Journal de Théorie des Nombres
de Bordeaux **16** (2004), 1–17

Nombres de Bell et somme de factorielles

par Daniel BARSKY et Bénali BENZAGHOU

Résumé. Dj. Kurepa a conjecturé que pour tout nombre premier impair, p, la somme $\sum_{n=0}^{p-1} n!$ n'est pas divisible par p. Cette somme est reliée aux nombres de Bell qui apparaissent en combinatoire énumérative. Nous donnons une expression du n-ième nombre de Bell modulo p comme la trace de la puissance n-ième d'un élément fixe dans l'extension d'Artin-Schreier de degré p du corps premier à p éléments. Cette expression permet de démontrer la conjecture de Kurepa en la ramenant à un problème d'algèbre linéaire.

Abstract. Dj. Kurepa has conjectured that for any odd prime number p, the sum $\sum_{n=0}^{p-1} n!$ is not divisible by p. This sum is related to the Bell numbers that occur in enumerative combinatorics. We give a formula for the n-th Bell number modulo p as the trace of the n-th power of a fixed element in the Artin-Schreier extension of degree p of the field with p elements. This formula allows us to prove the Kurepa's conjecture by reducing it to a linear algebra problem.

1. Introduction.

Dj. Kurepa a conjecturé dans [7] que si p est un nombre premier impair, la somme $\kappa_p = \sum_{n=0}^{p-1} n!$ n'est pas divisible par p, par exemple

$$\kappa_2 = 2,\ \kappa_3 \equiv 1 \mod 3,\ \kappa_5 \equiv 4 \mod 5,$$
$$\kappa_7 \equiv 6 \mod 7, \ldots,\ \kappa_{53} \equiv 13 \mod 53, \ldots$$

A. Gertsch a remarqué dans sa thèse, [4], que les nombres de Bell qui apparaissent en combinatoire énumérative sont liés aux $\kappa_p \pmod p$. En effet si l'on note P_n le n-ième nombre de Bell alors par définition

$$P_n = \sum_{k=1}^{n} S(n,k)$$

où $S(n,k)$ est le nombre de Stirling de deuxième espèce, cf. [3]. Or

$$S(p-1,k) \equiv (p-1-k)! \mod p\mathbb{Z},\ 1 \le k \le p-1$$

Manuscrit reçu le 2 avril 2002.

et donc $P_{p-1} - 1 \equiv \kappa_p$.

Nous utilisons cette remarque et les résultats que nous avons sur les nombres de Bell modulo p pour démontrer cette conjecture.

1.1. Notations. Le n-ième nombre de Bell, P_n, compte le nombre de partitions d'un ensemble à n-éléments en sous-ensembles non-vides. Leurs premières valeurs sont :

$P_0 = 1$, $P_1 = 1$, $P_2 = 2$, $P_3 = 5$, $P_4 = 15$, $P_5 = 52, \ldots$, $P_{15} = 1\,382\,958\,545$

Nous notons respectivement $\mathbb{N} = \{1, 2, \ldots\}$ les entiers naturels, $\mathbb{Z}$ les entiers relatifs, $\mathbb{Q}$ les nombres rationnels.

Soit p un nombre premier, que nous supposerons impair sauf indication contraire. Nous notons $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$ le corps premier à p éléments, $\overline{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$. Nous confondrons les éléments de $\mathbb{F}_p$ avec leurs antécédents dans $\mathbb{Z}$ par la surjection canonique de $\mathbb{Z}$ sur $\mathbb{F}_p$.

1.2. Résultats. Le résultat principal est la preuve de la conjecture de Kurepa au théorème 3. Nous montrons au théorème 1 que la fonction génératrice des nombres de Bell, $F(x) = \sum_{n\geq 0} P_n x^n$, est congrue modulo $p\mathbb{Z}[[x]]$ à (la série de Taylor en zéro de) la fraction rationnelle :

$$F_p(x) = \frac{\sum_{n=0}^{p-1} x^n (1-(n+1)x)\ldots(1-(p-1)x)}{1 - x^{p-1} - x^p}\,. \tag{1}$$

Remarque. Ce résultat se généralise aisément, on peut montrer que la série génératrice des nombres de Bell est congrue modulo $p^h\mathbb{Z}[[x]]$ à une fraction rationnelle $F_{p,h}(x)$. On en déduit des congruences modulo $p^h\mathbb{Z}$ pour les nombres de Bell en utilisant un peu d'analyse p-adique. Ce point de vue est développé dans [2].

On pose $F_p(x) = \sum_{n\geq 0} P_{n,p} x^n$, on a donc $P_{n,p} \equiv P_n \pmod{p\mathbb{Z}}$. La fraction rationnelle $F_p(x)$ possède un développement en série de Laurent à l'infini noté $\sum_{n\geq 0} -\frac{P_{-n,p}}{x^n}$. On constate que $P_{-1,p} \equiv \sum_{n=0}^{p-1} n! \pmod{p\mathbb{Z}}$.

Soit θ^{-1} une racine dans $\overline{\mathbb{F}}_p$ du polynôme $x^p + x^{p-1} - 1$ et soit $\mathfrak{F}_p = \mathbb{F}_p[\theta]$. On montre au théorème 2 que, si $c_p = 1 + 2p + \cdots + (p-1)p^{p-2}$, on a pour $n \in \mathbb{Z}$

$$P_{n,p} \equiv -\operatorname{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\theta^{c_p}\right) \operatorname{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\theta^{-c_p-1+n}\right) \mod p\mathbb{Z}$$

Ch. Radoux, [9], avait déjà vu que l'extension d'Artin-Schreier $\mathbb{F}_p[\theta]$ joue un rôle important dans l'arithmétique des nombres de Bell.

