Bull. Aust. Math. Soc. **84** (2011), 153–158
doi:10.1017/S0004972711002218

ON A CURIOUS PROPERTY OF BELL NUMBERS

ZHI-WEI SUN ✉ and DON ZAGIER

(Received 27 November 2010)

Abstract

In this paper we derive congruences expressing Bell numbers and derangement numbers in terms of each other modulo any prime.

2010 *Mathematics subject classification*: primary 11B73; secondary 05A15, 05A18, 11A07.
Keywords and phrases: Bell numbers, derangement numbers, congruences modulo a prime.

1. Introduction

Let B_n denote the nth Bell number, defined as the number of partitions of a set of cardinality n (with $B_0 = 1$). In 1933 Touchard [2] proved that for any prime p we have

$$B_{p+n} \equiv B_n + B_{n+1} \pmod{p} \quad \text{for all } n = 0, 1, 2, \ldots. \tag{1.1}$$

Thus it is natural to look at the numbers $B_n \pmod{p}$ for $n < p$. In [1], the first author discovered experimentally that for a fixed positive integer m the sum $\sum_{n=0}^{p-1} B_n/(-m)^n$ modulo a prime p not dividing m is an integer independent of the prime p, a typical case being

$$\sum_{n=0}^{p-1} \frac{B_n}{(-8)^n} \equiv -1853 \pmod{p} \quad \text{for all primes } p \neq 2.$$

In this note we will prove this fact and give some related results.

Our theorem involves another combinatorial quantity, the derangement number D_n, defined either as the number of fixed-point-free permutations of a set of cardinality n (with $D_0 = 1$) or by the explicit formula

$$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \quad (n = 0, 1, 2, \ldots). \tag{1.2}$$

The first author is supported by the National Natural Science Foundation (grant 10871087) and the Overseas Cooperation Fund (grant 10928101) of China.

© 2011 Australian Mathematical Publishing Association Inc. 0004-9727/2011 $16.00

https://doi.org/10.1017/S0004972711002218 Published online by Cambridge University Press

THEOREM 1.1. *For every positive integer m and any prime p not dividing m we have*

$$\sum_{0<k<p} \frac{B_k}{(-m)^k} \equiv (-1)^{m-1} D_{m-1} \pmod{p}. \tag{1.3}$$

Using $\sum_{0<m<p}(-m)^{n-k} \equiv -\delta_{n,k} \pmod{p}$ for $k, n \in \{1, \ldots, p-1\}$, we immediately obtain a dual formula for B_n $(n < p)$ in terms of $D_0, \ldots, D_{p-2}$.

COROLLARY 1.2. *Let p be any prime. Then for all $n = 1, \ldots, p-1$ we have*

$$(-1)^n B_n \equiv \sum_{m=1}^{p-1} (-1)^m m^n D_{m-1} \pmod{p}.$$

Combining the case $n = p-1$ of this corollary with the congruence

$$\sum_{k=0}^{p-1} (-1)^k D_k \equiv \sum_{k=0}^{p-1} \binom{p-1}{k} D_k = (p-1)! \equiv -1 \pmod{p},$$

we get the following further consequence of Theorem 1.1.

COROLLARY 1.3. *For any prime p we have*

$$B_{p-1} \equiv D_{p-1} + 1 \pmod{p}.$$

For the reader's convenience we give a small table of values of B_n and D_n.

n	0	1	2	3	4	5	6	7	8
B_n	1	1	2	5	15	52	203	877	4140
D_n	1	0	1	2	9	44	265	1854	14833

We will prove Theorem 1.1 in the next section and derive an extension of it in Section 3.

2. Proof of Theorem 1.1

We first observe that it suffices to prove (1.3) for $0 < m < p$, since both sides are periodic in m (mod p) with period p. For the left-hand side this is obvious and for the right-hand side it follows from (1.2), which gives the expression $(-1)^n D_n \equiv \sum_{r=0}^{\infty}(-1)^r \prod_{0\le s<r}(n-s) \pmod{p}$ for D_n (mod p) as the sum of a terminating infinite series of polynomials in n.

We will prove (1.3) for $0 < m < p$ by induction on m. Denote by S_m the sum on the left-hand side of (1.3), where we consider the prime p as fixed and omit it from the notation. Since $D_n = nD_{n-1} + (-1)^n$ for $n = 1, 2, 3, \ldots$ (obvious from (1.2)), we have to prove the two formulas

$$S_1 \equiv 1 \pmod{p}, \qquad mS_m \equiv S_1 - S_{m+1} \pmod{p}. \tag{2.1}$$

https://doi.org/10.1017/S0004972711002218 Published online by Cambridge University Press

Recall that the Bell numbers can be given by the generating function

$$\sum_{n=0}^{\infty} B_n \frac{x^n}{n!} = e^{e^x - 1}, \tag{2.2}$$

equivalent to the well-known closed formula

$$B_n = \frac{1}{e} \sum_{r=0}^{\infty} \frac{r^n}{r!}.$$

Since the function $y = e^{e^x - 1}$ satisfies $y' = e^x y$, this also gives the recursive definition

$$B_0 = 1, \quad B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k \quad \text{for all } n \geq 0. \tag{2.3}$$

This recursion is the key ingredient in proving (2.1).

