Congruences pour les polynômes et nombres de Bell

Alexandre Junod*

Abstract

By elementary techniques based on umbral calculus ([10],[11]), we establish a new congruence for the Bell polynomials, which generalizes at once the congruences of Touchard, Radoux ([6],[7], [8],[4]), Comtet-Zuber ([4],[5]) and Carlitz [2] for Bell numbers. Congruences concerning the Stirling numbers of the first and second kind follow from this one. The generalized congruence satisfied by the Bell numbers can also be proved in an independent way with the "trace formula" of D.Barsky and B.Benzaghou [3].

1 Définitions

Etant donné un nombre premier p, on dénote par $\mathbb{Z}_p$ l'anneau des entiers p-adiques, muni de sa valuation ord_p. Les polynômes de Pochhammer

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

constituant une base du $\mathbb{Z}_p$-module libre $\mathbb{Z}_p[x]$, on peut considérer l'application linéaire

$$\Phi : \mathbb{Z}_p[x] \longrightarrow \mathbb{Z}_p[x],\ (x)_n \longmapsto x^n.$$

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

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

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

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

*Financé par le subside 20-56816.99 du FNRS suisse
Received by the editors June 2001.
Communicated by J. Mawhin.

2 Préliminaires

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

Preuve. On peut écrire $\alpha = \beta + m\gamma$ avec $\gamma \in \mathcal{A}$ et comme p divise m,

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

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

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

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

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

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

Remarquons que lemme reste valable pour un anneau commutatif $\mathcal{A}$ qui contient $\mathbb{Z}$, à condition que l'entier n soit une puissance de p (les unités de $\mathbb{Z}$ sont $l = \pm 1$).

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

Lemme 2. *Considèrons un nombre premier p et deux entiers $m, n \geqslant 0$. Si $ord_p(m) \geqslant 1$, alors*

$$1. \qquad (x)_m (x)_n \equiv (x)_{m+n} \mod \left(\tfrac{mn}{p}\right)\mathbb{Z}_p[x],$$

en particulier

$$2. \qquad (x)_m^n \equiv (x)_{mn} \mod \left(\tfrac{m^2}{p}\right)\mathbb{Z}_p[x].$$

Preuve. Nous avons $x^m \Phi((x)_n) = x^{m+n} = \Phi((x)_{m+n}) = \Phi((x)_m (x-m)_n)$ et par linéarité, il en découle

$$x^m \Phi(f(x)) = \Phi((x)_m f(x-m)) \text{ pour tout polynôme } f(x) \in \mathbb{Z}_p[x]. \qquad (*)$$

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

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

avec $A_k = \binom{n}{k}(m)_k = k!\binom{m}{k}\binom{n}{k}$. Pour tout $k \geqslant 1$, nous avons

$$\begin{aligned} ord_p(A_k) &= ord_p(k!) + ord_p(\tbinom{m}{k}) + ord_p(\tbinom{n}{k}) \\ &\geqslant (ord_p((k-1)!) + ord_p(k)) + (ord_p(m) - ord_p(k)) + (ord_p(n) - ord_p(k)) \\ &= ord_p(m) + ord_p(n) + ord_p((k-1)!) - ord_p(k) \\ &\geqslant ord_p(m) + ord_p(n) - 1, \end{aligned}$$

la dernière inégalité provenant du fait que $ord_p(k) \leqslant ord_p((k-1)!) + 1$. En fin de compte, nous obtenons $\Phi((x)_m(x)_n) \equiv x^{m+n} = \Phi((x)_{m+n}) \mod \left(\frac{mn}{p}\right)\mathbb{Z}_p[x]$, ce qui démontre la première affirmation. La deuxième assertion en découle, par induction sur $n \geqslant 1$. ∎

