin{matrix} n \\ k-1 \end{matrix} \right] \quad (3).$$

Les nombres de Stirling de deuxième espèce  $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$  ( $n, k \geq 0$ ) sont les entiers positifs définis par la formule

$$x^n = \sum_{0 \leq k \leq n} \left\{ \begin{matrix} n \\ k \end{matrix} \right\} (x)_k \quad (4).$$

Ils vérifient la relation de récurrence

$$\left\{ \begin{matrix} n+1 \\ k \end{matrix} \right\} = k \left\{ \begin{matrix} n \\ k \end{matrix} \right\} + \left\{ \begin{matrix} n \\ k-1 \end{matrix} \right\} \quad (5).$$

## 2 Une fonction génératrice

### 2.1 Série de Mahler

On considère le développement formel

$$1 - x + x(x-1) - x(x-1)(x-2) \pm \dots = \sum_{n \geq 0} (-1)^n (x)_n,$$

qui s'écrit aussi

$$\sum_{n \geq 0} (-1)^n n! \binom{x}{n}.$$

Puisque les coefficients  $c_n = (-1)^n n!$  tendent  $p$ -adiquement vers 0, il s'agit d'une série de Mahler dans  $\mathbb{Z}_p$  et cette série définit une fonction continue  $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ . L'évaluation en  $x = -1$  donne

$$f(-1) = \sum_{n \geq 0} n! = S.$$

On voit aisément que  $f$  vérifie la relation

$$f(x) = 1 - x f(x - 1),$$

relation dont on tire les valeurs particulières

$n$	...	-3	-2	-1	0	1	2	3	4	5	6	...
$f(n)$	...	$S/2 - 1$	$S - 1$	$S$	1	0	1	-2	9	-44	265	...

En particulier, si  $S$  est irrationnelle (resp. transcendante), alors  $f(-n)$  l'est aussi pour tout  $n \in \mathbb{N}$ .

## 2.2 Analyse combinatoire

Considérons le groupe  $S_n$  des permutations de l'ensemble  $\{1, 2, \dots, n\}$ ; soit  $D_n$  le nombre de permutations sans point fixe de  $\{1, 2, \dots, n\}$ ; ces permutations sont parfois appelées "dérangements" de  $\{1, 2, \dots, n\}$ .

On connaît les formules [26]

$$D_n = (n - 1)[D_{n-1} + D_{n-2}] \quad (D_0 = 1, D_1 = 0),$$

$$D_n = nD_{n-1} + (-1)^n \quad (D_0 = 1).$$

et de manière explicite

$$D_n = (n)_n - (n)_{n-1} + (n)_{n-2} \mp \dots = \sum_{0 \leq i \leq n} \frac{n!}{i!} (-1)^i.$$

REMARQUES.- 1) Les formules de récurrence présentent des analogies avec celles qui définissent la factorielle. En effet, on a

$$n! = (n - 1)[(n - 1)! + (n - 2)!] \quad (0! = 1, 1! = 1)$$

$$\text{et} \quad n! = n(n - 1)! \quad (0! = 1).$$

2) Le nombre  $D_n$  est l'entier le plus proche de  $\frac{n!}{e} = \frac{\Gamma(n+1)}{e}$ .

Reprenons notre fonction

$$f(x) = \sum_{k \geq 0} (-1)^k (x)_k.$$

Pour  $x = n \in \mathbb{N}$ , on obtient

$$f(n) = \sum_{k \geq 0} (-1)^k (n)_k = (-1)^n \sum_{0 \leq k \leq n} (-1)^{n+k} (n)_k = (-1)^n D_n.$$

PROPOSITION 2.1.- Pour  $n = p - 1$ , avec  $p$  un nombre premier impair, on a

$$D_{p-1} \equiv \kappa_p \pmod{p}.$$

PREUVE.- On calcule simplement

$$D_{p-1} = f(p-1) \equiv f(-1) \equiv \kappa_p \pmod{p}. \quad \square$$

COROLLAIRE 2.1.- L'hypothèse de Kurepa est équivalente à l'énoncé

$$D_{p-1} \not\equiv 0 \pmod{p}$$

quel que soit  $p$  premier impair.

Rappelons qu'une permutation est dite *paire* si elle s'écrit comme produit d'un nombre pair de transpositions, et *impaire* sinon. Soient  $N_n^+$ , respectivement  $N_n^-$ , le nombre de permutations paires, respectivement impaires sans point fixe de l'ensemble  $\{1, 2, \dots, n\}$ . On connaît la somme  $N_n^+ + N_n^- = D_n$ . On a de plus

$$N_n^+ - N_n^- = (-1)^{n-1} (n-1).$$

Pour  $n = p - 1$ ,  $p$  premier impair, il s'ensuit

$$N_{p-1}^+ - N_{p-1}^- = -(p-2) \equiv 2 \pmod{p}$$

alors que

$$N_{p-1}^+ + N_{p-1}^- = D_{p-1} \equiv \kappa_p \pmod{p}.$$

On en tire les congruences

$$\kappa_p \equiv 2(N_{p-1}^+ - 1) \pmod{p} \quad \text{et} \quad \kappa_p \equiv 2(N_{p-1}^- + 1) \pmod{p}.$$

Soit  $G$  un groupe et  $X$  un  $G$ -ensemble (i.e.  $G$  agit sur  $X$  via  $\alpha : G \times X \rightarrow X$ ). Rappelons le lemme de Burnside [24].

LEMME 2.1.- *Supposons que  $X$  et  $G$  sont finis ; soit  $N$  le nombre de  $G$ -orbites de  $X$  ; alors*

$$N = \frac{1}{|G|} \sum_{\tau \in G} F(\tau)$$

où  $F(\tau)$  est le nombre de points  $x \in X$  fixés par  $\tau \in G$ .

APPLICATION.- Soit  $G = S_n$  ; alors  $|G| = n!$  et  $N = 1$  ( $G$  est transitif). Dénotons par  $a_i$ ,  $0 \leq i \leq n$ , le nombre d'éléments de  $S_n$  qui ont  $i$  points fixes. Alors  $a_0 = D_n$  et

$$|S_n| = n! = \sum_{0 \leq i \leq n} a_i = D_n + \sum_{1 \leq i \leq n} a_i.$$

D'autre part, le lemme de Burnside fournit

$$|S_n| = n! = \sum_{\tau \in S_n} F(\tau) = \sum_{0 \leq i \leq n} i a_i = \sum_{1 \leq i \leq n} i a_i.$$

On obtient donc

$$D_n = n! - \sum_{1 \leq i \leq n} a_i = \sum_{1 \leq i \leq n} (i-1) a_i$$

et l'hypothèse de Kurepa ( $n = p-1$ ) est équivalente à

$$\sum_{1 \leq i \leq p-1} (i-1) a_i \not\equiv 0 \pmod{p}$$

ou encore à

$$\sum_{1 \leq i \leq p-1} a_i + 1 \not\equiv 0 \pmod{p}$$

grâce à la congruence  $(p-1)! \equiv -1 \pmod{p}$  (Wilson).

## 2.3 Série de puissances

Les résultats suivants vont permettre d'exprimer  $f$  sous forme de série de puissances.

PROPOSITION 2.2.- *Les congruences*

$$\left[ \begin{matrix} p^\nu + j \\ k \end{matrix} \right] \equiv 0 \pmod{p^\nu}$$

sont valables pour tous  $\nu \geq 1$ ,  $0 \leq k < p^{\nu-1}$  et  $j \in \mathbb{N}$ .

PREUVE.- Pour  $p > 2$  (le cas  $p = 2$  se traite de manière analogue), on tire des relations (1) et (2) (voir 1.2)

$$x^{p^{\nu-1}}(x^{p-1} - 1)^{p^{\nu-1}} \equiv \sum_{0 \leq k \leq p^{\nu}} \binom{p^{\nu}}{k} (-1)^{p^{\nu}-k} x^k \pmod{p^{\nu} \mathbb{Z}_p[x]}.$$

Dans le membre de gauche, la première puissance de  $x$  apparaissant est  $x^{p^{\nu-1}}$ , ce qui implique que

$$\binom{p^{\nu}}{k} \equiv 0 \pmod{p^{\nu}} \quad (0 \leq k < p^{\nu-1}).$$

Par induction sur  $j$ , on montre alors aisément que

$$\binom{p^{\nu} + j}{k} \equiv 0 \pmod{p^{\nu}} \quad (\nu \geq 1, 0 \leq k < p^{\nu-1}, j \in \mathbb{N}),$$

et ce grâce à la formule de récurrence (3) (voir 1.2) appliquée à  $n = p^{\nu} + j$  et à  $k < p^{\nu-1}$ .  $\square$

COROLLAIRE 2.2.- Pour tout  $k \geq 0$ , la suite  $\left(\binom{m+k}{k}\right)$  converge vers 0 dans  $\mathbb{Z}_p$  lorsque  $m \rightarrow \infty$ . On peut donc définir

$$a_k = (-1)^k \sum_{m \geq 0} \binom{m+k}{k} \in \mathbb{Z}_p$$

(car  $\mathbb{Z}_p$  est complet) pour tout  $k \geq 0$ .

PREUVE.- Soit  $k \in \mathbb{N}$  fixé et  $\nu \geq 1$  tel que  $p^{\nu-1} > k$ ; alors, pour tout  $\mu \geq \nu$  et  $m \geq p^{\mu}$ , on a

$$\binom{m+k}{k} = \binom{p^{\mu} + j}{k} \equiv 0 \pmod{p^{\mu}},$$

et on en déduit la convergence de  $\binom{m+k}{k}$  vers 0.  $\square$

Grâce à la formule (2) (voir 1.2) et au corollaire 2.2, la fonction  $f$  s'écrit maintenant en série de puissances

$$f(x) = \sum_{n \geq 0} \sum_{0 \leq k \leq n} \binom{n}{k} (-1)^k x^k = \sum_{k \geq 0} a_k x^k$$

où

$$a_k = (-1)^k \sum_{n \geq k} \binom{n}{k} = (-1)^k \sum_{m \geq 0} \binom{m+k}{k}.$$

**COROLLAIRE 2.3.**— La fonction  $f$  est localement analytique ; elle est analytique dans toute boule stricte  $B_{<1}(m) \subset \mathbb{C}_p$ ,  $m \in \{0, 1, \dots, p-1\}$ .

