CONGRUENCES FOR BELL AND TANGENT NUMBERS

IRA GESSEL
Massachusetts Institute of Technology, Cambridge, MA 02139

1. INTRODUCTION

The Bell numbers B_n defined by

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

and the tangent numbers T_n defined by

$$\sum_{n=0}^{\infty} T_n \frac{x^n}{n!} = \tan x$$

are of considerable importance in combinatorics, and possess interesting number-theoretic properties. In this paper we show that for each positive integer n, there exist integers $a_0, a_1, \ldots, a_{n-1}$ and $b_1, b_2, \ldots, b_{n-1}$ such that for all $m \geq 0$,

$$B_{m+n} + a_{n-1}B_{m+n-1} + \cdots + a_0 B_m \equiv 0 \pmod{n!}$$

and

$$T_{m+n} + b_{n-1}T_{m+n-1} + \cdots + b_1 T_{m+1} \equiv 0 \pmod{(n-1)!n!}.$$

Moreover, the moduli in these congruences are best possible. The method can be applied to many other integer sequences defined by exponential generating functions, and we use it to obtain congruences for the derangement numbers and the numbers defined by the generating functions $e^{x+x^2/2}$ and $(2 - e^x)^{-1}$.

2. THE METHOD

A *Hurwitz series* [5] is a formal power series of the form

$$\sum_{n=0}^{\infty} a_n \frac{x^n}{n!},$$

where the a_n are integers. We will use without further comment the fact that Hurwitz series are closed under multiplication, and that if f and g are Hurwitz series and $g(0) = 0$, then the composition $f \circ g$ is a Hurwitz series. In particular, $g^k/k!$ is a Hurwitz series for any nonnegative integer k. We will work with Hurwitz series in two variables, that is, series of the form

$$\sum_{m,n=0}^{\infty} a_{mn} \frac{x^m}{m!} \frac{y^n}{n!},$$

where the a_{mn} are integers. The properties of these series that we will need follow from those for Hurwitz series in one variable.

The exact procedure we follow will vary from series to series, but the general outline is as follows: The kth derivative of the Hurwitz series

$$f(x) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!} \quad \text{is} \quad f^{(k)}(x) = \sum_{n=0}^{\infty} a_{n+k} \frac{x^n}{n!}$$

Our goal is to find some linear combination with integral coefficients of

$$f(x), f'(x), \ldots, f^{(n)}(x)$$

all of whose coefficients are divisible by $n!$ (or in some cases a larger number). To do this we use Taylor's theorem

$$f(x + y) = \sum_{k=0}^{\infty} f^{(k)}(x)\frac{y^k}{k!}.$$

We then make the substitution $y = g(z)$ and multiply by some series $h(z)$ to get

$$h(z)f[x + g(z)] = \sum_{k=0}^{\infty} f^{(k)}(x)h(z)\frac{[g(z)]^k}{k!}.$$

If $h(z)$ and $g(z)$ are chosen appropriately, the coefficient of $\frac{x^m}{m!}z^n$ on the left will be integral. Then the coefficient of $\frac{x^m}{m!}\frac{z^n}{n!}$ on the right is divisible by $n!$, and we obtain the desired congruence.

3. BELL NUMBERS

We define the *exponential polynomials* $\phi_n(t)$ by

$$\sum_{n=0}^{\infty} \phi_n(t)\frac{x^n}{n!} = e^{t(e^x - 1)}.$$

Thus

$$\phi_n(1) = B_n \quad \text{and} \quad \phi_n(t) = \sum_{k=0}^{\infty} S(n, k)t^k,$$

where $S(n, k)$ is the Stirling number of the second kind. We will obtain a congruence for the exponential polynomials that for $t = 1$ reduces to the desired Bell number congruence.