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

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

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

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

Au total, on obtient $(x)_{p^2} \equiv (x)_p^p \mod (p^2/2)\mathbb{Z}_p[x]$, c'est-à-dire $(x)_4 \equiv (x)_2^2 \mod 2\mathbb{Z}[x]$ et $(x)_{p^2} \equiv (x)_p^p \mod p^2\mathbb{Z}[x]$ pour p premier impair (ceci améliore légèrement le lemme 2 qui fournit cette même congruence modulo $p\mathbb{Z}_p[x]$). On conclut alors par induction sur $\nu = ord_p(n)$ à l'aide des deux lemmes précédents :

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

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

Le lemme 3 dit que $(x^p - x)^n \equiv (x)_{np} \mod np\mathbb{Z}_p$ pour p impair, la même congruence étant valable modulo $n\mathbb{Z}_2[x]$ lorsque $p = 2$. Nous distinguerons désormais ces deux cas mais nous présenterons les démontrations uniquement pour p impair, le lemme ci-dessus montrant comment traiter le cas $p = 2$.

3 Nombres et polynômes de Bell

Le lemme 3 (avec la relation $(*)$) fournit

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

Cette formule peut être généralisée comme suit.

Proposition. *Pour tous les entiers $n \geqslant 1$ et $\nu \geqslant 1$, nous avons*

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

pour p premier impair, la même congruence étant valable modulo $n\mathbb{Z}_2[x]$ si $p = 2$.

Preuve. Nous avons

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

En supposant que la proposition est vérifiée pour $\nu \geqslant 1$ et par le fait que

$$ord_p\Big(\tbinom{n}{k}\Big) \geqslant ord_p(n) - ord_p(k) \ \text{ pour } \ k = 1, \ldots, n,$$

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

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

Comme $(x^p-x)^{p^\nu} + (x^{p^\nu}-x) \equiv x^{p^{\nu+1}} - x \mod p\mathbb{Z}_p[x]$, on a (à l'aide du lemme 1)

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

et la proposition est ainsi démontrée pour $\nu+1$. ∎

Nous pouvons maintenant énoncer le résultat principal de cette note.

Théorème. *Soient $m, n \geqslant 0$ et $\nu \geqslant 1$ trois entiers. Pour un nombre premier p impair, les polynômes de Bell vérifient alors*

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

la même congruence étant valable modulo $n\mathbb{Z}_2[x]$ lorsque $p = 2$.

Preuve. Pour tout polynôme $f(x) \in \mathbb{Z}_p[x]$, on a

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

Par la proposition et par le fait que $ord_p(\binom{n}{k}) \geqslant ord_p(n) - ord_p(k)$ pour $k = 1, \ldots, n$, on obtient ainsi la congruence

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

Le théorème s'ensuit en considérant $f(x) = x^m$. ∎

On montre facilement que la formule d'inversion binomiale [1] est valable dans l'anneau $(\mathbb{Z}_p/np\mathbb{Z}_p)[x]$. En l'appliquant au théorème, nous obtenons une formulation duale :

Corollaire 1. *Sous les hypothèses du théorème, nous avons*

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

la même congruence étant valable modulo $n\mathbb{Z}_2[x]$ lorsque $p = 2$.

Pour p impair, le théorème fournit en particulier

$$B_{m+np^\nu} \equiv \sum_{k=0}^{n} \binom{n}{k} \nu^{n-k} B_{m+k} \mod np\mathbb{Z}_p.$$

Cette congruence, qui s'obtient également avec la formule de trace de Barsky-Benzaghou, généralise celles de Touchard ($B_{m+p} \equiv B_m + B_{m+1} \mod p\mathbb{Z}$), Radoux ($B_{m+p^\nu} \equiv B_{m+1} + \nu B_m \mod p\mathbb{Z}$) et Comtet-Zuber ($B_{np} \equiv B_{n+1} \mod np\mathbb{Z}_p$). On sait que les nombres de Bell vérifient une certaine périodicité dans tout corps fini (Carlitz). Le théorème qui vient d'être établi permet de généraliser également ce fait.

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

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

pour p premier impair, la même congruence étant valable modulo $n\mathbb{Z}_2$ si $p = 2$.