**PREUVE.**— Comme  $|a_k| \leq 1 \ \forall k \geq 0$ ,  $f(x)$  est analytique dans la boule  $B_{<1}(0) \subset \mathbb{C}_p$ . En vertu de l'égalité

$$f(x-1) = \frac{1-f(x)}{x},$$

$f$  est aussi analytique dans  $B_{<1}(1) \subset \mathbb{C}_p$ , et par extension dans toute boule  $B_{<1}(m) \subset \mathbb{C}_p$ ,  $m \in \{0, 1, \dots, p-1\}$ .  $\square$

On a de plus

$$S = f(-1) = \sum_{k \geq 0} a_k (-1)^k = \sum_{k \geq 0} \sum_{n \geq k} \begin{bmatrix} n \\ k \end{bmatrix} = \sum_{n \geq 0} n!;$$

c'est la somme (par colonnes) de tous les nombres de Stirling de première espèce ! Or, sachant que  $\begin{bmatrix} n+1 \\ 1 \end{bmatrix} = n!$ , on a aussi

$$S = \sum_{n \geq 0} n! = \sum_{n \geq 0} \begin{bmatrix} n \\ 1 \end{bmatrix},$$

ce qui correspond à la somme des éléments d'une colonne du tableau des nombres de Stirling de première espèce ! Il en découle en particulier

$$\sum_{k \geq 2} \sum_{n \geq k} \begin{bmatrix} n \\ k \end{bmatrix} = -1 = \sum_{n \geq 0} n \cdot n!.$$

En dérivant successivement la relation  $f(x) = 1 - xf(x-1)$ , on obtient

$$f^{(n)}(x) = -nf^{(n-1)}(x-1) - xf^{(n)}(x-1), \quad n \geq 1.$$

En particulier  $f^{(n)}(0) = -nf^{(n-1)}(-1)$  et donc

$$S = f(-1) = -f'(0) = \sum_{n \geq 0} n!.$$

## 2.4 Tronquées de $f$

Pour un nombre premier  $p$ , considérons les  $p$  premiers termes de la somme définissant  $f$  en posant

$$\kappa_p(x) := \sum_{0 \leq n \leq p-1} (-1)^n (x)_n.$$

On a alors

$$\kappa_p(-1) = \sum_{0 \leq n \leq p-1} n! = \kappa_p \equiv f(-1) \pmod{p}.$$

PROPOSITION 2.3.- La relation

$$f(x) = \kappa_p(x) - (x)_p f(x-p)$$

est valable pour tout nombre premier  $p$ .

PREUVE.- On a simplement

$$\begin{aligned} f(x) &= \kappa_p(x) + \sum_{m \geq 0} (-1)^{m+p} (x)_{m+p} = \kappa_p(x) - \sum_{m \geq 0} (-1)^m (x)_p (x-p)_m \\ &= \kappa_p(x) - (x)_p f(x-p). \end{aligned} \quad \square$$

Il s'ensuit que

$$\begin{aligned} f(x) &= \kappa_p(x) - (x)_p \sum_{0 \leq n \leq p-1} (-1)^n (x-p)_n \\ &\quad - (x)_{2p} \sum_{0 \leq n \leq p-1} (-1)^n (x-2p)_n \\ &\quad - (x)_{3p} \sum_{0 \leq n \leq p-1} \dots - \dots \\ &\equiv \kappa_p(x) - (x)_p \kappa_p(x) - (x)_{2p} \kappa_p(x) - \dots \pmod{p\mathbf{Z}_p[x]} \end{aligned}$$

et au total

$$f(x) \equiv \kappa_p(x) (1 - (x)_p - (x)_{2p} - \dots) \pmod{p\mathbf{Z}_p[x]}.$$

Sachant que  $(x)_{np} \equiv (x)_p^n \pmod{p\mathbf{Z}_p[x]}$ , on peut encore écrire (dans  $\mathbf{Q}_p(x)$ )

$$1 - (x)_p - (x)_{2p} - \dots \equiv 2 - \sum_{n \geq 0} (x)_p^n = 2 - \frac{1}{1 - (x)_p} \pmod{p\mathbf{Z}_p[x]},$$

et donc

$$f(x) \equiv \kappa_p(x) \left( 2 - \frac{1}{1 - x^p + x} \right) \equiv \kappa_p(x) \frac{1 - 2x^p + 2x}{1 - x^p + x} \pmod{p\mathbf{Z}_p[x]}.$$

On a vu que  $f(-1) = \sum_{n \geq 0} n! \equiv \kappa_p \pmod{p\mathbf{Z}_p}$ ; modulo  $p^2$ , on obtient la

PROPOSITION 2.4.- On a

$$f(-1) \equiv (1-p)\kappa_p \pmod{p^2\mathbf{Z}_p}$$

PREUVE.- On écrit

$$\begin{aligned} \sum_{n \geq 0} n! &\equiv \kappa_p + p!(1 + (p+1) + (p+1)(p+2) + \dots) \pmod{p^2\mathbf{Z}_p} \\ &\equiv \kappa_p + p(p-1)!\kappa_p \pmod{p^2\mathbf{Z}_p} \end{aligned}$$

et le résultat découle de la congruence de Wilson  $(p-1)! \equiv -1 \pmod{p}$ .  $\square$

REMARQUE.- Modulo  $p^3$ , on obtient de manière analogue

$$f(-1) = \sum_{n \geq 0} n! \equiv \kappa_p + p! \sum_{0 \leq k \leq p-1} (p+k)_k + 2p^2\kappa_p \pmod{p^3\mathbf{Z}_p}$$

qui s'écrit aussi

$$\begin{aligned} f(-1) &= \sum_{n \geq 0} n! \equiv \kappa_p + p!\kappa_p + 2p^2\kappa_p + p \cdot p! \sum_{0 \leq k \leq p-1} k!H_k \pmod{p^3\mathbf{Z}_p} \\ &\equiv \kappa_p + p!\kappa_p + p^2 \left( 2\kappa_p - \sum_{0 \leq k \leq p-1} k!H_k \right) \pmod{p^3\mathbf{Z}_p} \end{aligned}$$

où  $H_k$  représente le  $k$ -ième nombre harmonique. Dans le cas général, on a la formule

$$\begin{aligned} f(-1) = \sum_{n \geq 0} n! &\equiv \sum_{0 \leq l \leq \nu} (lp)! \sum_{0 \leq k \leq p-1} (lp+k)_k \pmod{p^{\nu+1}\mathbf{Z}_p} \\ &\equiv \sum_{0 \leq l \leq \nu} (lp)! \sum_{0 \leq k \leq p-1} k! \binom{lp+k}{k} \pmod{p^{\nu+1}\mathbf{Z}_p}. \end{aligned}$$

### 3 Congruences fortes pour les nombres de Stirling

À l'instar du triangle de Pascal formé des coefficients binomiaux, on peut considérer les triangles de Stirling formés des nombres de Stirling de première, respectivement de deuxième espèce. Appelons  $T_1$  le triangle de Stirling de

première espèce et  $T_2$  le triangle de Stirling de deuxième espèce; on a

$$T_1 = \begin{array}{cccccccc} 1 & & & & & & & & \\ 0 & 1 & & & & & & & \\ 0 & 1 & 1 & & & & & & \\ 0 & 2 & 3 & 1 & & & & & \\ 0 & 6 & 11 & 6 & 1 & & & & \\ 0 & 24 & 50 & 35 & 10 & 1 & & & \\ 0 & 120 & 274 & 225 & 85 & 15 & 1 & & \\ 0 & 720 & 1764 & 1624 & 735 & 175 & 21 & 1 & \\ 0 & 5040 & 13068 & 13132 & 6769 & 1960 & 322 & 28 & 1 \\ \vdots & & \dots & & \dots & & \dots & & \dots \end{array}$$

et

$$T_2 = \begin{array}{cccccccc} 1 & & & & & & & & \\ 0 & 1 & & & & & & & \\ 0 & 1 & 1 & & & & & & \\ 0 & 1 & 3 & 1 & & & & & \\ 0 & 1 & 7 & 6 & 1 & & & & \\ 0 & 1 & 15 & 25 & 10 & 1 & & & \\ 0 & 1 & 31 & 90 & 65 & 15 & 1 & & \\ 0 & 1 & 63 & 301 & 350 & 140 & 21 & 1 & \\ 0 & 1 & 127 & 966 & 1701 & 1050 & 266 & 28 & 1 \\ \vdots & & \dots & & \dots & & \dots & & \dots \end{array}$$

Les relations de récurrence (voir 1.2) permettent de calculer les éléments de la  $(n + 1)$ -ième ligne du triangle à partir de ceux de la  $n$ -ième ligne.