Nous en déduisons en particulier que

$$P_{-1,p} \equiv -\operatorname{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\theta^{c_p}\right)\operatorname{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\theta^{-c_p-2}\right),$$

donc

$$P_{-1,p} \equiv 0 \mod p\mathbb{Z} \Longleftrightarrow \operatorname{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\theta^{-c_p-2}\right) = 0\,.$$

On décompose θ^{-c_p} sur la $\mathbb{F}_p$-base normale de $\mathfrak{F}_p$, constituée par les éléments $\dfrac{1}{\theta+i}$ $(0 \le i \le p-1)$. On pose $\theta^{-c_p} = \displaystyle\sum_{i=0}^{p-1} \frac{\lambda_i}{\theta+i}$, $(\lambda_i \in \mathbb{F}_p)$. On montre au lemme 9 que les λ_i satisfont un système de p équations linéaires que nous ne savons pas résoudre explicitement en toute généralité. Par contre on montre que l'on a toujours $\lambda_1 = 0$, (cf. relations (16)), et que $\kappa_p = 0$ équivaut à $\lambda_{p-1} = 0$, (cf. lemme 10).

Pour montrer la conjecture de Kurepa nous raisonnons par l'absurde. Nous montrons au théorème 3 que, pour p premier impair, l'hypothèse $\kappa_p \equiv 0 \pmod p$ implique que $\lambda_i = 0$ pour $0 \le i \le p-1$, autrement dit que $\theta^{-c_p} = 0$, ce qui est absurde car l'équation $x^p - x - 1$ n'a pas $x = 0$ comme racine.

Nous remercions A. Robert pour avoir attiré notre attention sur ce problème. Nous remercions A. Junod et S. Zerroukhat de nous avoir signalé des erreurs graves dans les versions antérieures.

1.3. Rappels sur les nombres de Bell. Nous rappelons tout d'abord la définition des nombres de Bell. Pour toutes les questions de combinatoire notre référence est Comtet, cf. [3].

Définition 1. *Le n-ième nombre de Bell, P_n, est le nombre de partitions d'un ensemble à n éléments en sous-ensembles non-vides.*

Lemme 1. *Les nombres de Bell sont caractérisés par la relation de récurrence suivante :*

$$P_0 = 1 \qquad et \qquad P_{n+1} = \sum_{k=0}^{n} \binom{n}{k} P_k \quad si\ n \ge 0\,.$$

Leur fonction génératrice ordinaire est :

$$F(x) = \sum_{n\ge 0} P_n x^n = \sum_{n\ge 0} \frac{x^n}{(1-x)\dots(1-nx)}$$

Démonstration : Pour la démonstration voir [3]. □

Les nombres de Bell ont de nombreuses autres caractérisations, cf. par exemple [2].

2. Nombres de Bell modulo p.

Nous notons $P_{n,p}$ la réduction modulo $p\mathbb{Z}$ du n-ième nombre de Bell que nous confondrons avec l'image de P_n dans $\mathbb{F}_p$.

Nous utiliserons dans toute la suite la définition classique suivante :

Définition 2. *Soient $G(x)$, $H(x)$ deux fractions rationnelles de $\mathbb{Q}(x)$, on suppose que $G(x)$ et $H(x)$ sont développables formellement au voisinage de zéro en séries de Taylor à coefficients entiers relatifs :*

$$G(x)=\sum_{n\geq 0} g_n x^n \in \mathbb{Z}[[x]], \quad H(x)=\sum_{n\geq 0} h_n x^n \in \mathbb{Z}[[x]]\,.$$

On dira que $G(x)$ est congrue à $H(x)$ modulo $p\mathbb{Z}[[x]]$ si leurs séries de Taylor en zéro le sont, autrement dit :

$$G(x)\equiv H(x) \mod p\mathbb{Z}[[x]] \Longleftrightarrow \sum_{n\geq 0} g_n x^n \equiv \sum_{n\geq 0} h_n x^n \mod p\mathbb{Z}[[x]]\,.$$

Avec cette définition on a :

Théorème 1. *Soit p un nombre premier et soit*

$$F_p(x)=\frac{\sum_{n=0}^{p-1} x^n(1-(n+1)x)\dots(1-(p-1)x)}{1-x^{p-1}-x^p}$$

alors la fonction génératrice des nombres de Bell est congrue modulo $p\mathbb{Z}[[x]]$ à $F_p(x)$.

Démonstration : La preuve est élémentaire. On a :

$$\begin{aligned}\sum_{n\geq 0} P_n x^n &= \sum_{n\geq 0} \frac{x^n}{(1-x)\dots(1-nx)} \\ &= \sum_{n=0}^{p-1}\sum_{j\geq 0} \frac{x^{jp+n}}{(1-x)\dots(1-(jp+n)x)}\end{aligned}$$

donc

$$\sum_{n\geq 0} P_n x^n = \\ = \sum_{n=0}^{p-1}\sum_{j\geq 0} \frac{x^n}{(1-(jp+1)x)\dots(1-(jp+n)x)}\cdot\frac{x^{jp}}{(1-x)\dots(1-jpx)}\,.$$

On remarque que

$$\frac{x^{jp}}{(1-x)\dots(1-jpx)} \equiv \left(\frac{x^p}{(1-x)\dots(1-px)}\right)^j \mod p\mathbb{Z}[[x]]$$

et que

$$\frac{x^n}{(1-(jp+1)x)\dots(1-(jp+n)x)} \equiv \frac{x^n}{(1-x)\dots(1-nx)} \mod p\mathbb{Z}[[x]]\,.$$

De là il vient immédiatement :

$$\sum_{n\geq 0} P_{n,p}x^n \equiv$$
$$\equiv \sum_{n=0}^{p-1} \frac{x^n}{(1-x)\dots(1-nx)} \sum_{j\geq 0}\left(\frac{x^p}{(1-x)\dots(1-px)}\right)^j \mod p\mathbb{Z}[[x]]\,,$$

et en sommant la série géométrique en j, il vient finalement :

$$\sum_{n\geq 0} P_{n,p}x^n \equiv \frac{\sum_{n=0}^{p-1} x^n(1-(n+1)x)\dots(1-(p-1)x)}{(1-x)\dots(1-(p-1)x)-x^p} \mod p\mathbb{Z}[[x]]$$

où par convention dans la somme $\sum_{n=0}^{p-1} x^n(1-(n+1)x)\dots(1-(p-1)x)$ le terme correspondant à $n=p-1$ vaut x^{p-1}, (on applique la convention classique : un produit vide vaut 1). □