Preuve. Fixons un entier $a \in \mathbb{Z}$ et considérons l'opérateur linéaire

$$\Phi_a : \mathbb{Z}_p[x] \longrightarrow \mathbb{Z}_p[x],\ f(x) \longmapsto \Phi(f(x))\Big|_{x=a}.$$

Le théorème se formule alors (à l'aide du lemme 1)

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

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

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

1) Si p ne divise pas a, alors $x(x+a)(x+2a)\cdots(x+(p-1)a) \equiv x^p - x \mod p\mathbb{Z}[x]$ (les deux polynômes sont unitaires, de même degré, et ont les mêmes racines dans $\mathbb{F}_p$). Par le lemme 1, on a donc $(x(x+a)(x+2a)\cdots(x+(p-1)a))^n \equiv (x^p - x)^n \mod np\mathbb{Z}_p[x]$ et ainsi

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

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

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

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

Pour $k > 0$, on a $a^{kp} \equiv 0 \mod kp\mathbb{Z}_p$ par le lemme 1, de sorte que $\binom{n}{k} a^{kp} \equiv 0 \mod np\mathbb{Z}_p$ (puisque $ord_p(\binom{n}{k}) \geqslant ord_p(n) - ord_p(k)$), ce qui nous permet de conclure également dans ce cas. ∎

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

4 Nombres de Stirling

Le théorème principal de cette note permet d'obtenir naturellement de nouvelles congruences pour les nombres de Stirling. Par exemple, pour $\nu = 1$ et p impair, on peut expliciter

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

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

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

en rappelant que $\left\{ {i \atop j} \right\}$ est nul si $j < 0 \leqslant i$ ou si $j > i$.
En choisissant $n = p^a$ $(a \geqslant 0)$, on obtient en particulier

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

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

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

On voit apparaître ici les nombres de Stirling de première espèce $\left[{k \atop m} \right]$ et nous obtenons une généralisation d'un résultat de [5].
De même, si on considère $n = 1$ ($\nu = a \geqslant 1$ quelconque et p impair), le théorème fournit

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

Références

[1] M.Aigner, *Combinatorial Theory,* Springer-Verlag New York Inc, 1979.

[2] D.Barsky, *Analyse p-adique et nombres de Bell,* Comptes Rendus Acad. Sc. 282 série A (1976), 1257-1259.

[3] D.Barsky, B.Benzaghou, *Sommes de factorielles et nombres de Bell,* Preprint, 2001.

[4] A. Gertsch, A. Robert, *Some Congruences concerning the Bell Numbers,* Bull. Belg. Math. Soc. 3 (1996), 467-475.

[5] A. Gertsch, *Congruences pour quelques suites classiques de nombres, sommes de factorielles et calcul ombral,* Travail de doctorat, Université de Neuchâtel, février 1999.

[6] C. Radoux, *Nouvelles propriétés arithmétiques des nombres de Bell,* Sém. Delange-Pisot-Poitou, Univ. Paris VI, 16e année, exposé no 22, 1974-75.

[7] C. Radoux, *Nombres de Bell modulo p premier et extensions de degré p de* $\mathbf{F}_p$*,* Comptes Rendus Acad. Sc. 281 série A (1975), 879-882.

[8] C. Radoux, *Une congruence pour les polynômes* $P_n(x)$ *de fonction génératrice* $e^{x(e^z-1)}$*,* Comptes Rendus Acad. Sc. 284 série A (1977), 637-639.

[9] A. Robert, *A Course in p-adic Analysis,* GTM 198, Springer, 2000.

[10] S. Roman, G.-C. Rota, *The Umbral Calculus,* Advances in Math. 27 (1978), 95-188.

[11] G-C Rota, D. Kahaner, A. Odlyzko, *Finite Operator Calculus,* Journal of Mathematical Analysis and Applications, vol.42, no.3, juin 1973.

Institut de Mathématiques
Université de Neuchâtel
Rue Emile Argand 11
CH-2007 Neuchâtel