Considérons maintenant les triangles  $T_1^{(p)}$  et  $T_2^{(p)}$  formés des éléments des lignes (et des colonnes) d'indice  $1, \dots, p - 1$  de  $T_1$  et  $T_2$  calculés modulo  $p$ ; pour  $p = 3, 5, 7, 11$ , on observe

$$\begin{array}{cc} T_1^{(3)} = \begin{array}{ccc} 1 & & \\ 1 & 1 & \end{array} & T_2^{(3)} = \begin{array}{ccc} 1 & & \\ 1 & 1 & \end{array} \\ \\ T_1^{(5)} = \begin{array}{cccc} 1 & & & \\ 1 & 1 & & \\ 2 & 3 & 1 & \\ 1 & 1 & 1 & 1 \end{array} & T_2^{(5)} = \begin{array}{cccc} 1 & & & \\ 1 & 1 & & \\ 1 & 3 & 1 & \\ 1 & 2 & 1 & 1 \end{array} \end{array}$$

$$T_1^{(7)} = \begin{matrix} 1 \\ 1 & 1 \\ 2 & 3 & 1 \\ 6 & 4 & 6 & 1 \\ 3 & 1 & 0 & 3 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{matrix}$$

$$T_2^{(7)} = \begin{matrix} 1 \\ 1 & 1 \\ 1 & 3 & 1 \\ 1 & 0 & 6 & 1 \\ 1 & 1 & 4 & 3 & 1 \\ 1 & 3 & 6 & 2 & 1 & 1 \end{matrix}$$

$$T_1^{(11)} = \begin{matrix} 1 \\ 1 & 1 \\ 2 & 3 & 1 \\ 6 & 0 & 6 & 1 \\ 2 & 6 & 2 & 10 & 1 \\ 10 & 10 & 5 & 8 & 4 & 1 \\ 5 & 4 & 7 & 9 & 10 & 10 & 1 \\ 2 & 0 & 9 & 4 & 2 & 3 & 6 & 1 \\ 5 & 2 & 6 & 8 & 9 & 4 & 7 & 3 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{matrix}$$

$$T_2^{(11)} = \begin{matrix} 1 \\ 1 & 1 \\ 1 & 3 & 1 \\ 1 & 7 & 6 & 1 \\ 1 & 4 & 3 & 10 & 1 \\ 1 & 9 & 2 & 10 & 4 & 1 \\ 1 & 8 & 4 & 9 & 8 & 10 & 1 \\ 1 & 6 & 9 & 7 & 5 & 2 & 6 & 1 \\ 1 & 2 & 0 & 4 & 10 & 6 & 0 & 3 & 1 \\ 1 & 5 & 2 & 5 & 10 & 2 & 6 & 2 & 1 & 1 \end{matrix}$$

On observe que les lignes de  $T_1^{(p)}$  deviennent les colonnes de  $T_2^{(p)}$ , lues depuis la droite et de bas en haut. En d'autres termes, on observe les congruences

$$\begin{bmatrix} n \\ k \end{bmatrix} \equiv \begin{bmatrix} p-k \\ p-n \end{bmatrix} \pmod{p}, \quad 1 \leq n, k \leq p-1.$$

Pour  $p$  premier impair, on va démontrer une généralisation de ces congruences. Partons de la congruence polynomiale (1) du paragraphe 1.2, qui s'écrit aussi

$$\sum_{0 \leq k \leq p^\nu} \begin{bmatrix} p^\nu \\ k \end{bmatrix} (-1)^{k+1} x^k \equiv \sum_{0 \leq i \leq p^\nu-1} \binom{p^\nu-1}{i} (-1)^{i+1} x^{p^\nu-1+i(p-1)} \pmod{p^\nu \mathbb{Z}_p[x]}.$$

Dans le membre de droite, aucune puissance de  $x$  n'apparaît entre  $x^{p^\nu-(p-1)}$  et  $x^{p^\nu}$ . On en tire les congruences

$$\begin{bmatrix} p^\nu \\ p^\nu - k \end{bmatrix} \equiv 0 \pmod{p^\nu}, \quad 1 \leq k < p-1 \quad (*).$$

LEMME 3.1.- On a

$$\begin{bmatrix} p^\nu - 1 \\ p^\nu - k \end{bmatrix} \equiv 1 \pmod{p^\nu}, \quad 1 \leq k \leq p-1.$$





GÉNÉRALISATION.- Les congruences

$$\begin{bmatrix} p^\nu - j \\ p^\nu - i \end{bmatrix} \equiv \begin{Bmatrix} i \\ j \end{Bmatrix} \pmod{p^\nu},$$

valables pour  $0 \leq j \leq i \leq p-1$  ( $\nu \geq 1$ ), le sont encore pour  $p \leq i \leq p^\nu$ ,  $i-p+1 \leq j \leq i$ ,  $\nu \geq 1$ .

PREUVE.- Cela découle des relations de récurrence (3) et (5) du paragraphe 1.2; pour  $1 \leq j \leq i+1 \leq p$ , on a

$$\begin{aligned} \begin{Bmatrix} i+1 \\ j \end{Bmatrix} &= j \begin{Bmatrix} i \\ j \end{Bmatrix} + \begin{Bmatrix} i \\ j-1 \end{Bmatrix} \\ &\equiv j \begin{bmatrix} p^\nu - j \\ p^\nu - i \end{bmatrix} + \begin{bmatrix} p^\nu - (j-1) \\ p^\nu - i \end{bmatrix} \pmod{p^\nu} \\ &\equiv \begin{bmatrix} p^\nu - (j-1) \\ p^\nu - i \end{bmatrix} - (p^\nu - j) \begin{bmatrix} p^\nu - j \\ p^\nu - i \end{bmatrix} \pmod{p^\nu} \\ &\equiv \begin{bmatrix} p^\nu - j \\ p^\nu - (i+1) \end{bmatrix} \pmod{p^\nu} \end{aligned}$$

et on conclut par induction sur  $i$ . □

## 4 Polynômes et nombres de Bell

Les polynômes de Bell  $B_n(x)$  ( $n \geq 0$ ) sont définis par

$$B_n(x) = \sum_{0 \leq k \leq n} \begin{Bmatrix} n \\ k \end{Bmatrix} x^k.$$

En particulier  $B_n(1) = \sum_{0 \leq k \leq n} \begin{Bmatrix} n \\ k \end{Bmatrix} = B_n$  représente le  $n$ -ième nombre de Bell, défini également comme étant le nombre de partitions d'un ensemble à  $n$  éléments. Voici les premières valeurs

$n$	0	1	2	3	4	5	6	7	8	9	10	...
$B_n$	1	1	2	5	15	52	203	877	4140	21147	115975	...

et  $B_0(x) = 1$ ,  $B_1(x) = x$ ,  $B_2(x) = x^2 + x$ ,  $B_3(x) = x^3 + 3x^2 + x$ ,  
 $B_4(x) = x^4 + 6x^3 + 7x^2 + x \dots$

PROPRIÉTÉS.- 1) Pour un nombre premier  $p$ , on a la congruence (due à C.Radoux, [16])

$$B_p(x) \equiv x + x^p \pmod{pZ[x]};$$

on en tire en particulier  $B_p \equiv 2 \pmod p$ .

2) La relation de récurrence (5) de 1.2 montre que

$$B_n(x) = x(B_{n-1}(x) + B'_{n-1}(x)) \quad (n \geq 1).$$

Comme  $\begin{bmatrix} m+1 \\ 1 \end{bmatrix} = m!$ , on constate que

$$\kappa_p = \sum_{0 \leq n \leq p-1} n! = \sum_{0 \leq n \leq p-1} (p-n-1)! = \sum_{0 \leq n \leq p-1} \begin{bmatrix} p-n \\ 1 \end{bmatrix}.$$

Grâce aux congruences du paragraphe 3, on obtient le

**THÉORÈME 4.1.**— Soit  $p$  un nombre premier impair; alors

$$\kappa_p \equiv \sum_{0 \leq n \leq p-1} \begin{Bmatrix} p-1 \\ n \end{Bmatrix} - 1 \equiv B_{p-1} - 1 \pmod p.$$

La conjecture suivante constitue alors un corollaire équivalent à l'hypothèse de Kurepa.

**CONJECTURE 4.1.**— Pour  $p$  premier impair, le  $(p-1)$ -ième nombre de Bell  $B_{p-1}$  n'est jamais congru à 1 modulo  $p$ .

Les mêmes congruences permettent d'exprimer

$$\begin{aligned} \kappa_p(x) &= \sum_{0 \leq n \leq p-1} (-1)^n (x)_n = \sum_{0 \leq n \leq p-1} (-1)^n \sum_{0 \leq k \leq n} (-1)^{n-k} \begin{bmatrix} n \\ k \end{bmatrix} x^k \\ &= \sum_{0 \leq k \leq p-1} \sum_{k \leq n \leq p-1} (-1)^k \begin{bmatrix} n \\ k \end{bmatrix} x^k \\ &\equiv 1 + \sum_{1 \leq k \leq p-1} \sum_{1 \leq m \leq p-k} (-1)^k \begin{Bmatrix} p-k \\ m \end{Bmatrix} x^k \pmod{p\mathbb{Z}_p[x]} \end{aligned}$$

et au total

$$\kappa_p(x) \equiv 1 + \sum_{1 \leq k \leq p-1} (-1)^k B_{p-k} x^k \pmod{p\mathbb{Z}_p[x]}.$$

On retrouve

$$\kappa_p = \kappa_p(-1) \equiv \sum_{0 \leq k \leq p-1} B_k \equiv B_{p-1} - 1 \pmod p.$$

Revenons maintenant aux polynômes de Bell  $B_n(x) = \sum_{0 \leq k \leq n} \begin{Bmatrix} n \\ k \end{Bmatrix} x^k$  qui vérifient  $B_n(1) = B_n$ . On va démontrer une congruence pour des sommes partielles de factorielles.

PROPOSITION 4.1.— Soit  $p$  un nombre premier impair ; alors

$$\sum_{0 \leq i \leq k-1} i! \equiv (-1)^{k-1} B_{p-1}^{(k)}(1) + \kappa_p \pmod{p\mathbb{Z}_p} \quad (1 \leq k \leq p)$$

ou de manière équivalente

$$\sum_{k \leq i \leq p-1} i! \equiv (-1)^k B_{p-1}^{(k)}(1) \pmod{p\mathbb{Z}_p} \quad (1 \leq k \leq p).$$

PREUVE.— Les propriétés 1) et 2) permettent d'obtenir la formule

$$1 + x^{p-1} \equiv B_{p-1}(x) + B'_{p-1}(x) \pmod{p\mathbb{Z}_p[x]}$$

ou en d'autres termes

$$B'_{p-1}(x) \equiv 1 - B_{p-1}(x) + x^{p-1} \pmod{p\mathbb{Z}_p[x]}.$$

En dérivant successivement cette expression, on obtient

$$B_{p-1}^{(k)}(x) \equiv (-1)^{k-1} \left( \sum_{0 \leq i \leq k-1} i! x^{p-i-1} - B_{p-1}(x) + 1 \right) \pmod{p\mathbb{Z}_p[x]},$$

pour  $1 \leq k \leq p$ . En  $x = 1$ , cela donne l'expression

$$\sum_{0 \leq i \leq k-1} i! \equiv (-1)^{k-1} B_{p-1}^{(k)}(1) + B_{p-1} - 1 \pmod{p\mathbb{Z}_p}, \quad (1 \leq k \leq p)$$

dont on tire le résultat souhaité. □

## 5 Sommes de factorielles selon B. Dragovich

On fera appel ici à quelques résultats de B. Dragovich [5], [6].