We set

$$f(x) = e^{t(e^x - 1)} = \sum_{n=0}^{\infty} \phi_n(t)\frac{x^n}{n!}.$$

Then

$$\begin{aligned} f(x + y) &= \exp\,[t(e^{x+y} - 1)] = \exp\,[t(e^x - 1) + t(e^y - 1)e^x] \\ &= f(x)\,\exp\,[t(e^y - 1)e^x]. \end{aligned}$$

Now set $y = \log(1 + z)$. We then have

$$\sum_{k=0}^{\infty} f^{(k)}(x)\frac{[\log(1 + z)]^k}{k!} = f(x)e^{tze^x}.$$

Multiplying both sides by e^{-tz}, we obtain

$$\sum_{k=0}^{\infty} f^{(k)}(x)e^{-tz}\frac{[\log(1 + z)]^k}{k!} = f(x)e^{tz(e^x - 1)} = \sum_{n=0}^{\infty} z^n t^n f(x)\frac{(e^x - 1)^n}{n!}. \tag{1}$$

Now define polynomials $D_{n,k}(t)$ by

$$e^{-tz}\,\frac{[\log(1 + z)]^k}{k!} = \sum_{n=k}^{\infty} D_{n,k}(t)\frac{z^n}{n!}. \tag{2}$$

[Note that $D_{n,n}(t) = 1$.] Then the left side of (1) is

$$\sum_{k=0}^{\infty} f^{(k)}(x)\sum_{n=0}^{\infty} D_{n,k}(t)\frac{z^n}{n!} = \sum_{m,n=0}^{\infty} \frac{x^m}{m!}\frac{z^n}{n!}\sum_{k=0}^{n} D_{n,k}(t)\phi_{m+k}(t). \tag{3}$$

Since

$$\frac{[\log(1 + z)]^k}{k!} = \sum_{n=k}^{\infty} s(n, k)\frac{z^n}{n!},$$

where $s(n, k)$ is the Stirling number of the first kind, we have the explicit formula

$$D_{n,k}(t) = \sum_{j=0}^{n} (-1)^j \binom{n}{j} s(n - j, k)t^j. \tag{4}$$

Since

$$\frac{(e^x - 1)^n}{n!} = \sum_{m=n}^{\infty} S(m, n)\frac{x^m}{m!},$$

we have

$$f(x)\frac{(e^x - 1)^n}{n!} = \sum_{m=0}^{\infty} \frac{x^m}{m!}\sum_{j=0}^{m}\binom{m}{j} S(m - j, n)\phi_j(t),$$

hence the right side of (1) is

$$\sum_{m,n=0}^{\infty} \frac{x^m}{m} z^n t^n \sum_{j=0}^{m}\binom{m}{j} S(m - j, n)\phi_j(t). \tag{5}$$

Equating coefficients of $\frac{x^m}{m!}\frac{z^n}{n!}$ in (3) and (5) we have

Proposition 1: For all $m, n \geq 0$,

$$\sum_{k=0}^{n} D_{n,k}(t)\phi_{m+k}(t) = n!t^n \sum_{j=0}^{m}\binom{m}{j} S(m - j, n)\phi_j(t),$$

where

$$D_{n,k}(t) = \sum_{j=0}^{n} (-1)^j \binom{n}{j} s(n - j, k)t^j.$$

Now let $D_{n,k} = D_{n,k}(1)$. Setting $t = 1$ in Proposition 1, we obtain

Proposition 2: For $m, n \geq 0$,

$$\sum_{k=0}^{n} D_{n,k}B_{m+k} = n! \sum_{j=0}^{m}\binom{m}{j} S(m - j, n)B_j, \tag{6}$$

where

$$D_{n,k} = \sum_{j=0}^{n} (-1)^j \binom{n}{j} s(n - j, k).$$

A recurrence for the numbers $D_{n,k}$ is easily obtained. From (2), we have

$$\sum_{n=k}^{\infty} D_{n,k}\frac{z^n}{n!} = e^{-z}\frac{[\log(1 + z)]^k}{k!},$$

hence

$$D(u, z) = \sum_{n \geq k} D_{n,k}u^k\frac{z^n}{n!} = e^{-z}(1 + z)^u. \tag{7}$$

