Some congruences concerning the Bell numbers

Anne Gertsch   Alain M. Robert

Abstract

In this Note we give elementary proofs – based on umbral calculus – of the most fundamental congruences satisfied by the Bell numbers and polynomials. In particular, we establish the conguences of Touchard, Comtet and Radoux as well as a (new) supercongruence conjectured by M. Zuber.

1 Some polynomial congruences

In this note, p will always denote a fixed prime number and A will either be the ring $\mathbf{Z}$ of integers or the ring $\mathbf{Z}_p$ of p-adic integers. Let $f(x), g(x) \in A[x]$ be two polynomials in one variable x and coefficients in the ring A.

LEMMA 1.1.- *If* $f(x) \equiv g(x) \mod p^\nu A[x]$ *for some integer* $\nu \geq 1$, *then*

$$f(x)^p \equiv g(x)^p \mod p^{\nu+1} A[x].$$

PROOF.- By hypothesis

$$f(x) = g(x) + p^\nu h(x) \quad \text{where} \quad h(x) \in A[x].$$

Hence

$$f(x)^p = (g(x) + p^\nu h(x))^p = g(x)^p + p^{\nu+1} r(x) \quad \text{with} \quad r(x) \in A[x],$$

and

$$f(x)^p \equiv g(x)^p \mod p^{\nu+1} A[x].$$

∎

Received by the editors November 1995.
Communicated by Y. Félix.
1991 *Mathematics Subject Classification* : Primary 11-B-73, 05-A-40 Secondary 11-P-83.
Key words and phrases : Bell polynomials, congruences, umbral calculus.

Let us consider a product of p consecutive p^ν-translates of a polynomial f

$$f(x)f(x-p^\nu)\dots f(x-(p-1)p^\nu) = \prod_{0\le k<p} f(x-kp^\nu).$$

We have then

Lemma 1.2.- *Let us assume that the prime p is odd. Then for any integer $\nu \geq 0$ the following congruence holds*

$$\prod_{0\le k<p} f(x-kp^\nu) \equiv f(x)^p \ \ mod\ p^{\nu+1}A[x].$$

Proof.- We have $f(x-kp^\nu) = f(x) - kp^\nu f'(x) + p^{2\nu}\alpha_{k,\nu}(x) \in A[x]$, with $\alpha_{k,\nu}(x)\in A[x]$. We infer

$$f(x-kp^\nu) \equiv f(x) - kp^\nu f'(x) \ \ mod\ p^{2\nu}A[x],$$

whence

$$\begin{aligned}\prod_{0\le k<p} f(x-kp^\nu) &\equiv f(x)^p - \sum_{0<k<p} kp^\nu f'(x)f(x)^{p-1} && mod\ p^{2\nu}A[x]\\ &\equiv f(x)^p - \frac{p-1}{2}p\cdot p^\nu f'(x)f(x)^{p-1} && mod\ p^{2\nu}A[x]\\ &\equiv f(x)^p && mod\ p^{\nu+1}A[x].\end{aligned}$$

∎

It is obvious here that for $p=2$ we only get

$$f(x)f(x-2^\nu)\equiv f(x)^2 \ \ mod\ 2^\nu A[x]$$

and we loose one factor 2 with respect to the case p odd.

Let us now consider the *Pochhammer* system of polynomials defined by

$$(x)_n = x(x-1)\dots(x-n+1)$$

for $n\in\mathbf{N}$ (with $(x)_0=1$ by convention). Thus $(x)_n$ is a unitary polynomial of degree n with integer coefficients. This system is a basis of the A-module $A[x]$.

Lemma 1.3.- *For $\nu\geq 1$, the polynomials $(x)_{p^\nu} = x(x-1)\dots(x-p^\nu+1)$ verify the following congruence*

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

Proof.- We proceed by induction on ν. The two polynomials $(x)_p$ and x^p-x have the same roots in the prime field $\mathbf{F}_p$ with p elements. Hence they coincide in the ring $\mathbf{F}_p[x]$. This proves the first step of the induction

$$(x)_p = x(x-1)\dots(x-p+1) \equiv x^p - x \ \ mod\ pA[x].$$

Suppose now $(x)_{p^\nu} \equiv (x^p - x)^{p^{\nu-1}}$ *mod* $p^\nu A[x]$, and apply lemma 1.2 to the polynomial $f(x) = (x)_{p^\nu}$. The equality

$$\begin{aligned}(x)_{p^{\nu+1}} &= (x)_{p^\nu}(x-p^\nu)_{p^\nu}(x-2p^\nu)_{p^\nu}\dots(x-(p-1)p^\nu)_{p^\nu}\\ &= \prod_{0\le k<p} f(x-kp^\nu)\end{aligned}$$