Corollaire 1. *La (série de Taylor en zéro) de la fraction rationnelle $F_p(x)$ est congrue modulo $p\mathbb{Z}[[x]]$ à*

$$F_p(x) \equiv \frac{\left(\sum_{n=0}^{p-2} P_{n,p}x^n\right) + (P_{p-1,p}-P_{0,p})x^{p-1}}{1-x^{p-1}-x^p} \mod p\mathbb{Z}[[x]] \tag{2}$$

Démonstration : On a montré au théorème 1 que

$$\sum_{n\geq 0} P_{n,p}x^n \equiv \frac{\sum_{n=0}^{p-1} x^n(1-(n+1)x)\dots(1-(p-1)x)}{1-x^{p-1}-x^p} \mod p\mathbb{Z}[[x]]$$

multiplions les deux membres par $1-x^{p-1}-x^p$ et identifions, il vient :

$$\sum_{n=0}^{p-2} P_{n,p}x^n + (P_{p-1,p}-P_{0,p})x^{p-1} \equiv$$
$$\equiv \sum_{n=0}^{p-1} x^n(1-(n+1)x)\dots(1-(p-1)x) \mod p\mathbb{Z}[[x]]\,.$$

On en déduit immédiatement que

$$F_p(x) \equiv \frac{\sum_{n=0}^{p-2} P_{n,p}x^n + (P_{p-1,p}-P_{0,p})x^{p-1}}{1-x^{p-1}-x^p} \mod p\mathbb{Z}[[x]] \qquad \square$$

Nous allons étudier les zéros dans $\overline{\mathbb{F}}_p$ du dénominateur $D_p(x)$ de la fraction rationnelle $F_p(x)$.

Lemme 2. *Soit $D_p(x) = 1 - x^{p-1} - x^p$. Notons θ_i^{-1} , $1 \leq i \leq p$, les racines de $D_p(x)$ dans $\overline{\mathbb{F}}_p$, elles vérifient*

- $\theta_i^p = \theta_i + 1$.
- $\theta_i \neq \theta_j$ *dans* $\overline{\mathbb{F}}_p$*si* $i \neq j$.
- $\mathfrak{F}_p = \mathbb{F}_p(\theta_i)$ *est une extension d'Artin-Schreier de degré* p *de* $\mathbb{F}_p$, *dont le groupe de Galois* $\mathrm{Gal}(\mathfrak{F}_p/\mathbb{F}_p)$, *isomorphe à* $(\mathbb{Z}/p\mathbb{Z}, +)$, *a pour générateur le Frobenius* $\sigma_p : \quad x \longmapsto x^p$.

Démonstration : Le polynôme $x^p - x - 1 = x^p D_{p,1}\big(x^{-1}\big)$ est à racines simples car $\dfrac{d}{dx} D_{p,1}(x) = (px + (p-1)x)x^{p-2}$. Il est irréductible sur $\mathbb{F}_p$, cf. [8]. On a $\theta_i^p - \theta_i - 1 = 0$. On vérifie que, dans $\overline{\mathbb{F}}_p$, si θ est une racine de $x^p - x - 1$, alors $\theta + 1$ aussi car :

$$(\theta+1)^p - (\theta+1) - 1 = (\theta^p + 1) - (\theta + 1) + 1 = \theta^p - \theta - 1 = 0$$

donc dans $\overline{\mathbb{F}}_p$ les racines de $D_{p,1}$ sont $\dfrac{1}{\theta}$, $\dfrac{1}{\theta+1}$,..., $\dfrac{1}{\theta+(p-1)}$.

Le polynôme $x^p - x - 1$ est de type Artin-Schreier et on sait que ces polynômes engendrent des extensions séparables de $\mathbb{F}_p$, dont le groupe de Galois $\mathrm{Gal}(\mathfrak{F}_p/\mathbb{F}_p)$, isomorphe à $(\mathbb{Z}/p\mathbb{Z}, +)$, est engendré par le Frobenius $\sigma_p : x \mapsto x^p$, cf. [8]. □

Nous allons donner une expression des nombres de Bell modulo p au théorème 1 comme la trace de certaines puissances de θ. Pour les propriétés des corps finis notre référence est [8].

Dans le lemme suivant nous donnons quelques propriétés élémentaires des racines θ du polynôme $x^p - x - 1$ dans $\overline{\mathbb{F}}_p$.

Lemme 3. *Soit θ une racine du polynôme $x^p - x - 1$ dans $\overline{\mathbb{F}}_p$. Les autres racines dans $\overline{\mathbb{F}}_p$ de ce polynôme sont $\theta + i$ pour $1 \leq i \leq p-1$. On a :*

$$\mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}(\theta^i) = 0 \quad \textit{pour} \quad 0 \leq i \leq p-2,$$
$$-\mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}(\theta^{-1}) = \mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}(\theta^{p-1}) = 1\,.$$

Posons :

$$t_p = \frac{p^p - 1}{p-1} = 1 + p + \cdots + p^{p-1}, \quad c_p = \frac{p^p - t_p}{p-1} = 1 + 2p + \cdots + (p-1)p^{p-2}\,,$$

Notons encore, $\sigma_p : x \longmapsto x^p$, *le Frobenius absolu de* $\overline{\mathbb{F}}_p$. *Avec ces notations on a dans* $\mathfrak{F}_p$ *:*

$$\theta^{p^s} = \sigma_p^s(\theta) = \theta + s, \qquad \theta^{t_p} = 1 \tag{3}$$

$$\big(n\theta^{c_p}\big)^{p-1} = \theta \tag{4}$$

$$\sigma_p^s\big(\theta^{c_p}\big) = \theta^{c_p} \cdot \theta(\theta+1)\ldots(\theta+s-1)\,. \tag{5}$$

Démonstration : On a vu que le polynôme $x^p - x - 1$ engendre une extension d'Artin-Schreier, $\mathfrak{F}_p = \mathbb{F}_p[\theta]$ de $\mathbb{F}_p$. Un générateur de $\mathrm{Gal}(\mathfrak{F}_p/\mathbb{F}_p)$ est le Frobenius absolu, σ_p, qui à $a \in \mathfrak{F}_p$ associe $\sigma_p(a) = a^p$. On a bien évidemment dans $\mathfrak{F}_p$:

$$\sigma_p^i(\theta) = \theta^{p^i} = \theta + i \quad \text{pour} \quad i \in \mathbb{Z}, \quad \text{et} \quad (\theta+i)^p - (\theta+i) - 1 = 0$$
$$\mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}(1) = \mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}(\theta) = \ldots = \mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}(\theta^{p-2}) = 0$$
$$\mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}(\theta^{p-1}) = \mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\frac{1}{\theta+1} - 1\right) = \mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\frac{1}{\theta}\right)$$

et il est évident que $Tr_{\mathfrak{F}_p/\mathbb{F}_p}\left(\frac{1}{\theta}\right) = -1$ car le polynôme réciproque de $x^p - x - 1$ est $x^p + x^{p-1} - 1$.

