On Some Congruences for the Bell Numbers and for the Stirling Numbers

HIROFUMI TSUMURA

Aoyamagakuin Kotobu, 4-4-25 Shibuya Shibuya-ku, Tokyo, 150 Japan

Communicated by H. Zassenhaus

Received March 8, 1990

We shall give some congruences for the Bell numbers, and for the Stirling numbers, by investigating the elementary properties of $p$-adic integrals.

The Bell numbers $B(n)$ and the second kind of Stirling numbers $S(n, k)$ are defined by

$$\text{Exp}(e^t - 1) = \sum_{n=0}^{\infty} B(n) \frac{t^n}{n!},$$

and

$$\frac{(e^t - 1)^k}{k!} = \sum_{n=0}^{\infty} S(n, k) \frac{t^n}{n!},$$

for $k \geq 1$. These numbers are classical and important in number theory and in combinatorial analysis. Many authors investigated some properties of these numbers. But few congruences for them could be obtained.

In the present paper, we fix a prime number $p$ and prove the following congruences for these numbers.

**THEOREM A.** Suppose $n \geq 1$; then

$$B(p^n) \equiv (B(p) - 1)n + 1 \pmod{p}.$$  

**THEOREM B.** Suppose $0 \leq m \leq n$ and $m \equiv n \pmod{(p - 1)p^r}$, and put $N(k) = \min(m, e + 1)$. If $N(k) > 0$ then

$$S(m, k) \equiv S(n, k) \pmod{p^{N(k)}}.$$
Notation. Let $p$ be a prime number and $q = p$ for $p > 2$ ($q = 4$ for $p = 2$).

Let $\mathbb{Q}_p$ be the field of $p$-adic numbers, $\mathbb{Z}_p$ be the ring of $p$-adic integers, $\mathbb{Z}_p^*$ be the group of units in $\mathbb{Z}_p$, $v_p$ be the $p$-adic valuation on $\mathbb{Z}_p$ normalized by $v_p(p) = 1$, $| \cdot |$ be the $p$-adic absolute value which is equal to $p^{-v_p(\cdot)}$, and $W$ be the group of $(p - 1)$th root of unity in $\mathbb{Z}_p$. Then $\mathbb{Z}_p^* = W \times (1 + q\mathbb{Z}_p)$; $x = w(x)\langle x \rangle$, where $w(x)$ (resp. $\langle x \rangle$) denotes the projection of $x$ onto $W$ (resp. $1 + q\mathbb{Z}_p$). Let $R[T]$ be the ring of polynomials for a ring $R$, $R(T)$ be the rational function field of $R$, $R[[T - 1]]$ be the ring of power series of $(T - 1)$ and $\# S$ be the number of elements of the set $S$.

1. $p$-Adic Measures and Power Series

Let $K$ be a finite extension of $\mathbb{Q}_p$, and $\Theta$ be the ring of $p$-adic integers in $K$. Let $\{a_n\}$ be a sequence of rational numbers, and $A(t)$ be the generating function of $\{a_n\}$ as follows: $A(t) = \sum_{n \geq 0} a_n t^n/n!$. We assume that $A(t)$ is a rational function of $e^t$. Hence we can take a rational function $C(T) \in \Theta(T)$ with

$$A(t) = C(e^t).$$

Moreover, we assume that we can regard $C(T)$ as an element of $\Theta[[T - 1]]$. As is well known, we have the one-to-one correspondences as follows (see [4, Chap. 12]):

$$\Theta\text{-valued measures on } \mathbb{Z}_p \leftrightarrow \Theta[[T - 1]].$$

Let $\alpha$ be a $\Theta$-valued measure on $\mathbb{Z}_p$ which corresponds to $C(T)$; then

$$C(T) = \int_{\mathbb{Z}_p} T^\alpha \ d\alpha(z).$$

By considering the $n$th derivatives, it follows from (1) and (2) that

$$\int_{\mathbb{Z}_p} z^n \ d\alpha(z) = a_n,$$

for $n \geq 0$. Now we define the functions

$$f(s, \omega^i, \alpha) = \int_{\mathbb{Z}_p} \langle x \rangle^{-s} \omega^i(x) \ d\alpha(x),$$