### 5.1 Sommes infinies

Considérons les séries

$$S_\nu(f) = \sum_{n \geq 0} (n!)^\nu f(n), \quad \nu \geq 1,$$

où  $f \in \mathcal{F}$  est une fonction  $\mathbb{N} \rightarrow \mathbb{Z}_p$  ou une fonction bornée  $\mathbb{N} \rightarrow \mathbb{Q}_p$  (pour assurer la convergence de la série dans  $\mathbb{Q}_p$ ). Soient les opérateurs

$$\sigma_\nu: \mathcal{F} \rightarrow \mathcal{F} \quad \text{et} \quad \tau: \mathcal{F} \rightarrow \mathcal{F}$$

$$f(n) \mapsto n^\nu f(n) \quad \quad \quad f(n) \mapsto f(n+1);$$

on pose encore  $T_\nu := \tau\sigma_\nu - I$  où  $I$  est l'opérateur identité.

FORMULE DE SOMMATION.- Soit  $g \in \mathcal{F}$ ; on a

$$S_\nu(T_\nu g) = -g(0);$$

en d'autres termes

$$\sum_{n \geq 0} (n!)^\nu ((n+1)^\nu g(n+1) - g(n)) = -g(0).$$

PREUVE.- On calcule simplement

$$\begin{aligned} S_\nu(g) &= g(0) + \sum_{n \geq 1} (n!)^\nu g(n) \\ &= g(0) + \sum_{n \geq 0} (n!)^\nu (n+1)^\nu g(n+1) = g(0) + S_\nu(\tau\sigma_\nu g). \quad \square \end{aligned}$$

COROLLAIRE 5.1.- S'il existe  $g \in \mathcal{F}$  telle que  $f(n) = (n+1)^\nu g(n+1) - g(n)$ , c'est-à-dire si  $f$  est dans l'image de l'opérateur  $T_\nu$ , alors on peut calculer la somme

$$S_\nu(f) = \sum_{n \geq 0} (n!)^\nu f(n) = -g(0).$$

Étudions l'image de l'opérateur  $T_\nu$  dans le cas où  $f$  est un polynôme à coefficients dans  $\mathbb{Q}$ . Si le polynôme  $g \in \mathbb{Q}[x]$  vérifie  $g \in \text{Im } T_\nu$ , alors  $S_\nu(g)$  est rationnelle!

PROPOSITION 5.1.- La codimension de l'image de  $T_\nu : \mathbb{Q}[x] \rightarrow \mathbb{Q}[x]$  vaut

$$\text{Codim}(\text{Im } T_\nu) = \nu.$$

PREUVE.- L'image par  $T_\nu$  du polynôme de base  $f_k(n) = n^k$  ( $\text{deg } f_k = k$ ) vaut  $T_\nu f_k = (n+1)^{k+\nu} - n^k$  et  $\text{deg}(T_\nu f_k) = k + \nu$ .  $\square$

REMARQUE.- L'élément  $f_0(n) = 1$  n'est pas dans  $\text{Im } T_1$ ; en particulier on ne peut rien dire de  $\sum_{n \geq 0} n! \dots$

CAS PARTICULIER.- Soit  $f(n) = \zeta^n g(n)$ , où  $g \in \mathcal{F}$  et  $\zeta \in \mu_{p-1} \subset \mathbb{Z}_p$  est une racine  $(p-1)$ -ième de l'unité. On regarde alors la somme

$$S_{\zeta, \nu}(g) := S_\nu(f) = \sum_{n \geq 0} (n!)^\nu \zeta^n g(n)$$

et l'opérateur  $T_{\zeta, \nu} = \tau\sigma_{\zeta, \nu} - I$  où  $\sigma_{\zeta, \nu} g(n) = \zeta^n g(n)$ . Construisons la matrice  $M_n^{\zeta, \nu}$  de  $T_{\zeta, \nu} |_{\mathbb{Q}_{<n-\nu+1}[x]}$ , de taille  $(n+1) \times (n-\nu+1)$ ; on a

$$T_{\zeta, \nu}(x^{k-\nu}) = \zeta(x+1)^k - x^{k-\nu} = \zeta \sum_{0 \leq i \leq k} \binom{k}{i} x^i - x^{k-\nu}$$

d'où

$$M_n^{\zeta, \nu} = \begin{pmatrix} \zeta - 1 & \zeta & \zeta & \dots & \dots & \dots & \dots & \zeta \\ \zeta \binom{\nu}{1} & \zeta \binom{\nu+1}{1} - 1 & \zeta \binom{\nu+2}{1} & \dots & \dots & \dots & \dots & \zeta \binom{n}{1} \\ \zeta \binom{\nu}{2} & \zeta \binom{\nu+1}{2} & \zeta \binom{\nu+2}{2} - 1 & \dots & \dots & \dots & \dots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & & & & & \vdots \\ \zeta \binom{\nu}{\nu-1} & & & & & & & \vdots \\ \zeta & \dots & \dots & \dots & \dots & \dots & \dots & \zeta \binom{n}{n-\nu-1} \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & \zeta \binom{n}{n-\nu} - 1 \\ \vdots & \dots & \dots & \dots & \dots & \dots & \dots & \zeta \binom{n}{n-\nu+1} \\ \vdots & \dots & \dots & \dots & \dots & \dots & \dots & \zeta \binom{n}{n-\nu+2} \\ \vdots & & & & & & & \vdots \\ \vdots & & & & & & & \vdots \\ \vdots & & & & & & & \zeta \binom{n}{n-1} \\ 0 & \dots & \dots & \dots & \dots & \dots & 0 & \zeta \end{pmatrix}$$

Dans le cas particulier où  $\nu = 1$ , on obtient alors une matrice  $M_n^\zeta$  de taille  $(n+1) \times n$  que des opérations élémentaires de ligne permettent de mettre sous la forme

$$M_n^\zeta \sim \begin{pmatrix} u_1^\zeta & u_2^\zeta & \dots & \dots & u_n^\zeta \\ \zeta & 0 & \dots & \dots & 0 \\ 0 & \zeta^2 & 0 & \dots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & 0 \\ 0 & \dots & \dots & \dots & \zeta^n \end{pmatrix};$$

On obtient alors une base de l'image  $Q_k(x) = \zeta^k n^k + u_k^\zeta$  où  $u_k^\zeta$  est donné par la relation de récurrence

$$\begin{cases} u_1^\zeta = \zeta - 1 \\ u_{n+1}^\zeta = u_n^\zeta - \sum_{1 \leq i \leq n} \binom{n+1}{i} \zeta^{n+1-i} u_i^\zeta + \zeta^{n+1}. \end{cases}$$

En posant  $u_0^\zeta = -1$ , on écrit aussi cette suite

$$u_0^\zeta = -1, \quad u_1^\zeta = \zeta - 1 \quad \text{et} \quad u_{n+1}^\zeta = u_n^\zeta - \sum_{0 \leq i \leq n} \binom{n+1}{i} \zeta^{n+1-i} u_i^\zeta,$$

$$\text{i.e. } u_n^\zeta = \sum_{0 \leq i \leq n+1} \binom{n+1}{i} \zeta^{n-i+1} u_i^\zeta = {}^u(u^\zeta + \zeta)^{n+1} \quad (n \geq 1).$$

De là, on calcule la suite  $(v_k^\zeta)_{k \geq 1}$  vérifiant

$$\sum_{n \geq 0} \zeta^n n! (\zeta^k n^k + u_n^\zeta) = v_k^\zeta.$$

On obtient

$$\left\{ \begin{array}{l} v_0^\zeta = 0, \quad v_1^\zeta = -1 \quad \text{et} \quad v_{n+1}^\zeta = v_n^\zeta - \sum_{0 \leq i \leq n} \binom{n+1}{i} \zeta^{n-i+1} v_i^\zeta, \\ \text{i.e. } v_n^\zeta = \sum_{0 \leq i \leq n+1} \binom{n+1}{i} \zeta^{n-i+1} v_i^\zeta = {}^v(v^\zeta + \zeta)^{n+1} \quad (n \geq 1). \end{array} \right.$$

Les cas  $\zeta = \pm 1$  sont étudiés dans [5], [6]. Pour  $\zeta = 1$ , on trouve les suites d'entiers  $(u_k)_{k \geq 1}$  et  $(v_k)_{k \geq 1}$  qui vérifient

$$\sum_{n \geq 0} n! (n^k + u_n) = v_k.$$

Dans ce cas particulier, explicitons les premières paires  $(u_k, v_k)$  et quelques égalités auxquelles elles donnent lieu

$k$	1	2	3	4	5	6	7	8	9	10
$u_k$	0	1	-1	-2	9	-9	-50	267	-413	-2180
$v_k$	-1	1	1	-5	5	21	-105	141	777	-5513

d'où

- 1)  $\sum_{n \geq 0} n! n = -1$
- 2)  $\sum_{n \geq 0} n! (n^2 + 1) = 1$
- 3)  $\sum_{n \geq 0} n! (n^3 - 1) = 1$
- 4)  $\sum_{n \geq 0} n! (n^4 - 2) = -5$
- 5)  $\sum_{n \geq 0} n! (n^5 + 9) = 5.$

REMARQUE.— L. van Hamme nous a signalé que, pour  $\zeta = -1$ , on obtient des paires  $(\tilde{u}_k, \tilde{v}_k)$  faisant intervenir les nombres de Bell. Les premières valeurs sont en effet

$k$	0	1	2	3	4	5	6	7	8	9
$\tilde{u}_k$	-1	-2	-5	-15	-52	-203	-877	-4140	-21147	-115975
$\tilde{v}_k$	0	-1	-3	-9	-31	-121	-523	-2469	-12611	-69161

et l'on observe que

$$\tilde{u}_k = -B_{k+1} \quad (k \geq 0).$$

Par conséquent, la somme

$$\sum_{n \geq 0} (-1)^n n! (n^k + (-1)^{k+1} B_{k+1}) = \tilde{v}_k$$

est rationnelle pour tout  $k \geq 1$ .