leads to the congruence $(x)_{p^{\nu+1}} \equiv (x)_{p^\nu}^p$ *mod* $p^{\nu+1}A[x]$. Applying lemma 1.1 to the induction hypothesis $(x)_{p^\nu} \equiv (x^p - x)^{p^{\nu-1}}$ *mod* $p^\nu A[x]$ we get

$$(x)_{p^\nu}^p \equiv (x^p - x)^{p^\nu} \ \ mod \ \ p^{\nu+1}A[x].$$

Finally, we have

$$(x)_{p^{\nu+1}} \equiv (x^p - x)^{p^\nu} \ \ mod \ \ p^{\nu+1}A[x]$$

as expected. ■

For $p = 2$ we have similarly

$$(x)_{2^\nu} \equiv (x^2 - x)^{2^{\nu-1}} \ \ mod \ \ 2^{\nu-1}A[x].$$

Acknowledgment.- We thank A. Valette who supplied a first proof (based on the Bauer congruence) of lemma 1.3.

2 Umbral calculus

Let us consider the A-linear operator

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

Since the A-module $A[x]$ is free with basis $((x)_n)_{n\ge 0}$ this indeed defines a unique isomorphism Φ.

Definitions.- 1) The n-th *Bell polynomial* $B_n(x)$ is the image of x^n by Φ.
2) The n-th *Bell number* B_n is defined by

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

Proposition 2.1.- *For* $f \in A[x]$ *and* $n \in \mathbf{N}$, *we have*

$$x^n\Phi(f) = \Phi\left((x)_n f(x-n)\right),$$

$$x \cdot \Phi((x+1)^n) = \Phi(x^{n+1}).$$

Proof.- It is clear that $(x)_{n+m} = (x)_n(x-n)_m$ whence

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

$$x^n\Phi\left((x)_m\right) = \Phi\left((x)_n(x-n)_m\right).$$

If $f(x) = \sum_{\text{finite}} c_m(x)_m$, $(c_m \in A)$ we deduce by linearity

$$x^n\Phi(f) = \Phi\left((x)_n f(x-n)\right)$$

which is the first equality. For $n=1$ we get in particular

$$x\Phi(f) = \Phi(xf(x-1))$$

and taking the polynomial $f(x) = (x+1)^n$ we find

$$x\Phi((x+1)^n) = \Phi(x \cdot x^n) = \Phi(x^{n+1}).$$

■

Corollary 2.2.- *The Bell polynomials can be computed inductively by means of the following recurrence relation*

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

starting with $B_0(x) = 1$.

Proof.- This follows simply from the linearity of the operator Φ and the binomial expansion $(x+1)^n = \sum_{0\le k\le n}\binom{n}{k} x^k$.

Corollary 2.3.- *Let p be an odd prime, $\nu \ge 1$ and $f \in A[x]$. Then we have a congruence*

$$\Phi\left((x^p - x)^{p^{\nu-1}} f\right) \equiv x^{p^\nu}\Phi(f) \ \ mod\ p^\nu A[x].$$

Proof.- Put $n = p^\nu$ in proposition 2.1 and reduce the equality modulo p^ν. We get

$$x^{p^\nu}\Phi(f) \equiv \Phi\left((x)_{p^\nu} f\right) \ \ mod\ p^\nu A[x].$$

On the other hand using lemma 1.3

$$(x)_{p^\nu} \equiv (x^p - x)^{p^{\nu-1}} \ \ mod\ p^\nu A[x],$$

we infer

$$x^{p^\nu}\Phi(f) \equiv \Phi\left((x^p - x)^{p^{\nu-1}} f\right) \ \ mod\ p^\nu A[x].$$

■

LEMMA 2.4.- *If* $S, T : A[x] \longrightarrow A[x]$ *are two commuting linear operators and* $\nu \geq 1$ *an integer such that*

$$\Phi(Sf) \equiv \Phi(Tf) \ \ mod \ p^\nu A[x] \quad for\ all \ \ f \in A[x],$$

then

$$\Phi(S^k f) \equiv \Phi(T^k f) \ \ mod \ p^\nu A[x] \quad for\ all \ \ k \in \mathbf{N} \quad and\ all \ \ f \in A[x].$$

PROOF.- We proceed by induction on k. The case $k = 1$ corresponds to the hypothesis of the lemma. Let us assume that the congruence

$$\Phi(S^{k-1} f) \equiv \Phi(T^{k-1} f) \ \ mod \ p^\nu A[x]$$

holds for all $f \in A[x]$. Then

$$\begin{aligned} \Phi(S^k f) = \Phi(S(S^{k-1} f)) &\equiv \Phi(T(S^{k-1} f)) = \Phi(S^{k-1}(Tf)) \quad mod \ p^\nu A[x] \\ &\equiv \Phi(T^{k-1}(Tf)) = \Phi(T^k f) \qquad mod \ p^\nu A[x]. \end{aligned}$$