La norme de θ sur $\mathbb{F}_p$ est par définition :

$$\mathrm{N}_{\mathfrak{F}_p/\mathbb{F}_p}(\theta) = \theta^{1+p+\cdots+p^{p-1}} = \theta^{t_p}$$

cette norme vaut 1 car le polynôme minimal de θ est $x^p - x - 1$. Donc l'application

$$\mathbb{N} \longrightarrow \mathfrak{F}_p$$
$$n \longmapsto \theta^n$$

est périodique de période divisant t_p, par conséquent $\left(\theta^{c_p}\right)^{p-1} = \theta^{p^p - t_p} = \theta$. Un calcul élémentaire montre que $c_p = \dfrac{p^p - t_p}{p-1} = 1+2p+\cdots+(p-1)p^{p-2} \in \mathbb{N}$.

Considérons l'élément θ^{c_p} de $\mathfrak{F}_p$, alors :

$$\sigma_p\left(\theta^{c_p}\right) = \theta^{pc_p} = \theta^{p\cdot\frac{p^p-t_p}{p-1}} = \theta^{c_p+p^p-t_p} = \theta^{c_p} \times \theta^{p^p} = \theta^{c_p} \times \theta\,.$$

On montre alors facilement par récurrence que :

$$\sigma_p^s\left(\theta^{c_p}\right) = \theta^{c_p} \times \theta(\theta+1)\ldots(\theta+s-1)\,. \qquad \square$$

Remarque. La relation $\left(\theta^{c_p}\right)^{p-1} = \theta$ montre que θ^{c_p} est une racine $(p-1)$-ième de θ dans $\mathfrak{F}_p$, les racines $(p-1)$-ièmes de θ sont exactement les $n\theta^{c_p}$ pour $1 \le n \le p-1$.

Lemme 4. *Soit θ une racine dans $\mathfrak{F}_p$ du polynôme $x^p - x - 1$ et soit*

$$F_p(x) = \sum_{\theta^p = \theta+1} \frac{\mu_\theta}{1-\theta x}$$

la décomposition de $F_p(x)$ en éléments simples dans $\mathfrak{F}_p(x)$. On a :

$$(6) \quad \mu_\theta = -\theta^{-c_p-1}\,\mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\theta^{c_p}\right) = \\ = -(P_{0,p}\cdot\theta^{p-1} + \ldots + P_{1,p}\cdot\theta + (P_{p-1,p} - P_{0,p}))\,.$$

Démonstration : On a dans $\mathfrak{F}_p$:

$$\mu_\theta = \frac{\sum_{n=0}^{p-1} \theta^{-n}(1-(n+1)\theta^{-1})\dots(1-(p-1)\theta^{-1})}{-\theta^{1-p}}\,.$$

Donc :

$$\mu_\theta = -\sum_{n=0}^{p-1}(\theta-(n+1))\dots(\theta-(p-1)) = -\sum_{n=0}^{p-1}(\theta+1)\dots(\theta+n)$$

avec la convention que pour $n=0$ le terme correspondant dans la dernière somme vaut 1.

D'après la relation (5) on a

$$\begin{aligned}\mu_\theta &= -\theta^{-c_p-1}\Big(\theta^{c_p}\big\{1+\theta+\theta(\theta+1)+\dots+\theta(\theta+1)\dots(\theta+p-2)\big\}\Big)\\ &= -\theta^{-c_p-1}\sum_{i=0}^{p-1}\sigma_p^i\big(\theta^{c_p}\big) = -\theta^{-c_p-1}\operatorname{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\theta^{c_p}\right).\end{aligned}$$

On a aussi d'après le corollaire 1 :

$$\mu_\theta = -\big(P_{0,p}\cdot\theta^{p-1}+P_{1,p}\cdot\theta^{p-2}+\dots+P_{p-2,p}\cdot\theta+(P_{p-1,p}-P_{0,p})\big)\,. \qquad \square$$

Définition 3. *La fraction rationnelle $F_p(x)\in\mathbb{F}_p(x)$ possède un développement de Laurent au voisinage de l'infini que l'on note :*

$$F_p(x) = -\sum_{n\geq 1}\frac{P_{-n,p}}{x^n}\,. \tag{7}$$

En effet on a

$$\begin{aligned}F_p(x) &= \frac{\sum_{n=0}^{p-1}x^n(1-x(n+1))\dots(1-x(p-1))}{1-x^{p-1}-x^p}\\ &= \frac{1}{x}\frac{\sum_{n=0}^{p-1}(x^{-1}-x(n+1))\dots(x^{-1}-(p-1))}{x^{-p}-x^{-1}-1}\end{aligned}$$

il est clair que l'on peut développer cette dernière expression en série de Laurent.