From (7), we obtain

$$\frac{\partial}{\partial z}D(u, z) = -e^{-z}(1 + z)^u + ue^{-z}(1 + z)^{u-1},$$

thus

$$\begin{aligned}(1 + z)\frac{\partial}{\partial z}D(u, z) &= -(1 + z)D(u, z) + uD(u, z)\\ &= (u - 1 - z)D(u, z). \end{aligned} \tag{8}$$

Equating coefficients of $u^k \frac{z^n}{n!}$ in (8), we have

$$D_{n+1,\,k} = D_{n,\,k-1} - (n+1)D_{n,\,k} - nD_{n-1,\,k} \text{ for } n,\ k \geq 0,$$

with $D_{0,\,0} = 1$ and $D_{n,\,k} = 0$ for $k > n$ or $k < 0$. Here are the first few values of $D_{n,\,k}$:

Table 1

$n \backslash k$	0	1	2	3	4	5	6	7
0	1							
1	-1	1						
2	1	-3	1					
3	-1	8	-6	1				
4	1	-24	29	-10	1			
5	-1	89	-145	75	-15	1		
6	1	-415	814	-545	160	-21	1	
7	-1	2372	-5243	4179	-1575	301	-28	1

Thus the first few instances of (6) yield

$$B_{m+2} + B_{m+1} + B_m \equiv 0 \pmod 2$$

$$B_{m+3} + 2B_{m+1} - B_m \equiv 0 \pmod 6$$

$$B_{m+4} - 10B_{m+3} + 5B_{m+2} + B \equiv 0 \pmod{24}.$$

If we set

$$D_n(u) = \sum_{k=0}^{n} D_{n,\,k}u^k,$$

then from (7) we have

$$D_n(u) = \sum_{j=0}^{n} (-1)^{n-j}\binom{n}{j}(u)_j,$$

where $(u)_j = u(u-1)\ldots(u-j+1)$. It can be shown that for prime p, $D_n(u)$ satisfies the congruence $D_{n+p}(u) \equiv (u^p - u - 1)D_n(u) \pmod p$. In particular, $D_p(u) \equiv u^p - u - 1 \pmod p$, and we recover Touchard's congruence [8]

$$B_{n+p} \equiv B_n + B_{n+1} \pmod p.$$

Touchard later [9] found the congruence

$$B_{2p} - 2B_{p+1} - 2B_p + p + 5 \equiv 0 \pmod{p^2},$$

which is a special case of

$$B_{n+2p} - 2B_{n+p+1} - 2B_{n+p} + B_{n+2} + 2B_{n+1} + (p+1)B \equiv 0 \pmod{p^2},$$

but these congruences do not seem to follow from Proposition 2.

We now show that in a certain sense the congruence obtained from Proposition 2 cannot be improved.

Proposition 3: Let $A_0, A_1, A_2, \ldots$ be a sequence of integers and let $a_0, a_1, \ldots, a_n$ be integers such that

$$\sum_{k=0}^{n} a_k A_{m+k} = \begin{cases} 0 & \text{if } 0 \leq m < n \\ N & \text{if } m = n \end{cases}.$$

Let $b_0, b_1, \ldots, b_n$ be integers such that $\sum_{k=0}^{n} b_k A_{m+k}$ is divisible by R for all $m \geq 0$. Then R divides $b_n N$.

Proof: Let

$$S = \sum_{i,j=0}^{n} a_i b_j A_{i+j}.$$

Since

$$S = \sum_{i=0}^{n} a_i \left[\sum_{j=0}^{n} b_j A_{i+j} \right],$$

R divides S. But

$$S = \sum_{j=0}^{n} b_j \left[\sum_{i=0}^{n} a_i A_{j+i} \right] = b_n N.$$

Corollary: If for some integers $b_0, b_1, \ldots, b_{n-1}$, we have

$$B_{m+n} + b_{n-1}B_{m+n-1} + \cdots + b_0 B_m \equiv 0 \pmod{R} \text{ for all } m \geq 0,$$

then R divides $n!$.