■

3 The Radoux congruences for the Bell polynomials

PROPOSITION 3.1.- *For* $\nu \geq 1$ *and p prime, the following congruence holds*

$$B_{n+p^\nu}(x) \equiv B_{n+1}(x) + (x^p + \ldots + x^{p^\nu}) B_n(x) \ \ mod \ pA[x].$$

PROOF.- By corollary 2.3 (and also when $p = 2$ by the observation made after the proof of lemma 1.3) we have

$$\begin{aligned} \Phi\left((x^p - x) f\right) &\equiv x^p \Phi(f) \quad mod \ pA[x] \\ \Phi\left((x^p - x)^p f\right) &\equiv x^{p^2} \Phi(f) \quad mod \ pA[x] \\ &\vdots \\ \Phi\left((x^p - x)^{p^{\nu-1}} f\right) &\equiv x^{p^\nu} \Phi(f) \quad mod \ pA[x]. \end{aligned}$$

Use

$$(x^p - x)^{p^k} \equiv x^{p^{k+1}} - x^{p^k} \ \ mod \ pA[x],$$

and add the preceding congruences term by term. The telescoping sum reduces to

$$\Phi\left((x^{p^\nu} - x) f\right) \equiv (x^p + x^{p^2} + \ldots + x^{p^\nu}) \Phi(f) \ \ mod \ pA[x].$$

Taking $f(x) = x^n$ we obtain

$$B_{n+p^\nu}(x) - B_{n+1}(x) \equiv (x^p + \ldots + x^{p^\nu}) B_n(x) \ \ mod \ pA[x]$$

thereby proving the announced congruence (Radoux [4], [5]).

■

Corollary 3.2.- *We have*

$$B_{n+p}(x) \equiv B_{n+1}(x) + x^p B_n(x) \;\; mod \;\; pA[x],$$

$$\begin{aligned} B_{p^\nu}(x) &\equiv x + x^p + \ldots + x^{p^\nu} && mod \;\; pA[x] \\ &\equiv x + B_{p^{\nu-1}}(x^p) && mod \;\; pA[x]. \end{aligned}$$

Comment.- Since $x^n = \sum_{0\leq k\leq n} S_{k,n}(x)_n$ where the coefficients are the Stirling numbers (of the second kind), we also have $B_n(x) = \sum_{0\leq k\leq n} S_{k,n}x^n$. All congruences proved for the Bell polynomials concern congruences for the corresponding Stirling numbers. If we recall that $S_{k,n}$ represents the number of partitions of the set $\{1,\ldots,n\}$ into k non empty parts, we also deduce that $B_n = B_n(1) = \sum_k S_{k,n}$ represents the total number of partitions of $\{1,\ldots,n\}$.

4 A supercongruence for the Bell numbers

We are going to show that the congruence (Comtet [2])

$$B_{np} \equiv B_{n+1} \;\; mod \; p \quad (n \in \mathbf{N}, \; p \text{ odd})$$

in fact holds modulo higher powers of the prime p. This had been conjectured by M. Zuber (it seems to be the only general congruence modulo powers of primes that is known for the Bell numbers).

Introduce the linear form

$$\varphi : A[x] \longrightarrow A$$

defined by $\varphi(f) = \Phi(f)|_{x=1}$. It is characterized by $\varphi((x)_n) = 1 \;\; (n \in \mathbf{N})$ and the Bell numbers B_n can also be defined by $B_n = \varphi(x^n)$.

On $A[x]$, we consider the equivalence relations

$$f \overset{p^\nu}{\sim} g \quad \text{whenever} \quad \varphi(f) \equiv \varphi(g) \;\; mod \;\; p^\nu A.$$

Theorem 4.1.- *For $f \in A[x]$, $\nu \geq 1$ and an odd prime p, we have the following congruence*

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

Proof.- We proceed by induction on ν. For $\nu = 1$ $(x)_p \equiv x^p - x \;\; mod \;\; pA[x]$ whence

$$(x)_p f \equiv (x^p - x)f \;\; mod \;\; pA[x] \quad \text{for} \quad f \in A[x].$$

Moreover by proposition 2.1 (with $n = p$) $\Phi((x)_p f) \equiv x^p\Phi(f) \;\; mod \;\; pA[x]$. If we evaluate this at $x = 1$ we get $(x)_p f \overset{p}{\sim} f$. This proves $f \overset{p}{\sim} (x^p - x)f$, and