Théorème 2. *On a dans $\mathbb{F}_p$, pour $n\in\mathbb{Z}$*

$$P_{n,p} = -\operatorname{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\theta^{c_p}\right)\cdot\operatorname{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\theta^{-c_p-1+n}\right). \tag{8}$$

Démonstration : On tire du lemme 4 que dans $\mathbb{F}_p$ on a pour $n\in\mathbb{Z}$:

$$P_{n,p} = \sum_{\theta^p=\theta+1}\mu_\theta\theta^n\,.$$

Le lemme 4 permet d'écrire l'expression précédente sous la forme

$$P_{n,p} = -\sum_{\theta^p=\theta+1}\operatorname{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\theta^{c_p}\right)\cdot\theta^{-c_p-1+n}\,.$$

Or les racines du polynôme $x^p - x - 1$ dans $\mathfrak{F}_p$ se déduisent de l'une d'entre elle par l'action des puissances successives du Frobenius. On en déduit que dans $\mathbb{F}_p$ on a :

$$P_{n,p} = -\operatorname{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\theta^{c_p}\right)\operatorname{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\theta^{-c_p-1+n}\right),$$

d'où la formule (8). □

3. Preuve de la conjecture de Kurepa.

Posons pour tout nombre premier $\kappa_p = \sum_{n=0}^{p-1} n!$. Nous sommes maintenant en mesure de démontrer la conjecture de Dj. Kurepa, cf. [7] :

$$\kappa_p \text{ n'est pas divisible par } p \text{ si } p > 2.$$

Lemme 5. *Avec les notations précédentes on a dans* $\mathfrak{F}_p$ *:*

$$P_{-1,p} = P_{p-1,p} - P_{0,p}, \quad \textit{et} \quad P_{-1,p} = \sum_{n=0}^{p-1} n! = \kappa_p$$

Démonstration : On a vu au corollaire 1 que dans $\mathbb{F}_p$,

$$F_p(x) = \frac{P_{0,p} + P_{1,p}x + \cdots + P_{p-2,p}x^{p-2} + (P_{p-1,p} - P_{0,p})x^{p-1}}{1 - x^{p-1} - x^p}$$

d'où la première expression de $P_{-1,p}$ (comparer avec l'introduction).

Pour la deuxième expression, soit

$$F_p(x) = \frac{\sum_{n=0}^{p-1} x^n(1-(n+1)x)\dots(1-(p-1)x)}{1 - x^{p-1} - x^p},$$

d'après la définition 3 cette fraction rationnelle possède un développement en série de Laurent noté : $F(x) = -\sum_{n\geq 1} \dfrac{P_{-n,p}}{x^n}$. On a donc par identification :

$$P_{-1,p} = \sum_{n=0}^{p-1} (-1)^{p-n-1}(n+1)(n+2)\dots(p-1) \tag{9}$$

En remplaçant n par $p-(p-n)$ dans l'expression précédente il vient

$$P_{-1,p} = \sum_{n=0}^{p-1} (-1)^{p-(n+1)}(p-(p-(n+1))(p-(p-(n+2))\dots 2\cdot 1$$

et en réduisant modulo p il vient

$$P_{-1,p} \equiv \sum_{n=0}^{p-1} n! \pmod{p}$$

d'où le résultat. □

Lemme 6. *Les éléments de* $\mathfrak{F}_p$, $\dfrac{1}{\theta+i}$ $(0 \le i \le p-1)$, *forment une* $\mathbb{F}_p$*-base normale de* $\mathfrak{F}_p$. *Si* $Z \in \mathfrak{F}_p$ *et si* $Z = \displaystyle\sum_{i=0}^{p-1} \frac{\alpha_i}{\theta+i}$, $(\alpha_i \in \mathbb{F}_p)$, *alors*

$$\alpha_i = \mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\Big(\frac{Z}{\theta+i}\Big) \qquad et \qquad \mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}(Z) = -\sum_{i=0}^{p-1}\alpha_i$$

Démonstration : On remarque tout d'abord que par définition les $\dfrac{1}{\theta+i}$, $0 \le i \le p-1$, sont les racines dans $\overline{\mathbb{F}}_p$ du polynôme $-D_p(x) = x^p + x^{p-1} - 1$ et donc

$$\mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\Big(\frac{1}{\theta+i}\Big) = -1 \tag{10}$$

Par ailleurs on a

$$\Big(\mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\Big(\frac{1}{(\theta+i)}\Big)\Big)^2 = \mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\Big(\frac{1}{(\theta+i)^2}\Big) - 2\sum_{0\le i<j\le p-1}\frac{1}{(\theta+i)(\theta+j)} = 1$$

Si $p \ge 3$ le coefficient de x^{p-2} dans $D_p(x)$ est nul donc :

$$\sum_{0\le i<j\le p-1}\frac{1}{(\theta+i)(\theta+j)} = 0$$

ce qui entraîne

$$\mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\Big(\frac{1}{(\theta+i)^2}\Big) = 1\,.$$

Si $p = 2$ on a $\dfrac{1}{\theta^2} = \dfrac{1}{\theta+1}$ et donc $\mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\Big(\dfrac{1}{(\theta+i)^2}\Big) = 1$ dans $\mathfrak{F}_2$.

Par ailleurs on a

$$\mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\Big(\frac{1}{\theta+i}\cdot\frac{1}{\theta+j}\Big) =$$

$$= \begin{cases} \dfrac{1}{i-j}\Big(\mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\Big(\dfrac{1}{\theta+j}\Big) - \mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\Big(\dfrac{1}{\theta+i}\Big)\Big), & \text{si } 0 \le i < j \le p-1 \\ \mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\Big(\dfrac{1}{(\theta+i)^2}\Big), & \text{si } 0 \le i = j \le p-1\,. \end{cases}$$

Finalement on a montré que :

$$\mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\Big(\frac{1}{\theta+i}\cdot\frac{1}{\theta+j}\Big) = \begin{cases} 0 & \text{si} \quad 0 \le i < j \le p-1 \\ 1 & \text{si} \quad 0 \le i = j \le p-1\,. \end{cases} \tag{11}$$

Autrement dit les $\left(\dfrac{1}{\theta+i}\right)$, $0 \leq i \leq p-1$, forment une base auto-duale pour la forme bilinéaire non dégénérée sur $\mathfrak{F}_p$, $\langle x, y\rangle = \mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}(xy)$ cf. [8]. On tire immédiatement de la relation (11)

$$\alpha_i = \mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\frac{Z}{\theta+i}\right)$$

On peut remarquer de manière alternative que dans $\mathfrak{F}_p$:

$$\frac{1}{\theta+i} = (\theta+i)^{p-1} - 1 = (\theta+i+1)(\theta+i+2)\dots(\theta+i+p-1)\,.$$

Autrement dit les $\dfrac{1}{\theta+i}$, $0 \leq i \leq p-1$, sont au coefficient -1 près les valeurs en θ des polynômes d'interpolation de Lagrange sur les points 0, 1,... $p-1$, ce qui suffit à montrer qu'ils forment une $\mathbb{F}_p$-base de $\mathfrak{F}_p$.