Considérons maintenant l'équation sous sa forme générale

$$\sum_{n \geq 0} n! (C_k n^k + C_{k-1} n^{k-1} + \dots + C_0) = D_k, \quad C_0, \dots, C_k, D_k \in \mathbb{Q}.$$

PROPOSITION 5.2.— L'équation ci-dessus est vérifiée pour  $C_0 = \sum_{1 \leq j \leq k} C_j u_j$  et  $D_k = \sum_{1 \leq j \leq k} C_j v_j$ .

REMARQUE.— Les résultats sont analogues pour  $\zeta = -1$ .

Tout le problème de l'irrationalité de  $\sum_{n \geq 0} n!$  réside dans la question de l'unicité de la paire  $(u_k, v_k)$  ( $k \geq 1$ ). On démontre aisément les trois résultats suivants.

PROPOSITION 5.3.— S'il existe  $k \geq 1$  tel que  $(u_k, v_k)$  n'est pas unique dans  $\mathbb{Q}$ , alors  $\sum_{n \geq 0} n!$  est rationnelle dans  $\mathbb{Q}_p$ .

PROPOSITION 5.4.— Si  $\sum_{n \geq 0} n!$  est rationnelle, alors  $\sum_{n \geq 0} n^k n!$  est rationnelle pour tout  $k \geq 1$ .

PROPOSITION 5.5.— Si (par exemple)  $(u_2, v_2) = (1, 1)$  est l'unique solution rationnelle de  $\sum_{n \geq 0} n!(n^2 + u_2) = v_2$ , alors  $\sum_{n \geq 0} n!$  est irrationnelle.

## 5.2 Sommes finies

On obtient des résultats analogues pour des sommes finies du type

$$S_{n,\nu}(f) = \sum_{0 \leq i \leq n-1} (i!)^\nu f(i), \quad \nu \geq 1,$$

FORMULE DE SOMMATION.— Soit  $g \in \mathcal{F}$ ; on a

$$S_{n,\nu}(T_\nu g) = -g(0) + (n!)^\nu g(n);$$

en d'autres termes

$$\sum_{0 \leq i \leq n-1} (i!)^\nu ((i+1)^\nu g(i+1) - g(i)) = -g(0) + (n!)^\nu g(n).$$

PREUVE.— On a en fait

$$\begin{aligned} S_{n,\nu}(g) &= g(0) + \sum_{1 \leq i \leq n-1} (i!)^\nu g(i) \\ &= g(0) + \sum_{0 \leq i \leq n-1} (i!)^\nu (i+1)^\nu g(i+1) - (n!)^\nu g(n) \\ &= g(0) + S_{n,\nu}(\tau \sigma_\nu g) - (n!)^\nu g(n). \quad \square \end{aligned}$$

COROLLAIRE 5.2.— Si  $p$  est un nombre premier et  $g$  prend ses valeurs dans  ${}_{\epsilon} \mathbf{Z}_p$ , alors on a

$$S_{p,\nu}(T_\nu g) \equiv -g(0) \pmod{p^\nu \mathbf{Z}_p},$$

c'est-à-dire

$$\sum_{0 \leq n \leq p-1} (n!)^\nu ((n+1)^\nu g(n+1) - g(n)) \equiv -g(0) \pmod{p \mathbf{Z}_p}.$$

CAS PARTICULIER.— Soit  $f(n) = \varepsilon^n g(n)$ , où  $g \in \mathcal{F}$  et  $\varepsilon$  est l'élément de  $\mathbf{F}_p^\times$  vérifiant  $\zeta \equiv \varepsilon \pmod{p}$ ,  $\zeta \in \mu_{p-1} \subset \mathbf{Z}_p$ . On regarde alors la somme

$$S_{n,\varepsilon,\nu}(g) = \sum_{0 \leq i \leq n-1} (i!)^\nu \varepsilon^i g(i).$$

REMARQUE.— Les suites  $(u_k^\varepsilon)$  et  $(v_k^\varepsilon)$  étudiées précédemment vérifient évidemment

$$\sum_{0 \leq n \leq p-1} n! \varepsilon^n (\varepsilon^k n^k + u_k^\varepsilon) \equiv v_k^\varepsilon \pmod{p}.$$

B. Dragovich [6] traite du cas particulier où  $\nu = 1$ ,  $\varepsilon = \pm 1$  et  $f$  est un polynôme à coefficients dans  $\mathbf{Q}$ . Pour  $\varepsilon = 1$ , soit  $P_k(i) = i^k + u_k \in \text{Im } T_1$ ,  $u_k \in \mathbf{Q}$ , i.e. il existe  $A_{k-1} \in \mathbf{Q}[X]$  tel que

$$i^k + u_k = (i+1)A_{k-1}(i+1) - A_{k-1}(i);$$

on a alors  $u_k = A_{k-1}(1) - A_{k-1}(0)$  et la somme

$$\sum_{0 \leq i \leq n-1} i!(i^k + u_k) = -A_{k-1}(0) + n!A_{k-1}(n)$$

est entièrement déterminée par le polynôme  $A_{k-1}$ .

REMARQUE.- Pour  $n \rightarrow \infty$ , on retrouve la formule

$$\sum_{i \geq 0} i!(i^k + u_k) = -A_{k-1}(0) = u_k$$

du paragraphe précédent.

Posons  $\sigma_k(n) = \sum_{0 \leq i \leq n-1} i!i^k$ ,  $k \in \mathbb{N}$ .

THÉORÈME 5.1.- *La relation de récurrence*

$$\sigma_{k+1}(n) = -k\sigma_k(n) - \sum_{0 \leq l \leq k-1} \binom{k+1}{l} \sigma_l(n) + n!n^k$$

est valable pour  $k \geq 1$ .

Cette formule permet également d'obtenir les relations de récurrence pour  $u_k$ ,  $v_k$  et  $A_{k-1}(n)$ . Les premières valeurs donnent lieu aux identités

- 1)  $\sum_{0 \leq i \leq n-1} i!i = -1 + n!$
- 2)  $\sum_{0 \leq i \leq n-1} i!(i^2 + 1) = 1 + n!(n-1)$
- 3)  $\sum_{0 \leq i \leq n-1} i!(i^3 - 1) = 1 + n!(n^2 - 2n - 1)$
- 4)  $\sum_{0 \leq i \leq n-1} i!(i^4 - 2) = -5 + n!(n^3 - 3n^2 + 5)$

THÉORÈME 5.2.- *Soit  $P_k(i) = \sum_{0 \leq r \leq k} C_r i^r$ ,  $C_r \in \mathbb{Q}$ ; alors la relation*

$$\sum_{0 \leq i \leq n-1} i!P_k(i) = v_k + n!Q_{k-1}(n)$$

est valable lorsque  $C_0 = \sum_{1 \leq r \leq k} C_r u_r$ ,  $v_k = \sum_{1 \leq r \leq k} C_r v_r$  et  $Q_{k-1}(n) = \sum_{1 \leq r \leq k} C_r A_{r-1}(n)$ .

Observons encore quelques relations de congruence. On a

$$\sum_{0 \leq i \leq n-1} i!(i^k + u_k) = v_k + n!A_{k-1}(n) \equiv v_k \pmod{n!}.$$

On voit que les propriétés de divisibilité de  $\sum_{0 \leq i \leq n-1} i!$  par les facteurs de  $n!$  sont liées à celles de  $\sum_{0 \leq i \leq n-1} i! i^k$  sauf si  $u_k$  est nul, i.e. si  $A_{k-1}(1) = A_{k-1}(0)$  (ce qui ne semble être le cas que si  $k = 1$ ).

On va énoncer des résultats équivalents à l'hypothèse de Kurepa dont la plupart figurent dans [6]. L'entier  $p$  désigne un nombre premier impair.

Considérons la matrice

$$M = \begin{pmatrix} -2 & 2 & 0 & \dots & \dots & \dots & 0 \\ -1 & -1 & 3 & 0 & \dots & \dots & 0 \\ -1 & 0 & -1 & 4 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & & \ddots & \ddots & \ddots & 0 \\ -1 & 0 & \dots & \dots & 0 & -1 & p-1 \\ -1 & 0 & \dots & \dots & \dots & 0 & -1 \end{pmatrix} \quad \text{de taille } (p-1) \times (p-1).$$

**THÉORÈME 5.3.**— *Les assertions suivantes sont équivalentes.*

- i) L'hypothèse de Kurepa est vraie,
- ii)  $\det M \not\equiv 0 \pmod p$ ,
- iii)  $v_{p-1} \not\equiv -1 \pmod p$ ,
- iv)  $v_p \not\equiv -1 \pmod p$ ,
- v) il existe  $k \geq 1$  tel que  $u_k \not\equiv 0 \pmod p$  et  $\sum_{0 \leq i \leq p-1} i! i^k \not\equiv v_k \pmod p$ .