for $s \in \mathbb{Z}_p$, and $i = 0, 1, \ldots, p - 2$. Note that $f(s, \omega^i, \alpha)$ is called a $p$-adic $T$-transform. So we can see that $f(s, \omega^i, \alpha)$ is a $p$-adic analytic function on $\mathbb{Z}_p$ (see [4]).
For a non-positive integer $n$ with $n \equiv i \pmod{p-1}$ and $0 \leq i < p-1$,
\[
 f(-n, \omega', x) = \int_{\mathbb{Z}_p} x^n d\alpha(x) - \int_{p\mathbb{Z}_p} x^n d\alpha(x). \tag{5}
\]
Since $\alpha$ is a $\Theta$-valued measure, we can see that
\[
 \int_{p\mathbb{Z}_p} x^n d\alpha(x) \equiv 0 \pmod{p^n}, \tag{6}
\]
from the definition of $p$-adic integrals. By (3), (5), and (6), we have
\[
 f(-n, \omega', x) \equiv a_n \pmod{p^n}. \tag{7}
\]
On the other hand, we see that
\[
 f(-m, \omega', x) \equiv f(-n, \omega', x) \pmod{p^{n+1}}, \tag{8}
\]
for $0 \leq m \leq n$ with $m \equiv n \pmod{(p-1)p^e}$ and for $0 \leq i < p-1$ with $m \equiv n \equiv i \pmod{p}$ (see [3, Theorem 1]).
By (7) and (8), we obtain the following lemma.

**Lemma 1.** In the above notations,
\[
 a_m \equiv a_n \pmod{p^N},
\]
where $N = \min(m, e+1)$.

**2. Proofs of Theorems**

Let $C(T) = \exp(p(T-1))$; then we can see that $C(T) \in \mathbb{Z}_p[[T-1]]$, since $v_p(n!) \leq n/(p-1)$ for $n \geq 1$. We define the $p$-multiple Bell numbers $P(n, p)$ by
\[
 C(e') = \sum_{n=0}^{\infty} P(n, p) \frac{t^n}{n!}. \tag{9}
\]
From the definition of the Bell numbers, we have
\[
 P(n, p) = \sum_{n_1=0}^{n} \sum_{n_2=0}^{n_1} \cdots \sum_{n_{p-1}=0}^{n_{p-2}} \prod_{j=1}^{p-1} \binom{n}{n_j} B(n_{p-j} - n_{p-j-1}), \tag{10}
\]
where $\binom{n}{k}$ is the combination function.
From Lemma 1, we obtain the following:

PROPOSITION 1. Suppose $0 \leq m \leq n$ and $m \equiv n \pmod{(p-1)p^e}$; then

$$P(m, p) \equiv P(n, p) \pmod{p^N},$$

for $N = \text{Min}(m, e + 1)$.

For $0 \leq n_1 \leq n_2 \leq \cdots \leq n_{p-1} \leq p^k$, let $j_1 = p^k - n_1, j_2 = n_1 - n_2, \ldots, j_{p-1} = n_{p-2} - n_{p-1}, j_p = n_{p-1}$. Then

$$\left| \begin{array}{c|c|c|c|c|c} p^k \\ n_1 \\ n_2 \\ \vdots \\ n_{p-2} \\ n_{p-1} \end{array} \right| = \frac{p^k!}{j_1!j_2!\cdots j_p!}. \quad (11)$$

From (10), we have

$$P(p^k, p) = \sum_{j_1 \geq 0} \sum_{j_2 \geq 0} \cdots \sum_{j_{p-1} \geq 0} \sum_{j_{p} \geq 0} \frac{p^k!}{j_1!j_2!\cdots j_p!} B(j_1) \cdots B(j_p). \quad (12)$$

Now we permute the set $\{j_1, j_2, \ldots, j_p\}$ in a bigger order, and denote this permuted set by $J(j_1, j_2, \ldots, j_p)$. Let $S = \{0, 1, 2, \ldots, p^k\}$, $S^p$ be the $p$-tuple direct sum of $S$, and $T = \{[t_1, \ldots, t_p] \in S^p; 0 \leq t_1 \leq \cdots \leq t_p, t_1 + t_2 + \cdots + t_p = p^k\}$. Then we have

$$P(p^k, p) = \sum_{[t_1, \ldots, t_p] \in T} \frac{p^k!}{t_1! \cdots t_p!} R(t_1) \cdots R(t_p) \times A(t_1, \ldots, t_p), \quad (13)$$

where $A(t_1, \ldots, t_p) = \# \{\{j_1, \ldots, j_p\} \in S^p; J(j_1, \ldots, j_p) = [t_1, \ldots, t_p]\}$.

LEMMA 2. Suppose $[t_1, \ldots, t_p] \in T$; then $A(t_1, \ldots, t_p) \equiv 0 \pmod{p}$, with the exception of the case $t_1 = \cdots = t_p = p^{k-1}$.

Proof. Suppose $t_1 = \cdots = t_m \neq t_{m+1}$ for $1 \leq m < p$; then

$$A(t_1, \ldots, t_p) = \left| \begin{array}{cccc} p^k \\ m \end{array} \right| \equiv 0 \pmod{p}. \quad \blacksquare$$

LEMMA 3. Suppose $[t_1, \ldots, t_p] \in T$, then $p^{k!} / t_1! \cdots t_p! \equiv 0 \pmod{p}$, with the exception of the cases $t_1 = \cdots = t_{p-1} = 0$ and $t_p = p^k$.