On tire immédiatement de la relation (10) que si $Z \in \mathfrak{F}_p$ avec $Z = \sum_{i=0}^{p-1} \dfrac{\alpha_i}{\theta+i}$, $(\alpha_i \in \mathbb{F}_p)$ alors $\mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}(Z) = -\sum_{i=0}^{p-1} \alpha_i$. □

Remarque. Tous les calculs qui suivent sont faits dans $\mathfrak{F}_p$.

Lemme 7. *On a l'équivalence i) $\Longleftrightarrow$ii)*

- **i):** *la constante de Kurepa, $\kappa_p = 0! + 1! + \cdots + (p-1)!$, est première à p*
- **ii):** $\mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\dfrac{1}{\theta^{c_p}(\theta-1)}\right) \neq 0$

Démonstration : On a vu au lemme 5 que

$$\big(\kappa_p \equiv 0 \mod p\big) \Longleftrightarrow \big(P_{-1,p} \equiv 0 \mod p\big)$$

et au théorème 2 que $P_{-1,p} = -\,\mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\theta^{c_p}\right) \cdot \mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\theta^{-c_p-2}\right)$.

Or $-\,\mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\theta^{c_p}\right) \neq 0$ dans $\mathbb{F}_p$, par exemple parce que $P_{0,p} = 1$, (on peut en fait calculer sa valeur en fonction de p). On a donc nécessairement

$$\kappa_p = 0 \Longleftrightarrow \mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}(\theta^{-c_p-2}) = 0\,.$$

Or d'après le lemme 3 on a $\theta^{-c_p-2} = \theta^{-pc_p}\theta^{-1} = \sigma_p\big(\theta^{-c_p}(\theta-1)^{-1}\big)$, et il est évident que

$$\mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}(\theta^{-c_p-2}) = \mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\sigma_p\big(\theta^{-c_p}(\theta-1)^{-1}\big)\right) = \mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\theta^{-c_p}(\theta-1)^{-1}\right).$$

□

Nous allons calculer les composantes λ_i, $0 \leq i \leq p-1$, de θ^{-c_p} sur la $\mathbb{F}_p$-base de $\mathfrak{F}_p$, $\dfrac{1}{\theta+i}$, $0 \leq i \leq p-1$ sous l'hypothèse $\kappa_p = 0$. Nous allons montrer que sous cette hypothèse les coefficients λ_i sont tous nuls ce qui

contredit évidemment $\theta^{-c_p-2} \neq 0$, puisque $\theta \neq 0$ en tant que racine du polynôme $x^p - x - 1$.

Lemme 8. *On pose* $\theta^{-c_p} = \sum_{i=0}^{p-1} \frac{\lambda_i}{\theta+i}$ *où* $\lambda_i \in \mathbb{F}_p$. *On a*

$$\lambda_i = \mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\theta^{-c_p}(\theta+i)^{-1}\right). \tag{12}$$

Démonstration : D'après le lemme 6, $\lambda_i = \mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\frac{\theta^{-c_p}}{\theta+i}\right)$. □

Lemme 9. *Si* $p > 2$, *les composantes* λ_i *de* θ^{-c_p} *sur la* $\mathbb{F}_p$*-base* $(\theta+i)^{-1}$ *vérifient les relations*

$$\sum_{i=1}^{p-1} \frac{\lambda_i}{i} - \lambda_0 = \lambda_{p-1} \tag{13}$$

$$\begin{cases} \lambda_0 - \lambda_1 = \lambda_0 \\ \frac{\lambda_0}{2} - \frac{\lambda_2}{2} = \lambda_1 \\ \vdots, \\ \frac{\lambda_0}{i} - \frac{\lambda_i}{i} = \lambda_{i-1} \\ \vdots \\ \frac{\lambda_0}{p-1} - \frac{\lambda_{p-1}}{p-1} = \lambda_{p-2} \end{cases} \tag{14}$$

en particulier si $p > 2$ *on a toujours* $\lambda_1 = 0$ *(Si* $p = 2$ *on a* $c_2 = 1$ *et donc* $\theta^{-c_2} = \theta^{-1}$*).*

Démonstration : On a en effet, d'après le lemme 3, la relation $\theta^{-c_p-1} = \theta^{-pc_p}$ que l'on va exprimer dans la $\mathbb{F}_p$-base de $\mathfrak{F}_p$, $(\theta+i)^{-1}$ $(0 \leq i \leq p-1)$.

On a d'une part d'après le lemme 3

$$\theta^{-pc_p} = \sum_{i=0}^{p-1} \frac{\lambda_i}{\theta+i+1}. \tag{15}$$

On a d'autre part

$$\theta^{-c_p-1} = \sum_{i=0}^{p-1} \frac{\lambda_i}{\theta(\theta+i)} = \frac{\lambda_0}{\theta^2} + \sum_{i=1}^{p-1} \frac{\lambda_i}{\theta(\theta+i)}.$$

Or on a vu au lemme 3 que $\mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\frac{1}{\theta}\right) = -1$, et donc :

$$-1 = \sum_{i=0}^{p-1} \frac{1}{\theta+i} \Longrightarrow -\frac{1}{\theta} = \sum_{i=0}^{p-1} \frac{1}{\theta(\theta+i)}$$

par conséquent

$$-\frac{1}{\theta}=\frac{1}{\theta^2}+\sum_{i=1}^{p-1}\frac{1}{\theta(\theta+i)}=\frac{1}{\theta^2}+\sum_{i=1}^{p-1}\frac{i^{-1}}{\theta}-\frac{i^{-1}}{\theta+i}$$

autrement dit

$$\frac{1}{\theta^2}=\frac{1}{\theta}\Big(-1-\sum_{i=1}^{p-1}i^{-1}\Big)+\sum_{i=1}^{p-1}\frac{i^{-1}}{\theta+i}\,.$$