Proof: Since $S(n, k) = 0$ if $n < k$ and $S(n, n) = 1$, the right side of (6) is zero for $0 \leq m < n$ and $n!$ for $m = n$. Thus Proposition 3 applies, with $b_n = 1$.

For other Bell number congruences to composite module, see Barsky [1] and Radoux [7].

4. TANGENT NUMBERS

We have

$$\tan(x + y) = \frac{\tan x + \tan y}{1 - \tan x \tan y} = \tan x + \sum_{n=1}^{\infty} \sec^2 x \tan^{n-1} x \tan^n y.$$

Now set $y = \arctan z$. Then

$$\tan(x + \arctan z) = \tan x + \sum_{n=1}^{\infty} z^n \sec^2 x \tan^{n-1} x, \tag{9}$$

and by Taylor's theorem,

$$\tan(x + \arctan z) = \sum_{k=0}^{\infty} \tan^{(k)} x \frac{(\arctan z)^k}{k!}, \tag{10}$$

where $\tan^{(k)} x = \dfrac{d^k}{dx^k} \tan x$.

Now let us define integers $T(n, k)$ and $t(n, k)$ by

$$\frac{\tan^k x}{k!} = \sum_{n=k}^{\infty} T(n, k)\frac{x^n}{n!} \quad \text{and} \quad \frac{(\arctan x)^k}{k!} = \sum_{n=k}^{\infty} t(n, k)\frac{x^n}{n!}.$$

Tables of $T(n, k)$ and $t(n, k)$ can be found in Comtet [3, pp. 259-260]. Note that

$$\frac{d}{dx}\frac{\tan^k x}{k!} = \sec^2 x \frac{\tan^{k-1} x}{(k-1)!},$$

so

$$\sec^2 x \tan^{n-1} x = (n - 1)! \sum_{m=n-1}^{\infty} T(m + 1, n)\frac{x^m}{m!} \text{ for } n \geq 1.$$

Then from (9) and (10), we have

$$\sum_{m,n=0}^{\infty} \frac{x^m}{m!}\frac{z^n}{n!}\sum_{k=0}^{n} t(n, k)T_{m+k} = \tan x + \sum_{m=1}^{\infty} \sum_{n=0}^{\infty} \frac{x^m}{m!} z^n n!(n - 1)!T(m + 1, n).$$

Then by equating coefficients of $\dfrac{x^m}{m!}\dfrac{z^n}{n!}$ we have

Proposition 4: For $m \geq 0$, $n \geq 1$,

$$\sum_{k=0}^{n} t(n,\ k)T_{m+k} = n!(n - 1)!T(m + 1,\ n). \tag{11}$$

From Proposition 4, we obtain the congruence

$$\sum_{k=0}^{n} t(n,\ k)T_{m+k} \equiv 0 \pmod{n!(n-1)!}.$$

The first few instances are

$$\begin{aligned} &T_{m+2} \equiv 0 \pmod{2}\\ &T_{m+3} - 2T_{m+1} \equiv 0 \pmod{12}\\ &T_{m+4} - 8T_{m+2} \equiv 0 \pmod{144}\\ &T_{m+5} - 20T_{m+3} + 24T_{m+1} \equiv 0 \pmod{2880}\\ &T_{m+6} - 40T_{m+4} + 184T_{m+2} \equiv 0 \pmod{86400}. \end{aligned}$$

Note that the right side of (11) is zero for $m < n - 1$ and $n!(n - 1)!$ for $m = n - 1$. Proposition 3 does not apply directly, but if we observe that

$$t(n,\ 0) = 0 \text{ for } n > 0,$$

and write T_n' for T_{n+1}, then (11) becomes

$$\sum_{k=0}^{n-1} t(n,\ k + 1)T_{m+k}' = n!(n - 1)!T(m + 1,\ n),$$

to which Proposition 3 applies: if for some integers $b_1,\ b_2,\ \ldots,\ b_{n-1}$, we have

$$T_{m+n} + b_{n-1}T_{m+n-1} + \cdots + b_1T_{m+1} \equiv 0 \pmod{R} \text{ for all } m \geq 0,$$

then R divides $n!(n - 1)!$.