PREUVE.— i)  $\Leftrightarrow$  ii) : Un calcul montre que

$$\det M = \sum_{0 \leq i \leq p-1} i! = \kappa_p.$$

i)  $\Leftrightarrow$  v) : Cette équivalence découle de la relation

$$\sum_{0 \leq i \leq p-1} i!(i^k + u_k) = \sum_{0 \leq i \leq p-1} i! i^k + u_k \kappa_p \equiv v_k \pmod p.$$

iii)  $\Rightarrow$  i) : Si l'hypothèse de Kurepa est fautive, alors  $\kappa_p \equiv 0 \pmod p$  et

$$\sum_{0 \leq i \leq p-1} i! i^{p-1} \equiv v_{p-1} \pmod p.$$

Grâce au petit théorème de Fermat, on obtient

$$v_{p-1} \equiv \sum_{0 \leq i \leq p-1} i! i^{p-1} \equiv \sum_{0 \leq i \leq p-1} i! - 1 \equiv \kappa_p - 1 \equiv -1 \pmod p.$$

iii)  $\iff$  iv) : La relation de récurrence définissant la suite  $(v_k)$  fournit

$$v_p = v_{p-1} - \sum_{1 \leq i \leq p-1} \binom{p}{i} v_i \equiv v_{p-1} \pmod{p}.$$

i)  $\implies$  iv) : Cette dernière implication sera démontrée à l'aide du calcul ombral dans le paragraphe 6.1.  $\square$

## 6 Calcul ombral

Soit  $A$  un anneau ( $A = \mathbf{Z}$  ou  $\mathbf{Z}_p$ ); considérons l'opérateur linéaire

$$\begin{aligned} \Phi : A[[x]] &\longrightarrow A[[x]] \\ (x)_n &\longmapsto x^n \end{aligned}$$

pour lequel on a  $\Phi(x^n) = B_n(x)$  ( $n$ -ième polynôme de Bell) (voir [7]). Reprenons  $f(x) = \sum_{n \geq 0} (-1)^n (x)_n$ ; alors

$$\Phi f(x) = \sum_{n \geq 0} (-1)^n x^n = \frac{1}{1+x}$$

et

$$\Phi \kappa_p(x) = \sum_{0 \leq n \leq p-1} (-x)^n = \frac{1+x^p}{1+x} \quad (p \text{ impair});$$

modulo  $p$ , on obtient

$$\Phi \kappa_p(x) \equiv (1+x)^{p-1} \pmod{p \mathbf{Z}_p[x]}.$$

D'autre part, comme  $\kappa_p(x) \equiv 1 + \sum_{1 \leq k \leq p-1} (-1)^k B_{p-k} x^k \pmod{p \mathbf{Z}_p[x]}$ , on a

$$\Phi \kappa_p(x) \equiv 1 + \sum_{1 \leq k \leq p-1} (-1)^k B_{p-k} B_k(x) \pmod{p \mathbf{Z}_p[x]},$$

d'où la relation

$$(1+x)^{p-1} \equiv 1 + \sum_{1 \leq k \leq p-1} (-1)^k B_{p-k} B_k(x) \pmod{p \mathbf{Z}_p[x]}.$$

## 6.1 Une autre application

Pour  $\alpha, \beta \in \mathbb{Z}_p$  et  $\varepsilon \in \{0, \dots, p-1\}$ , considérons la suite

$$a_0^\varepsilon = \alpha, \quad a_1^\varepsilon = \beta \quad \text{et} \quad a_{n+1}^\varepsilon = a_n^\varepsilon - \sum_{0 \leq i \leq n} \binom{n+1}{i} \varepsilon^{n-i+1} a_i^\varepsilon, \quad n \geq 1$$

i.e.  $a_n^\varepsilon = "(a^\varepsilon + \varepsilon)^{n+1}"$ ,  $n \geq 1$ .

Soit  $\psi_\varepsilon : \mathbb{Z}_p[x] \rightarrow \mathbb{Z}_p$  l'opérateur linéaire défini par

$$\psi_\varepsilon(x^k) = a_k^\varepsilon \quad (k \geq 0).$$

Alors

$$\psi_\varepsilon((x + \varepsilon)^{n+1}) = \sum_{0 \leq i \leq n+1} \binom{n+1}{i} \varepsilon^{n-i+1} a_i^\varepsilon = a_n^\varepsilon = \psi_\varepsilon(x^n), \quad n \geq 1.$$

(Pour  $n = 0$ ,  $\psi_\varepsilon(1) = a_0^\varepsilon = \alpha$  et  $\psi_\varepsilon(x + \varepsilon) = \varepsilon\alpha + \beta$ .)

Posons  $P(x) = \sum_{0 \leq n \leq m} c_n x^n \in \mathbb{Z}_p[x]$ ; alors

$$\begin{aligned} \psi_\varepsilon((x + \varepsilon)P(x + \varepsilon)) &= \psi_\varepsilon\left(\sum_{0 \leq n \leq m} c_n (x + \varepsilon)^{n+1}\right) \\ &= c_0(\varepsilon\alpha + \beta) + \psi_\varepsilon\left(\sum_{1 \leq n \leq m} c_n x^n\right) \\ &= c_0(\varepsilon\alpha + \beta) + \psi_\varepsilon(P(x)) - c_0\alpha \\ &= (\alpha(\varepsilon - 1) + \beta)P(0) + \psi_\varepsilon(P(x)). \end{aligned}$$

Pour  $P(x) = (x + \varepsilon)(x + 2\varepsilon) \dots (x + (n-1)\varepsilon)$  ( $n \geq 1$ ), on a  $P(0) = \varepsilon^{n-1}(n-1)!$  et  $(x + \varepsilon)P(x + \varepsilon) = (x + \varepsilon)(x + 2\varepsilon) \dots (x + n\varepsilon)$ . Ainsi

$$\begin{aligned} \psi_\varepsilon((x + \varepsilon) \dots (x + n\varepsilon)) &= \psi_\varepsilon((x + \varepsilon) \dots (x + (n-1)\varepsilon)) \\ &\quad + (\alpha(\varepsilon - 1) + \beta) \varepsilon^{n-1}(n-1)! \\ &= \psi_\varepsilon((x + \varepsilon) \dots (x + (n-2)\varepsilon)) \\ &\quad + [\varepsilon^{n-2}(n-2)! + \varepsilon^{n-1}(n-1)!](\alpha(\varepsilon - 1) + \beta) \\ &= \dots \\ &= \psi_\varepsilon(x + \varepsilon) + (\alpha(\varepsilon - 1) + \beta) \sum_{1 \leq k \leq n-1} \varepsilon^k k! \\ &= \alpha + (\alpha(\varepsilon - 1) + \beta) \sum_{0 \leq k \leq n-1} \varepsilon^k k!. \end{aligned}$$

Pour  $n = p$ , on obtient

$$\begin{aligned}\psi_\varepsilon((x + \varepsilon) \dots (x + p\varepsilon)) &\equiv \psi_\varepsilon(x^p - x) \pmod{p} \\ &\equiv a_p^\varepsilon - \beta \pmod{p}\end{aligned}$$

et donc

$$a_p^\varepsilon \equiv \alpha + \beta + (\alpha(\varepsilon - 1) + \beta) \cdot \sum_{0 \leq k \leq p-1} \varepsilon^k k! \pmod{p}.$$

Les mêmes calculs, effectués avec la suite  $(b_n^\varepsilon)_{n \geq 0}$  définie par

$$b_0^\varepsilon = \alpha, b_1^\varepsilon = \beta \text{ et } b_{n+1}^\varepsilon = \sum_{0 \leq i \leq n} \binom{n}{i} \varepsilon^{n-i} b_i^\varepsilon = {}^u (b^\varepsilon + \varepsilon)^n \quad (n \geq 1)$$

au lieu de la suite  $(a_n^\varepsilon)_{n \geq 0}$ , conduisent au résultat analogue

$$b_p^\varepsilon \equiv \alpha + \beta + (\beta - \alpha) \sum_{0 \leq k \leq p-1} (-1)^k \varepsilon^k k! \pmod{p}.$$

CAS PARTICULIERS.- 1)  $a_0^\varepsilon = -1, a_1^\varepsilon = \varepsilon - 1$  : on a  $a_k^\varepsilon = u_k^\varepsilon$  et

$$u_p^\varepsilon \equiv \varepsilon - 2 \pmod{p}.$$

2)  $a_0^\varepsilon = 0, a_1^\varepsilon = -1$  : on a  $a_k^\varepsilon = v_k^\varepsilon$  et

$$v_p^\varepsilon \equiv -1 - \sum_{0 \leq k \leq p-1} \varepsilon^k k! \pmod{p} \text{ ou encore } \sum_{k=0}^{p-1} \varepsilon^k k! \equiv -1 - v_p^\varepsilon \pmod{p}.$$

N.B. Les suites  $(u_k^\varepsilon)_{k \geq 1}$  et  $(v_k^\varepsilon)_{k \geq 1}$  satisfait

$$\sum_{0 \leq n \leq p-1} \varepsilon^n n! (\varepsilon^k n^k + u_k^\varepsilon) = v_k^\varepsilon.$$

Pour  $\varepsilon = 1$ , on retrouve les suites  $(u_i)$  et  $(v_i)$  de Dragovich, qui vérifient

$$u_p \equiv -1 \pmod{p} \text{ et } v_p \equiv -1 - \kappa_p \pmod{p}.$$

Cela montre que l'énoncé  $v_p \not\equiv -1 \pmod{p}$  est équivalent à l'hypothèse de Kurepa et achève ainsi la preuve du théorème 5.3.

3)  $\alpha = \beta \neq 0$  : alors

$$b_p^\varepsilon \equiv 2\alpha \pmod{p} \quad (\text{indépendamment de } \varepsilon).$$

Pour  $\alpha = \beta = \varepsilon = 1$ , on obtient la suite des nombres de Bell  $(B_n)_{n \geq 0}$  pour laquelle

$$B_p \equiv 2 \pmod{p}.$$

4)  $\beta = \alpha + 1$  : alors

$$b_p^\varepsilon - 2\alpha - 1 \equiv \sum_{0 \leq k \leq p-1} (-1)^k \varepsilon^k k! \pmod{p}.$$

## 7 Polynômes de Bell-Carlitz

À l'aide du calcul ombrial, nous allons montrer que la congruence

$$B_{np} \equiv B_{n+1} \pmod{npZ_p}$$

pour les nombres de Bell [7] s'étend à la généralisation de Carlitz des nombres de Bell.