Proof. Suppose $t_1 = \cdots = t_m = 0$ and $t_m \neq 0$ for $1 \leq m < p$. Determine $n_1, n_2, \ldots, n_{p-1}$ by $p^k - n_1 = t_1, n_1 - n_2 = t_2, \ldots, n_{p-2} - n_{p-1} = t_{p-1}$, and $n_{p-1} = t_{p-1}$. Then $n_1 = n_2 = \cdots = n_{m-1} = p^k$ and $n_m \neq p^k$. So

$$\frac{p^k!}{t_1! \cdots t_p!} = \left| \begin{array}{cccc} p^k \\ n_1 \\ n_2 \\ \vdots \\ n_m \\ \vdots \end{array} \right| \equiv 0 \pmod{p}. \quad \blacksquare$$
Proof of Theorem A. By using the above lemmas and (13),

\[ P(p^k, p) \equiv pB(p^k) + \frac{p^k!}{\{(p^k-1)\}^p} B(p^{k-1})^p \pmod{p^2}. \]  \hfill (14)

Note that

\[ \frac{p^k!}{\{(p^k-1)\}^p} = \begin{vmatrix} p^k & (p-1)p^{k-1} & \cdots & 2p^{k-1} \\ p^{k-1} & \cdots & \cdots & \cdots \\ \vdots & \cdots & \cdots & \cdots \\ p & \cdots & \cdots & \cdots \end{vmatrix}. \]  \hfill (15)

Suppose \( 1 \leq i < p \) and \( 1 \leq j < ip^k \); then

\[ v_p \left( \binom{ip^k}{j} \right) = v_p(ip^k) - v_p(j). \]

Hence we can see that the right-hand side of (15) \( \equiv 0 \pmod{p} \) and \( \not\equiv 0 \pmod{p^2} \). On the other hand, it follows from Proposition 1 that

\[ P(p^k, p) \equiv P(p^l, p) \pmod{p^k}, \]  \hfill (16)

for \( 1 \leq k \leq j \). By (14)–(16), we obtain

\[ B(p^k) + 1 \left\{ p^k \left| \frac{p^k}{p^{k-1}} \right| \left( \frac{p-1}{p} \right) p^{k-1} \right. \left| \frac{2p^{k-1}}{p^{k-1}} \right| \cdots \right. \left| \frac{p}{p-1} \right| \left| \frac{B(p^{k-1})^p}{B(p^{k-1})^p} \right. \equiv B(p^l) + 1 \left\{ p^l \left| \frac{p^l}{p^{l-1}} \right| \left( \frac{p-1}{p} \right) p^{l-1} \right. \left| \frac{2p^{l-1}}{p^{l-1}} \right| \cdots \right. \left| \frac{p}{p-1} \right| \left| \frac{B(p^{l-1})^p}{B(p^{l-1})^p} \right. \pmod{p} \]  \hfill (17)

for \( 1 \leq k \leq j \). Suppose \( 1 \leq i < p \) and \( k \geq 1 \); then

\[ \left( \frac{ip^{k-1}}{p^{k-1}} \right) \equiv i \pmod{p}, \]  \hfill (18)

and

\[ \frac{1}{p} \left| \frac{p^k}{p^{k-1}} \right| \equiv 1 \pmod{p}. \]  \hfill (19)

Moreover it follows from Wilson's Theorem that

\[ (p-1)! \equiv -1 \pmod{p}. \]  \hfill (20)

By combining (17)–(20), we get

\[ B(p^k) - B(p^{k-1})^p \equiv B(p^l) - B(p^{l-1})^p \pmod{p}, \]
for $1 \leq k \leq j$. Note that $B(p^{k-1})^p \equiv B(p^{k-1}) \pmod{p}$ in both of the following cases: $B(p^{k-1}) = 0$ and $\not\equiv 0 \pmod{p}$. Note that $B(p^0) = 1$. So inductively, we have the proof of Theorem A. 

Remark. Suppose $p = 2$. Since $B(2) = 2$, $B(2^n) \equiv n + 1 \pmod{2}$. So $B(2^n)$ is odd if and only if $n$ is even. In fact, the stronger results were proved in [1].

Proof of Theorem B. Let $r(k) = v_p(k!)$, and $C(T) = p^{r(k)}(T-1)^k/k!$ for $k \geq 1$. Then $C(T) \in \mathbb{Z}_p[[T-1]]$. Since

$$C(e^T) = \sum_{n=0}^{\infty} p^{r(k)} S(n, h) \frac{t^n}{n!},$$

it follows from Lemma 1 that we obtain the proof of Theorem B. 

REFERENCES

1. N. BALASUBRAMANIAN. On the numbers defined by $N_n = (1/e) \sum n^n/n!$. Math. Student 18 (1950), 130–132.