Or si $p>2$ on a $\displaystyle\sum_{i=1}^{p-1}i^{-1}=0$ dans $\mathbb{F}_p$ et si $p=2$ on a $\displaystyle\sum_{i=1}^{p-1}i^{-1}=1$, donc finalement

$$\frac{1}{\theta^2}=\begin{cases}-\dfrac{1}{\theta}+\displaystyle\sum_{i=1}^{p-1}\frac{i^{-1}}{\theta+i} & \text{si } p>2\\[2ex] \dfrac{1}{\theta+1} & \text{si } p=2\,.\end{cases}$$

De cette relation on tire immédiatement que si $p>2$

$$\theta^{-c_p-1}=\frac{1}{\theta}\Big(\sum_{i=1}^{p-1}\frac{\lambda_i}{i}-\lambda_0\Big)+\sum_{i=1}^{p-1}\Big(\frac{\lambda_0}{i}-\frac{\lambda_i}{i}\Big)\frac{1}{\theta+i}\,. \tag{16}$$

La rapprochement des relations (15) et (16) donne si $p>2$

$$\sum_{i=0}^{p-1}\frac{\lambda_i}{\theta+i+1}=\frac{1}{\theta}\Big(\sum_{i=1}^{p-1}\frac{\lambda_i}{i}-\lambda_0\Big)+\sum_{i=1}^{p-1}\Big(\frac{\lambda_0}{i}-\frac{\lambda_i}{i}\Big)\frac{1}{\theta+i}\,.$$

et en identifiant les coefficients de $(\theta+i)^{-1}$ dans les deux membres on obtient les relations annoncées.

La relation $\lambda_0-\lambda_1=\lambda_0$ implique $\lambda_1=0$. Le cas $p=2$ se traite directement. □

Lemme 10. *Avec les notations du lemme 8 on a*

$$\kappa_p=0\Longleftrightarrow\lambda_{p-1}=0$$

Démonstration : Par définition on a $\theta^{-c_p}=\displaystyle\sum_{i=0}^{p-1}\frac{\lambda_i}{\theta+i}$. D'après le lemme 8 on a $\lambda_i=\mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\theta^{-c_p}(\theta+i)^{-1}\right)$, en particulier

$$\lambda_{p-1}=\mathrm{Tr}_{\mathfrak{F}_p/\mathbb{F}_p}\left(\theta^{-c_p}(\theta-1)^{-1}\right)$$

et donc $\lambda_{p-1}=\kappa_p$ d'après le lemme 7. □

Théorème 3. *Pour p premier impair la constante de Kurepa, $\kappa_p=0!+1!+\cdots+(p-1)!$, est première à p (pour $p=2$ $\kappa_2=2$).*

Démonstration : On vérifie directement que $\kappa_2 = 0!+1! = 2$. On supposera donc dans toute la suite de la démonstration que $p > 2$.

On garde les notations du lemme 9. On pose donc

$$\theta^{-c_p} = \sum_{i=0}^{p-1} \frac{\lambda_i}{\theta + i}, \quad \lambda_i \in \mathbb{F}_p\,.$$

On raisonne par l'absurde en supposant que pour $p > 2$ on a $\kappa_p \equiv 0 \pmod p$. D'après le lemme 10 on a alors $\lambda_{p-1} = 0$. En tenant compte de la relation $\lambda_{p-1} = 0$, le lemme 9 donne alors la relation

$$\sum_{i=1}^{p-1} \frac{\lambda_i}{i} - \lambda_0 = 0\,. \tag{17}$$

Posons

$$X_0 = \lambda_0, \quad \text{et} \quad X_i = \frac{\lambda_0 - \lambda_i}{i}, \text{ pour } 1 \leq i \leq p-1\,.$$

Avec ces nouvelles inconnues le système (13) et (14) devient sous les hypothèses $p > 2$ et $\kappa_p = 0$, ($\Leftrightarrow \lambda_{p-1} = 0$) :

$$\sum_{i=1}^{p-1} X_i = X_0 \tag{18}$$

$$\begin{cases} X_1 = X_0 \\ X_2 = -X_1 + X_0 \\ X_3 = -2X_2 + X_0 \\ \vdots \\ X_i = -(i-1)X_{i-1} + X_0 \\ \vdots \\ X_{p-1} = -(p-2)X_{p-2} + X_0\,. \end{cases} \tag{19}$$

- La relation (18) provient de la relation (17) et de la remarque suivante : si $p > 2$ alors $\displaystyle\sum_{i=1}^{p-1} \frac{1}{i} = 0$ et donc $\displaystyle\sum_{i=1}^{p-1} \frac{\lambda_i}{i} - \lambda_0 = \sum_{i=1}^{p-1} \frac{\lambda_i - \lambda_0}{i} - \lambda_0$.
- Les relations (19) proviennent des relations (14) par un simple changement de variable.

Remarque. L'hypothèse $\kappa_p = 0$ n'est pas utilisée pour les relations (19) par contre elle l'est pour la relation (18)

On tire facilement par récurrence des relations (19) que pour $p > 2$:

$$(20)\qquad \begin{cases} X_1 = X_0 \\ X_2 = X_0(1-1) \\ X_3 = X_0(1-2+2\cdot 1) \\ X_4 = X_0(1-3+3\cdot 2-3\cdot 2\cdot 1) \\ \vdots \\ X_{i-1} = X_0\Big\{1-\sum_{k=0}^{i-3}(-1)^k(i-2)(i-3)\dots(i-2-k)\Big\} \\ X_i = X_0\Big\{1-\sum_{k=0}^{i-2}(-1)^k(i-1)(i-2)\dots(i-1-k)\Big\} \\ \vdots \\ X_{p-1} = X_0\Big\{1-\sum_{k=0}^{p-3}(-1)^k(p-2)\dots(p-2-k)\Big\}. \end{cases}$$

En effet faisons l'hypothèse de récurrence :

– Pour $2 \le i \le p-1$ on a

$$X_i = X_0\Big\{1-\sum_{k=0}^{i-2}(-1)^k(i-1)(i-2)\dots(i-1-k)\Big\}.$$

On vérifie directement que pour $i = 2$ on a bien $X_2 = X_0(1-1) = 0$. Les relations (19) donnent en tenant compte de l'hypothèse de récurrence :

$$\begin{aligned} X_{i+1} &= -i\cdot X_0\Big\{1-\sum_{k=0}^{i-2}(-1)^k(i-1)(i-2)\dots(i-1-k)\Big\} + X_0 \\ &= X_0\Big\{1-i+\sum_{k=0}^{i-2}(-1)^k i\cdot(i-1)(i-2)\dots(i-1-k)\Big\} \\ &= X_0\Big\{1-\sum_{k=0}^{i-1}(-1)^k i\cdot(i-1)\dots(i-k)\Big\}. \end{aligned}$$

Les relations (20) sont démontrées.