Proposition 3 does not preclude the possibility that a better congruence may hold with $m \geq M$ replacing $m \geq 0$, for some M. In fact, this is the case, since the tangent numbers are eventually divisible by large powers of 2; more precisely, $x \tan x/2$ is a Hurwitz series with odd coefficients (the Genocchi numbers).

5. OTHER NUMBERS

We give here congruences for other sequences of combinatorial interest, omitting some of the details of their derivation.

The numbers g_n defined by

$$\sum_{n=0}^{\infty} g_n \frac{x^n}{n!} = (2 - e^x)^{-1}$$

count "preferential arrangements" or ordered partitions of a set. They have been studied by Touchard [8], Gross [4], and others.

If we set $G(x) = (2 - e^x)^{-1}$, then

$$G(x + y) = e^{-y}\sum_{n=0}^{\infty} \frac{2^n(1 - e^{-y})^n}{(2 - e^x)^{n+1}}. \tag{12}$$

Substituting $y = -\log(1 - z)$ in (12), we have

$$G[x - \log(1 - z)] = (1 - z)\sum_{n=0}^{\infty} \frac{2^n z^n}{(2 - e^x)^{n+1}}. \tag{13}$$

Proceeding as before, we obtain from (13) the congruence

$$\sum_{k=0}^{n} c(n,\ k)g_{m+k} \equiv 0 \pmod{2^{n-1}n!},\ m \geq 0, \tag{14}$$

where $c(n,\ k) = |s(n,\ k)|$ is the unsigned Stirling number of the first kind,

$$\sum_{n=0}^{\infty} c(n,\ k)\frac{z^n}{n!} = \frac{[-\log(1-z)]^k}{k!}.$$

The first few instances of (14) are

$$g_{m+2} + g_{m+1} \equiv 0 \pmod 4$$

$$g_{m+3} + 3g_{m+2} + 2g_{m+1} \equiv 0 \pmod{24}$$

$$g_{m+4} + 6g_{m+3} + 11g_{m+2} + 6g_{m+1} \equiv 0 \pmod{192}.$$

The *derangement numbers* $d(n)$ may be defined by

$$\sum_{n=0}^{\infty} d(n)\frac{x^n}{n!} = \frac{e^{-x}}{1-x}.$$

It will be convenient to consider the more general numbers $d(n,\ s)$ defined by

$$D_s(x) = \sum_{n=0}^{\infty} d(n,\ s)\frac{x^n}{n!} = \frac{e^{-x}}{(1-x)^s}.$$

Then

$$D_s(x+y) = \frac{e^{-x}}{(1-x)^s}\,\frac{e^{-y}}{[1-y/(1-x)]^s} = e^{-y}\sum_{n=0}^{\infty} y^n\binom{n+s-1}{n}\frac{e^{-x}}{(1-x)^{n+s}}. \tag{15}$$

Multiplying both sides of (15) by e^y and equating coefficients, we obtain

$$\sum_{k=0}^{n}\binom{n}{k} d(m+k,\ s) = n!\binom{n+s-1}{n} d(m,\ n+s). \tag{16}$$

In particular, we find from (16) that for prime p,

$$d(m+p,\ s) + d(m,\ s) \equiv 0 \pmod p.$$

The numbers t defined by

$$T(x) = \sum_{n=0}^{\infty} t_n\frac{x^n}{n!} = e^{x+\frac{x^2}{2}}$$

have been studied by Chowla, Herstein, and Moore [2], Moser and Wyman [6], and others, and count partitions of a set into blocks of size one and two. We have $T(x+y) = T(x)T(y)e^{x+y}$; hence

$$T(y)^{-1}T(x+y) = T(x)e^{x+y}. \tag{17}$$

Let

$$W(y) = \sum_{n=0}^{\infty} w_n\frac{y^n}{n!} = T(y)^{-1} = e^{-y-\frac{y^2}{2}}.$$