For the first formula in (2.1) we use (2.3) with $n = p - 1$ to obtain

$$S_1 = \sum_{k=1}^{p-1} (-1)^k B_k \equiv \sum_{k=1}^{p-1} \binom{p-1}{k} B_k = B_p - B_0 \pmod{p},$$

so it suffices to prove that $B_p \equiv 2 \pmod{p}$. This is a special case of Touchard's congruence (1.1), but can also be seen by writing (2.2) in the form

$$\sum_{n=0}^{\infty} B_n \frac{x^n}{n!} = e^x + \sum_{1<r<p} \frac{(e^x - 1)^r}{r!} + \frac{x^p}{p!} + \mathrm{O}(x^{p+1})$$

to get $B_p/p! = 1/p! + (p\text{-integral}) + 1/p!$.

Now using Fermat's little theorem and (2.3), we obtain

$$\begin{aligned} -mS_m &\equiv \sum_{n=0}^{p-2} (-m)^{p-1-n} \sum_{k=0}^{n} \binom{n}{k} B_k \\ &\equiv \sum_{k=0}^{p-2} (-1)^k B_k \sum_{r=0}^{p-k-2} \binom{p-k-1}{r} m^{p-k-1-r} \qquad (r = n - k) \\ &\equiv \sum_{k=0}^{p-2} (-1)^k B_k ((m+1)^{p-1-k} - 1) \equiv S_{m+1} - S_1 \pmod{p} \end{aligned}$$

for $1 \leq m \leq p - 2$. This completes the proof of (2.1) and the theorem.

3. An extension of Theorem 1.1

We now give an extension of Theorem 1.1 from the Bell numbers B_n to the *Touchard polynomial* $T_n(x)$, defined by

$$T_n(x) = \sum_{k=0}^{n} S(n, k) x^k. \tag{3.1}$$

https://doi.org/10.1017/S0004972711002218 Published online by Cambridge University Press

The numbers $S(n, k)$ occurring here are the Stirling numbers of the second kind, which can be defined in at least four different ways:

- combinatorially as the number of partitions of a set of n elements into k nonempty subsets;
- by the generating function

$$\sum_{n=0}^{\infty} S(n, k)\frac{x^n}{n!} = \frac{(e^x - 1)^k}{k!} \quad (k \geq 0); \tag{3.2}$$

- by the recursion relation

$$S(n, k) = kS(n - 1, k) + S(n - 1, k - 1) \quad (n, k \geq 1) \tag{3.3}$$

together with the initial conditions $S(n, 0) = S(0, n) = \delta_{n,0}$;

- by the closed formula

$$S(n, k) = \sum_{j=0}^{k} \frac{(-1)^{k-j} j^n}{j!(k - j)!}. \tag{3.4}$$

From the first or third of these we see that $T_n(1) = B_n$, so the following result includes Theorem 1.1 as the special case $x = 1$.

THEOREM 3.1. *For any prime number p and any positive integer m not divisible by p,*

$$(-x)^m \sum_{0<n<p} \frac{T_n(x)}{(-m)^n} \equiv -x^p \sum_{l=0}^{m-1} \frac{(m - 1)!}{l!}(-x)^l \pmod{p\mathbb{Z}_p[x]}, \tag{3.5}$$

where $\mathbb{Z}_p$ denotes the ring of p-adic integers.

Observe that this congruence of polynomials implies the congruence

$$\sum_{0<n<p} \frac{T_n(x)}{(-m)^n} \equiv \frac{1}{(-x)^{m-1}} \sum_{l=0}^{m-1} \frac{(m - 1)!}{l!}(-x)^l \pmod{p}$$

for any p-adic integer x not divisible by p, special cases being

$$\sum_{0<n<p} \frac{T_n(x)}{(-2)^n} \equiv \frac{x - 1}{x} \pmod{p} \quad \text{for } p \neq 2,$$

$$\sum_{0<n<p} \frac{T_n(x)}{(-3)^n} \equiv \frac{x^2 - 2x + 2}{x^2} \pmod{p} \quad \text{for } p \neq 3,$$

$$\sum_{0<n<p} \frac{T_n(x)}{(-4)^n} \equiv \frac{x^3 - 3x^2 + 6x - 6}{x^3} \pmod{p} \quad \text{for } p \neq 2.$$