Avec la convention habituelle qu'un produit vide vaut 1, il vient si $d \ge i-2$:

$$1-\sum_{k=0}^{i-2}(-1)^k(i-1)(i-2)\dots(i-k) = -\sum_{k=-1}^{i-2}(-1)^k(i-1)(i-2)\dots(i-k) =$$
$$= -\sum_{k=-1}^{d}(-1)^k(i-1)(i-2)\dots(i-k) = -\sum_{k=-1}^{+\infty}(-1)^k(i-1)(i-2)\dots(i-k).$$

Ajoutons membre à membre les relations (20) il vient :

$$\sum_{i=1}^{p-1} X_i = -X_0\Big\{\sum_{i=1}^{p-1}\sum_{k=-1}^{p-2}(-1)^k(i-1)(i-2)\dots(i-1-k)\Big\}$$
$$= -X_0\Big\{\sum_{k=-1}^{p-2}(-1)^k\sum_{i=1}^{p-1}(i-1)(i-2)\dots(i-k)\Big\}.$$

Or, toujours avec la convention qu'un produit vide vaut 1, on a :

$$\begin{cases} \displaystyle\sum_{i=1}^{p-1}(i-1)\dots(i-k) = -1 = 0!\binom{p-1}{1}, & \text{si } k=0 \\ \displaystyle k!\sum_{i=1}^{p-1}\binom{i-1}{k} = k!\sum_{i=0}^{p-2}\binom{i}{k} = k!\binom{p-1}{k+1}, & \text{si } 1\le k\le p-2\,. \end{cases}$$

Comme $\binom{p-1}{k+1} = (-1)^{k+1}$ dans $\mathbb{F}_p$, on a :

$$\sum_{i=1}^{p-1} X_i = -X_0\Big\{\sum_{k=-1}^{p-2}(-1)^k k!\binom{p-1}{k+1}\Big\} = X_0\Big(\sum_{k=0}^{p-1}k!\Big) = X_0\cdot\kappa_p\,.$$

On vient donc de montrer que :

$$(p>2 \text{ et } \kappa_p = 0) \Longrightarrow \sum_{i=1}^{p-1} X_i = 0 \tag{21}$$

et donc en comparant la relation (21) avec la relation (18) il vient :

$$(p>2 \text{ et } \kappa_p = 0) \Longrightarrow X_0 = 0\,. \tag{22}$$

Or $X_0 = \lambda_0$, reportons la valeur $\lambda_0 = 0$ dans les relations (14) il vient immédiatemment en utilisant la relation $\lambda_1 = 0$ donnée au lemme 9 :

$$(p>2 \text{ et } \kappa_p = 0) \Longrightarrow \big(0 = \lambda_0 = \lambda_1 = \lambda_2 = \dots = \lambda_{p-2} = \lambda_{p-1}\big)\,. \tag{23}$$

On a donc montré que :

$$(p>2 \text{ et } \kappa_p = 0) \Longrightarrow \theta^{-c_p} = 0 \tag{24}$$

ce qui est absurde car $\theta \neq 0$ puisqu'il est racine de $x^p - x - 1 = 0$. La démonstration de la conjecture de Kurepa est complète. □

Bibliographie

[1] D. Barsky, *Analyse p-adique et nombres de Bell*. C. R. Acad Sc. Paris série A, **282** (1976), 1257–1259 & Groupe d'Étude d'Analyse Ultramétrique. (Y. Amice, Ph. Robba), 3-ième année, 1975/76, exposé n°11.

[2] D. Barsky & B. Benzaghou, *Congruences pour les nombres de Bell*, préprint, (1992).

[3] L. Comtet, *Analyse Combinatoire*. PUF, Collection Sup le mathématicien, Paris, 1970.

[4] A. Gertsch Hamadene, *Congruences pour quelques suites classiques de nombres ; sommes de factorielles et calcul ombral*. Thèse présentée à la faculté des sciences pour obtenir le grade de docteur ès sciences, Université de Neuchâtel, février 1999.

[5] A. Gertsch & A. Robert, *Some congruences concerning the Bell numbers*. Bulletin of the Belgian Mathematical Society Simon Stevin vol. **3** (1996), 467–475.

[6] A. Junod, *A Generalized Trace Formula for Bell Numbers*. A paraître dans Expositiones Mathematicae.

[7] Dj. Kurepa, *On the left factorial function* $!n$. Math. Balkanica vol. **1** (1971), 147–153.

[8] R. Lidl & H. Niederreiter, *Introduction to finite fields and their applications*. Revision of the 1986 first edition. Cambridge University Press, Cambridge, 1994.

[9] Ch. Radoux, *Nombres de Bell modulo p premier et extensions de degré p de* $\mathbb{F}_p$. C. R. Acad. Sc. Paris, série A, **281**, séance du 24 novembre 1975, 879–882.

[10] A. Robert, *A course in p-adic Analysis*. G.T.M. **198**, Springer-Verlag, 2000.

Daniel Barsky
Université Paris 13
Institut Galilée
LAGA, URA CNRS n°742
Av J.-B. Clément
F-93430 VILLETANEUSE, France
E-mail : barsky@math.univ-paris13.fr

Bénali Benzaghou
USTHB
Faculté de Mathématiques
El Alia BP 32
Bab Ezzouar
1611 ALGER, Algérie
E-mail : benrect@wissal.dz