### 7.1 Quelques congruences polynomiales

Soient  $p$  un nombre premier et  $P(x, y), Q(x, y) \in A[x, y]$  des polynômes à coefficients dans l'anneau  $A = \mathbf{Z}$  ou  $\mathbf{Z}_p$ .

LEMME 7.1.- Si  $P(x, y) \equiv Q(x, y) \pmod{p^r A[x, y]}$ , alors

$$P(x, y)^p \equiv Q(x, y)^p \pmod{p^{r+1} A[x, y]}.$$

Prenons maintenant un polynôme à une variable  $P(y) \in A[y]$ , et considérons le produit de  $p$  termes décalés

$$P(y)P(y - p^r) \dots P(y - (p-1)p^r) = \prod_{0 \leq k < p} P(y - kp^r).$$

LEMME 7.2.- Si  $p$  est un nombre premier impair, alors la congruence suivante est vérifiée

$$\prod_{0 \leq k < p} P(y - kp^r) \equiv P(y)^p \pmod{p^{r+1} A[y]}.$$

Considérons maintenant les polynômes de Pochhammer  $(y)_n$  ( $n \geq 0$ ), qui forment une base du module  $A[y]$ .

LEMME 7.3.- Pour  $\nu \geq 1$ , et  $p$  un nombre premier impair, les polynômes  $(y)_{p^\nu} = y(y-1)\dots(y-p^\nu+1)$  vérifient la congruence

$$(y)_{p^\nu} \equiv (y^p - y)^{p^{\nu-1}} \pmod{p^\nu A[y]}.$$

Les preuves de ces trois lemmes se trouvent dans [7].

LEMME 7.4.- Soit  $\nu \geq 1$  et  $p$  un nombre premier impair; dans l'espace des polynômes à deux variables, la congruence suivante est vérifiée

$$((x+y)^p - (x^p + y))^p \equiv (y^p - y)^{p^\nu} \pmod{p^{\nu+1} A[x, y]}.$$

PREUVE.- On a la congruence

$$(x+y)^p - (x^p + y) \equiv y^p - y \pmod{pA[x, y]}.$$

Le résultat souhaité découle alors directement du lemme 7.1. □

## 7.2 Calcul ombra

Sur le module  $A[x, y]$ , dont la famille  $\{x^i(y)^j, i, j \geq 0\}$  forme une base, on définit un opérateur linéaire  $\Psi$  par

$$\begin{aligned} \Psi : A[x, y] &\longrightarrow A[x] \\ x^i(y)^j &\longmapsto x^i. \end{aligned}$$

Sur  $A[x, y]$ , considérons la relation d'équivalence, notée  $\stackrel{\nu}{\sim}$ , définie par

$$f \stackrel{\nu}{\sim} g \text{ si et seulement si } \Psi(f) \equiv \Psi(g) \pmod{p^\nu A[x]}.$$

LEMME 7.5.- Si  $S, T : A[x, y] \longrightarrow A[x, y]$  sont deux opérateurs linéaires qui commutent et  $\nu \geq 1$  un entier tels que  $Sf \stackrel{\nu}{\sim} Tf$  pour toute  $f \in A[x, y]$ , alors  $S^k f \stackrel{\nu}{\sim} T^k f$  pour tout  $k \in \mathbb{N}$  et pour toute  $f \in A[x, y]$ .

PREUVE.- Procédons par induction sur  $k$ . Le cas  $k = 1$  correspond à l'hypothèse du lemme. Supposons alors que l'équivalence  $S^{k-1}f \stackrel{\nu}{\sim} T^{k-1}f$  est vraie pour toute  $f \in A[x, y]$ . Alors

$$S^k f = S^{k-1} S f \stackrel{\nu}{\sim} T^{k-1} S f = S T^{k-1} f \stackrel{\nu}{\sim} T T^{k-1} f = T^k f. \quad \square$$

LEMME 7.6.- Pour tout  $n \in \mathbf{N}$  et toute  $f \in A[x, y]$ , on a l'égalité

$$\Psi((y)_n f(x, y - n)) = \Psi(f(x, y)).$$

PREUVE.- On a  $x^i(y)_{n+k} = x^i(y)_n (y - n)_k$ , d'où

$$\Psi((y)_n x^i (y - n)_k) = \Psi(x^i (y)_{n+k}) = x^i = \Psi(x^i (y)_k).$$

Or, la fonction  $f$  peut s'écrire  $f(x, y) = \sum_{i,k} a_{i,k} x^i (y)_k$ ; des égalités précédentes on tire ainsi

$$\Psi((y)_n f(x, y - n)) = \Psi(f(x, y)). \quad \square$$

LEMME 7.7.- Si  $p$  est un nombre premier impair,  $\nu \geq 1$  un entier et  $f \in A[x, y]$ , alors la congruence suivante est vérifiée

$$f \stackrel{p^\nu}{\sim} ((x + y)^p - (x^p + y))^p f.$$

PREUVE.- Dans le lemme 7.6, posons  $n = p^\nu$  et réduisons l'égalité modulo  $p^\nu$ . On obtient

$$(y)_{p^\nu} f \stackrel{p^\nu}{\sim} f.$$

D'autre part, le lemme 7.3 énonce la congruence

$$(y)_{p^\nu} \equiv (y^p - y)^{p^{\nu-1}} \pmod{p^\nu A[y]};$$

on en tire  $f \stackrel{p^\nu}{\sim} (y^p - y)^{p^{\nu-1}} f$ , et le lemme 7.4 permet de conclure.  $\square$

THÉORÈME 7.1.- Si  $f \in A[x, y]$ ,  $\nu \geq 1$  et  $p$  est un nombre premier impair, alors la congruence suivante est vérifiée

$$(x + y)^{p^\nu} f \stackrel{p^\nu}{\sim} (x^p + 1 + y)^{p^{\nu-1}} f.$$

PREUVE.- Nous allons procéder par induction sur  $\nu$ . Pour  $\nu = 1$ , le lemme 7.7 donne  $f \stackrel{p}{\sim} ((x + y)^p - (x^p + y)) f$ , formule dont on tire immédiatement

$$(x + y)^p f \stackrel{p}{\sim} (x^p + 1 + y) f.$$

Supposons maintenant que la congruence  $(x + y)^{p^n} f \stackrel{p^n}{\sim} (x^p + 1 + y)^{p^{n-1}} f$  soit valable pour tout  $n \leq \nu$  et toute  $f \in A[x, y]$ . Il s'agit de montrer que l'on a

$$(x + y)^{p^{\nu+1}} f \stackrel{p^{\nu+1}}{\sim} (x^p + 1 + y)^{p^\nu} f.$$

Du lemme 7.7, on tire

$$(*) \quad f \stackrel{p^{\nu+1}}{\sim} ((x+y)^p - (x^p+y))^p f.$$

Développons ce dernier terme à l'aide du binôme de Newton. On obtient

$$\begin{aligned} ((x+y)^p - (x^p+y))^p &= \sum_{0 \leq k \leq p^{\nu}} \binom{p^{\nu}}{k} (x+y)^{kp} (-x^p-y)^{p^{\nu}-k} \\ &= (x+y)^{p^{\nu+1}} - (x^p+y)^{p^{\nu}} + \sum_{1 \leq k \leq p^{\nu}-1} \binom{p^{\nu}}{k} (x+y)^{kp} (-x^p-y)^{p^{\nu}-k}. \end{aligned}$$

Considérons le coefficient binomial  $\binom{p^{\nu}}{k}$ . Il existe  $m$  premier à  $p$  et  $\alpha$ ,  $0 \leq \alpha < \nu$ , tels que  $k = mp^{\alpha}$ . On a alors

$$\binom{p^{\nu}}{k} = \binom{p^{\nu}}{mp^{\alpha}} = p^{\nu-\alpha} \cdot \frac{1}{m} \binom{p^{\nu}-1}{mp^{\alpha}-1} \equiv 0 \pmod{p^{\nu-\alpha}A}.$$

De plus, pour  $f(x, y) = (-x^p - y)^{p^{\nu}-k}$ , l'hypothèse d'induction et le lemme 7.5, en prenant pour  $S$  et  $T$  les opérateurs de multiplication par  $(x+y)^{p^{\alpha+1}}$ , respectivement  $(x^p+1+y)^{p^{\alpha}}$ , donnent lieu à la congruence

$$(x+y)^{kp} (-x^p-y)^{p^{\nu}-k} = (x+y)^{mp^{\alpha+1}} f \stackrel{p^{\alpha+1}}{\sim} (x^p+1+y)^{mp^{\alpha}} f = (x^p+1+y)^k f.$$

Il s'ensuit que

$$\binom{p^{\nu}}{k} (x+y)^{kp} (-x^p-y)^{p^{\nu}-k} \stackrel{p^{\nu+1}}{\sim} \binom{p^{\nu}}{k} (x^p+1+y)^k (-x^p-y)^{p^{\nu}-k}.$$

Au total, nous avons donc établi la formule

$$\sum \binom{p^{\nu}}{k} (x+y)^{kp} (-x^p-y)^{p^{\nu}-k} \stackrel{p^{\nu+1}}{\sim} \sum \binom{p^{\nu}}{k} (x^p+1+y)^k (-x^p-y)^{p^{\nu}-k}.$$

où la somme porte sur les  $k : 1 \leq k \leq p^{\nu}-1$ . Or, le membre de droite s'exprime aussi par

$$\sum_{1 \leq k \leq p^{\nu}-1} \binom{p^{\nu}}{k} (x^p+1+y)^k (-x^p-y)^{p^{\nu}-k} = 1 - (x^p+1+y)^{p^{\nu}} + (x^p+y)^{p^{\nu}}.$$

Utilisons finalement (\*), qui donne

$$\begin{aligned} f &\stackrel{p^{\nu+1}}{\sim} ((x+y)^p - (x^p+y))^p f \\ &\stackrel{p^{\nu+1}}{\sim} \left( (x+y)^{p^{\nu+1}} - (x^p+y)^{p^{\nu}} + 1 - (x^p+1+y)^{p^{\nu}} + (x^p+y)^{p^{\nu}} \right) f \\ &\stackrel{p^{\nu+1}}{\sim} (x+y)^{p^{\nu+1}} f + f - (x^p+1+y)^{p^{\nu}} f. \end{aligned}$$

Ainsi,  $(x+y)^{p^{\nu+1}} f \sim^{p^{\nu+1}} (x^p+1+y)^{p^\nu} f$  comme souhaité.  $\square$

REMARQUE.— Cette congruence est également valable pour  $p = 2$  si  $\nu = 1$ . Pour  $p = 2$  et  $\nu > 1$  a lieu la congruence

$$(x+y)^{2^\nu} \sim^{2^{\nu-1}} (x^2+1+y)^{2^{\nu-1}}.$$

En effet, on perd un facteur  $p (= 2)$  dans la preuve du lemme 7.2.