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

Assume now that the congruence $x^{p^n} f \overset{p^n}{\sim} (1+x)^{p^{n-1}} f$ holds for all $n \leq \nu$ and all $f \in A[x]$. There remains to prove that

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

Let us also recall corollary 2.3 (after evaluation at $x = 1$)

$$(*) \qquad f \overset{p^{\nu+1}}{\sim} (x^p - x)^{p^\nu} f$$

and expand $(x^p - x)^{p^\nu}$ with Newton's binomial formula

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

The binomial coefficients $\binom{p^\nu}{k}$ appearing under the summation sign are all divisible by p. More precisely, let us write their index k as $k = mp^\alpha$ with $0 \leq \alpha < \nu$ and m prime to p. Then

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

In lemma 2.4 take for S the operator of multiplication by $x^{p^{\alpha+1}}$ and for T the operator of multiplication by $(1+x)^{p^\alpha}$. Then the induction hypothesis for $f(x) = (-x)^{p^\nu - k}$ leads to

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

Hence

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

Altogether we have established

$$\sum_{k=1}^{p^\nu - 1} \binom{p^\nu}{k} x^{kp} (-x)^{p^\nu - k} \overset{p^{\nu+1}}{\sim} \sum_{k=1}^{p^\nu - 1} \binom{p^\nu}{k} (1+x)^k (-x)^{p^\nu - k}.$$

But the right hand side is also

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

Finally, use $(*)$

$$f \overset{p^{\nu+1}}{\sim} (x^p - x)^{p^\nu} f \overset{p^{\nu+1}}{\sim} \left(x^{p^{\nu+1}} - x^{p^\nu} + 1 - (1+x)^{p^\nu} + x^{p^\nu} \right) f.$$

Hence

$$f \overset{p^{\nu+1}}{\sim} x^{p^{\nu+1}} f + f - (1+x)^{p^\nu} f$$

and $x^{p^{\nu+1}} f \overset{p^{\nu+1}}{\sim} (1+x)^{p^\nu} f$ as wanted.

∎

Corollary 4.2.- *The Bell numbers satisfy the supercongruences*

$$B_{np} \equiv B_{n+1} \quad mod \;\; np\,\mathbf{Z}_p \quad (n \in \mathbf{N},\ p\ odd)$$

whereas for $p = 2$

$$B_{2n} \equiv B_{n+1} \quad mod \;\; n\mathbf{Z}_2.$$

In other words, if p^ν is the highest power of p that divides n, we have

$$B_{np} \equiv B_{n+1} \quad mod \;\; p^{\nu+1}$$

when p is odd and one power is lost when $p = 2$ (the comments in section 1 concerning the case $p = 2$ explain it).

Proof.- Let us write $n = kp^{\nu-1}$ with $k \in \mathbf{N}$, k prime to p, and $\nu \geq 1$. By theorem 4.1 and lemma 2.4

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

Taking for f the constant 1 we get $x^{kp^\nu} \overset{p^\nu}{\sim} (1+x)^{kp^{\nu-1}}$ namely $x^{np} \overset{p^\nu}{\sim} (1+x)^n$. This last expression means

$$\varphi\left(x^{np}\right) \equiv \varphi\left((1+x)^n\right) \quad mod \;\; np\,\mathbf{Z}_p.$$

Using the second equality of proposition 2.1 (evaluated at $x = 1$) we finally obtain

$$B_{np} \equiv B_{n+1} \quad mod \;\; np\,\mathbf{Z}_p.$$

■

References

[1] R.J. Clarke and M. Sved, *Derangements and Bell Numbers*, Math. Magazine 66 (1993), 299-303.

[2] L. Comtet, *Analyse combinatoire*, Presses Universitaires de France coll. SUP, le Mathématicien, I et II, 1970.

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

[4] 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.

[5] 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.

[6] J. Riordan, *Combinatorial Identities*, Wiley, New York, 1968.

[7] S. Roman, *The Umbral Calculus*, Academic Press, Orlando, FL, 1983.

[8] S. Roman, *The logarithmic binomial formula*, Amer. Math. Monthly 99 (1992), 641-648.

[9] S. Roman and G.-C. Rota, *The umbral calculus*, Advances in Math. 27 (1978), 95-188.

[10] G.-C. Rota, *The number of partitions of a set*, Amer. Math. Monthly 71 (1964), 498-504.

[11] L. Van Hamme, Problem no 6658 proposed in Amer. Math. Monthly 100 (1993), 953-954.

Institut de Mathématiques,
Emile-Argand 11,
CH-2007 Neuchâtel (Switzerland)