PROOF OF THEOREM 3.1. One can prove Theorem 3.1 by a slight modification of the argument used for Theorem 1.1, replacing the recursion (2.3) for the Bell numbers by

https://doi.org/10.1017/S0004972711002218 Published online by Cambridge University Press

the analogous recursion

$$T_0(x) = 1, \quad T_{n+1}(x) = x \sum_{k=0}^{n} \binom{n}{k} T_k(x) \quad \text{for } n \geq 0$$

for the Touchard polynomials. But it is in fact easier to prove this congruence of polynomials for each coefficient separately. We first observe that, just as in the case of Theorem 1.1, it suffices to consider m among $1, \ldots, p-1$, since by setting $l = m - 1 - r$ we can rewrite (3.5) in the form

$$\sum_{0<n<p} \frac{T_n(x)}{(-m)^n} \equiv \sum_{r=0}^{\infty} \biggl(\prod_{1 \leq s \leq r} (m-s) \biggr) (-x)^{p-1-r} \pmod{p\mathbb{Z}_p[x][\![x^{-1}]\!]}$$

in which both sides depend only on $m \pmod{p}$. (Note that the expression on the right is a polynomial modulo p, since $\prod_{1 \leq s \leq r}(m-s)$ is divisible by p for $r \geq p$.) Comparing the coefficients of x^k on both sides of this identity, we see that it suffices to prove the congruence

$$\sum_{n=k}^{p-1} \frac{S(n,k)}{(-m)^n} \equiv \prod_{0<s<p-k} (s-m) \pmod{p} \tag{3.6}$$

for m and k in $\{1, \ldots, p-1\}$. We can do this in two different ways.

- By downward induction on k. For $k = p-1$ both sides of (3.6) reduce to 1 modulo p, and from the recursion (3.3) we get

$$\begin{aligned} \sum_{n=k-1}^{p-1} \frac{S(n,k-1)}{(-m)^n} &= \sum_{n=k-1}^{p-1} \frac{S(n+1,k) - kS(n,k)}{(-m)^n} \\ &\equiv (-m-k) \sum_{n=k}^{p-1} \frac{S(n,k)}{(-m)^n} \pmod{p} \end{aligned}$$

  for $1 < k < p$, showing that the truth of (3.6) for k implies its truth for $k-1$. Here we have used the fact that $S(p,k) \equiv 0 \pmod{p}$ for $1 < k < p$, which can be seen either from the combinatorial definition of the Stirling numbers (the group $\mathbb{Z}/p\mathbb{Z}$ acts freely by translation on the set of its partitions into k nonempty subsets, so $p | S(p,k)$) or else from the generating function (3.2) (because the coefficient of x^p on the right-hand side of (3.2) is p-integral for $1 < k < p$).
- From the closed formula (3.4) for $S(n,k)$ together with the easily verified fact that $\sum_{0<n<p}(-j/m)^n$ is congruent to $-1 \pmod{p}$ if $j \equiv -m \pmod{p}$ and to $0 \pmod{p}$ otherwise. This gives

$$\sum_{0<n<p} \frac{S(n,k)}{(-m)^n} \equiv \frac{(-1)^{k+m}}{k!} \binom{k}{p-m} \pmod{p}$$

https://doi.org/10.1017/S0004972711002218 Published online by Cambridge University Press

for k and m in the range under consideration. If $k < p - m$ then

$$\binom{k}{p-m} = 0 \quad \text{and} \quad \prod_{0<s<p-k} (s-m) = 0.$$

If $k + m \geq p$, then the congruence that we have to prove is

$$\frac{(-1)^{k+m}}{(p-m)!(k+m-p)!} \equiv (-1)^k \frac{(m-1)!}{(k+m-p)!} \pmod{p},$$

and this is clear since $\binom{p-1}{m-1} \equiv (-1)^{m-1} \equiv (-1)^m (p-1)! \pmod{p}$. This completes the proof of (3.6) and of Theorem 3.1. □

Acknowledgements

This work was done during the authors' visit to the National Center for Theoretical Sciences (Hsinchu, Taiwan). Both authors are indebted to Professor Wen-Ching Winnie Li for the kind invitation and to the Center for its financial support.

References

[1] Z. W. Sun, 'A conjecture on Bell numbers' (a message to Number Theory List), http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1007&L=nmbrthry&T=0&P=1066.

[2] J. Touchard, 'Propriétés arithmétiques de certains nombres recurrents', *Ann. Soc. Sci. Bruxelles* **53A** (1933), 21–31.

ZHI-WEI SUN, Department of Mathematics, Nanjing University, Nanjing 210093,
PR China
e-mail: zwsun@nju.edu.cn

DON ZAGIER, Max-Planck-Institut für Mathematik, 53111 Bonn, Germany
and
Collège de France, 75005 Paris, France
e-mail: don.zagier@mpim-bonn.mpg.de

https://doi.org/10.1017/S0004972711002218 Published online by Cambridge University Press