Then from (17) we obtain

$$\sum_{k=0}^{n}\binom{n}{k} w_{n-k}t_{m+k} = n!\binom{m}{n} t_{m-n}, \tag{18}$$

where we take $t_n = 0$ for $n < 0$. We note that (18) satisfies the hypothesis of Proposition 3, so we obtain here a best possible congruence.

The numbers w_n have been studied by Moser and Wyman [6]. From the differential equation $W'(y) = -(1 + y)W(y)$, we obtain the recurrence

$$w_{n+1} = -(w_n + nw_{n-1}),$$

from which the w_n are easily computed. The first few instances of (18) are

$$t_{m+1} - t_m = mt_{m-1}$$

$$t_{m+2} - 2t_{m+1} = 2\binom{m}{2}t_{m-2}$$

$$t_{m+3} - 3t_{m+2} + 2t_m = 6\binom{m}{3}t_{m-3}$$

$$t_{m+4} - 4t_{m+3} + 8t_{m+1} - 2t_m = 24\binom{m}{4}t_{m-4}.$$

A natural question is: To what series does this method apply? In other words, we want to characterize those Hurwitz series $f(x)$ for which there exist Hurwitz series $h(z)$ and $g(z)$, with $h(0) = 1$, $g(0) = 0$, and $g'(0) = 1$, such that for all $m, n \geq 0$, the coefficient of $(x^m/m!)z^n$ in $h(z)f[x + g(z)]$ is integral.

REFERENCES

1. Daniel Barsky. "Analyse p-adique et nombres de Bell." *C. R. Acad. Sci. Paris* (A) 282 (1976):1257-1259.
2. S. Chowla, I. N. Herstein, & W. K. Moore. "On Recursions Connected with Symmetric Groups I." *Canad. J. Math.* 3 (1951):328-334.
3. L. Comtet. *Advanced Combinatorics.* Boston: Reidel, 1974.
4. O. A. Gross. "Preferential Arrangements." *Amer. Math. Monthly* 69 (1962): 4-8.
5. A. Hurwitz. "Ueber die Entwickelungscoefficienten der lemniscatischen Functionen." *Math. Annalen* 51 (1899):196-226.
6. Leo Moser & Max Wyman. "On Solutions of $x^d = 1$ in Symmetric Groups." *Canad. J. Math.* 7 (1955):159-168.
7. Chr. Radoux. "Arithmétique des nombres de Bell et analyse p-adique." *Bull. Soc. Math. de Belgique* (B) 29 (1977):13-28.
8. Jacques Touchard. "Propriétés arithmétique de certaines nombres recurrents." *Ann. Soc. Sci. Bruxelles* (A) 53 (1933):21-31.
9. Jacques Touchard. "Nombres exponentiels et nombres de Bernoulli." *Canad. J. Math.* 8 (1956):305-320.

*****

A QUADRATIC PROPERTY OF CERTAIN LINEARLY RECURRENT SEQUENCES

JULIO R. BASTIDA and M. J. DeLEON
Florida Atlantic University, Boca Raton, FL 33431

In [1] one of the authors proved the following result.

Let u be a real number such that $u > 1$, and let $\{x_n\}_{n \geq 0}$ be a sequence of nonnegative real numbers such that

$$x_{n+1} = ux_n + \sqrt{(u^2 - 1)(x_n^2 - x_0^2) + (x_1 - ux_0)^2}$$

for every $n \geq 0$. Then

$$x_{n+2} = 2ux_{n+1} - x_n$$

for every $n \geq 0$; and, in particular, if u, x_0, x_1 are integers, then x_n is an integer for every $n \geq 0$.