### 7.3 Les polynômes de Bell-Carlitz

Rappelons que le  $n$ -ième nombre de Bell  $B_n$  est défini par la fonction génératrice

$$e^{e^x-1} = \sum_{n \geq 0} B_n \frac{z^n}{n!}.$$

Intéressons-nous alors à une généralisation de ces nombres due à L. Carlitz (étudiée dans [13]). On définit le  $n$ -ième polynôme de Bell-Carlitz  $B_n^c(x)$  par

$$e^{xz+(e^x-1)} = \sum_{n \geq 0} B_n^c(x) \frac{z^n}{n!}.$$

On remarque alors que  $B_n = B_n^c(0)$ , et on a

$$e^{xz+(e^x-1)} = \sum_{m \geq 0} \frac{x^m z^m}{m!} \sum_{k \geq 0} B_k \frac{z^k}{k!} = \sum_{n \geq 0} \sum_{0 \leq m \leq n} \binom{n}{m} x^m B_{n-m} \frac{z^n}{n!},$$

formule dont on tire la relation

$$B_n^c(x) = \sum_{0 \leq m \leq n} \binom{n}{m} B_{n-m} x^m = "(x+B)^n".$$

En dérivant cette dernière relation, on obtient

$$B_n^c(x)' = n \cdot B_{n-1}^c(x),$$

ce qui signifie que ces polynômes forment une *famille d'Appell*. On observe par ailleurs que

$$B_n^c(1) = \sum_{0 \leq m \leq n} \binom{n}{m} B_m = B_{n+1}.$$

Reprenons maintenant l'application  $\Psi$  du paragraphe 7.2.

PROPOSITION 7.1.- L'image par  $\Psi$  de  $x^i y^j$  est  $x^i B_j$ .

PREUVE.- Dans [23], G.C.Rota montre que si  $\varphi : A[y] \rightarrow A$  envoie  $(y)_j$  sur 1, alors l'image par  $\varphi$  de  $y^j$  est  $B_j$ .  $\square$

COROLLAIRE 7.1.- Pour  $n \in \mathbb{N}$  et  $p$  un nombre premier impair, les polynômes de Bell-Carlitz vérifient la congruence

$$B_{np}^c(x) \equiv B_n^c(1+x^p) \pmod{np\mathbb{Z}_p[x]}.$$

PREUVE.- Il existe  $k \in \mathbb{N}$  premier à  $p$ , et  $\nu \geq 1$  tels que  $n = kp^{\nu-1}$ . Par ailleurs, on a, grâce au théorème 7.1 et au lemme 7.5

$$(x+y)^{kp^\nu} f \stackrel{p^\nu}{\sim} (x^p+1+y)^{kp^{\nu-1}} f.$$

Observons que

$$\begin{aligned} \Psi((x+y)^{kp^\nu}) &= \sum_{0 \leq i \leq kp^\nu} \binom{kp^\nu}{i} \Psi(x^i y^{kp^\nu-i}) \\ &= \sum_{0 \leq i \leq kp^\nu} \binom{kp^\nu}{i} x^i B_{kp^\nu-i} = B_{kp^\nu}^c(x) \end{aligned}$$

et que

$$\Psi((x^p+1+y)^{kp^{\nu-1}}) = B_{kp^{\nu-1}}^c(1+x^p),$$

et prenons  $f \equiv 1$ . On obtient alors la congruence

$$B_{kp^\nu}^c(x) \equiv B_{kp^{\nu-1}}^c(1+x^p) \pmod{p^\nu A[x]},$$

et donc  $B_{np}^c(x) \equiv B_n^c(1+x^p) \pmod{np\mathbb{Z}_p[x]}$ .  $\square$

REMARQUES.- 1) Pour  $x = 0$ , on trouve  $B_{np}^c(0) \equiv B_n^c(1) \pmod{np\mathbb{Z}_p}$ ; il s'agit de la congruence de Comtet-Zuber

$$B_{np} \equiv B_{n+1} \pmod{np\mathbb{Z}_p}.$$

2) Pour  $p = 2$ , on a la congruence

$$B_{2n}^c(x) \equiv B_n^c(1+x^2) \pmod{n\mathbb{Z}_2[x]} \quad (\text{puisqu'on perd un facteur 2}).$$

## Références

- [1] M. ABRAMOWITZ, I.A. STEGUN, *Handbook of Mathematical Functions*, Dover Publ., New York, 1965.
- [2] Y. AMICE, *Les Nombres  $p$ -adiques*, Presses univ. de France, coll. SUP, le Mathématicien, 1975.
- [3] B.C. CARLSON, *Special Functions of Applied Mathematics*, Academic Press, 1977.
- [4] L. COMTET, *Analyse combinatoire*, Presses univ. de France, coll. SUP, le Mathématicien, 1 et II, 1970.
- [5] B. DRAGOVICH, *On some  $p$ -adic Series with Factorials*, Proceedings of the 4th intern. Conf. on  $p$ -adic Functional Analysis.
- [6] B. DRAGOVICH, *On some finite Sums with Factorials*, à paraître.
- [7] A. GERTSCH, A. ROBERT, *Some Congruences concerning the Bell Numbers*, Bull. Belg. math. soc. 3 (1996), 467-475.
- [8] A. GERTSCH, *Nombres harmoniques généralisés*, Comptes rendus Acad. Sc. 324 série I (1997), 7-10.
- [9] R.L. GRAHAM, D.E. KNUTH, O. PATASHNIK, *Concrete Mathematics*, Addison - Wesley, 1989.
- [10] R.K. GUY, *Unsolved Problems in Number Theory*, Springer-Verlag, 1981.
- [11] G. HARDY, E. WRIGHT, *An Introduction to the Theory of Numbers*, 4th edition, Oxford, Clarendon Press, 1971.
- [12] Y. MATIYASEVICH, *What Divisibility Properties Do Generalized Harmonic Numbers Have ?*, Amer. Math. Monthly 99 (1992), 74-75.
- [13] A. MAZOUZ, *Nombres de Bell généralisés*, Comptes rendus Acad. Sc. 321 série I (1995), 131-134.
- [14] C. RADOUX, *Nouvelles Propriétés arithmétiques des Nombres de Bell*, Sémin. Delange-Pisot-Poitou, Univ. Paris VI, 16e année, exposé no 22, 1974-75.
- [15] C. RADOUX, *Nombres de Bell modulo  $p$  premier et extensions de degré  $p$  de  $F_p$* , Comptes rendus Acad. Sc. 281 série A (1975), 879-882.
- [16] C. RADOUX, *Une Congruence pour les Polynômes  $P_n(x)$  de fonction génératrice  $e^{x(e^x-1)}$* , Comptes rendus Acad. Sc. 284 série A (1977), 637-639.
- [17] J. RIORDAN, *Combinatorial Identities*, Wiley, New York, 1968.
- [18] A. ROBERT, *A Course in  $p$ -adic Analysis*, GTM Springer, à paraître.

- [19] A. ROBERT, *A note on the Numerators of the Bernoulli Numbers*, Expo. Math. 9 (1991), 189-191.
- [20] A. ROBERT, *Polynômes de Legendre mod p*, Séminaire d'Analyse, Publ. du département de Mathématiques pures, Université Blaise-Pascal, Clermont II, tome 6 (1990-1991), exposé no 19.
- [21] S. ROMAN, *The Umbral Calculus*, Academic Press, Orlando, FL, 1983.
- [22] S. ROMAN, G.-C. ROTA, *The Umbral Calculus*, Advances in Math. 27 (1978), 95-188.
- [23] G.C. ROTA, *The Number of Partitions of a Set*, Amer. Math. Monthly 71 (1964), 498-504.
- [24] J.J. ROTMAN, *An Introduction to the Theory of Groups*, Fourth Edition, Springer Verlag, 1995.
- [25] W.H. SCHIKHOF, *Ultrametric Calculus, an Introduction to p-adic Analysis*, Cambridge University Press, 1984.
- [26] N.YA. VILENKIN, *Combinatorics*, Academic Press New York and London, 1971.
- [27] M. ZUBER, *Propriétés de Congruence de certaines Familles classiques de Polynômes*, Comptes rendus Acad. Sc. 315 série I (1992), 869-872.
- [28] M. ZUBER, *Propriétés p-adiques de Polynômes classiques*, Thèse de doctorat, Université de Neuchâtel, 1992.
- [29] M. ZUBER, *Une Suite récurrente remarquable*, Comptes rendus Acad. Sc. 318 série I (1994), 205-208.
- [30] M. ZUBER, *Suites de Honda*, Annales de l'Université Blaise-Pascal, Clermont-Ferrand, Vol. 2 No 1 (1995), 307-314.
- [31] M. ZUBER, A. ROBERT, *The Kazandzidis Supercongruences - A simple proof and an application*, Rendiconti del Seminario Matematico dell'Università di Padova, Vol. 94 (1995), 235-243.
- [32] M. ZUBER, *Théorèmes de Bauer, Wolstenholme et Leudesdorf comme Applications du Théorème p-adique des Accroissements finis d'Ordre 2*, Neuchâtel, mai 1993.