Pacific Journal of Mathematics

SOME CONGRUENCES FOR THE BELL POLYNOMIALS

L. Carlitz

Vol. 11, No. 4 1961

SOME CONGRUENCES FOR THE BELL POLYNOMIMALS

L. CARLITZ

1. Let $\alpha_1, \alpha_2, \alpha_3, \cdots$ denote indeterminates. The Bell polynomial $\phi_n(\alpha_1, \alpha_2, \alpha_3, \cdots)$ may be defined by $\phi_0 = 1$ and

$$(1.1) \qquad \phi_n = \phi_n(\alpha_1, \alpha_2, \alpha_3, \cdots) = \sum \frac{n!}{k_1!(1!)^{k_1}k_2!(2!)^{k_2}\cdots}\alpha_1^{k_1}\alpha_2^{k_2}\cdots ,$$

where the summation is over all nonnegative integers k_j such that

$$k_1 + 2k_2 + 3k_3 + \cdots = n .$$

For references see Bell [2] and Riordan [5, p. 36]. The general coefficient

$$(1.2) \qquad A_n(k_1, k_2, k_3, \cdots) = \frac{n!}{k_1!(1!)^{k_1}k_2!(2!)^{k_2}\cdots}$$

is integral; this is evident from the representation

$$A_n(k_1, k_2, k_3, \cdots) = \frac{n!}{k_1!(2k_2)!(3k_3)!\cdots} \cdot \frac{(2k_2)!}{k_2!(2!)^{k_2}} \frac{(3k_3)!}{k_3!(3!)^{k_3}} \cdots$$

and the fact that the quotient

$$\frac{(rk)!}{k!(r!)^k}$$

is integral [1, p. 57].

The coefficient $A_n(k_1, k_2, k_3, \cdots)$ resembles the multinomial coefficient

$$M(k_1, k_2, k_3 \cdots) = \frac{(k_1 + k_2 + k_3 + \cdots)!}{k_1!k_2!k_3 \cdots} .$$

If p is a fixed prime it is known [3] that $M(k_1, k_2, k_3, \cdots)$ is prime to p if and only if

$$k_i = \sum_j a_{ij}p^j \qquad (0 \leqq a_{ij} < p) ,$$

$$k_1 + k_2 + k_3 + \cdots = \sum_j a_j p^j \qquad (0 \leqq a_j < p)$$

and

$$\sum_i a_{ij} = a_j \qquad (j = 0, 1, 2, \cdots) .$$

It does not seem easy to find an analogous result for $A_n(k_1, k_2, k_3, \cdots)$. For some special results see § 3 below.

Received October 31, 1960

Bell [2] showed that

$$\phi_p \equiv \alpha_1^p + \alpha_p \pmod{p} \tag{1.3}$$

and also determined the residues (mod p) of $\phi_{p+1}, \phi_{p+2}, \phi_{p+3}$. He also obtained an expression for the residue of ϕ_{p+r} as a determinant of order $r+1$. Generalizing (1.3) we shall show first that

$$\phi_{p^r} \equiv \alpha_1^{p^r} + \alpha_p^{p^{r-1}} + \cdots + \alpha_{p^r} \pmod{p} \tag{1.4}$$

and that

$$\phi_{pn}(\alpha_1, \alpha_2, \alpha_3, \cdots) \equiv \phi_n(\phi_p, \alpha_{2p}, \alpha_{3p}, \cdots) \pmod{p} \tag{1.5}$$

for all $n \geqq 1$. Note that on the right the first argument in ϕ_n is ϕ_p and not α_p.

2. From (1.1) we get the generating function

$$\sum_{n=0}^{\infty} \phi_n \frac{t^n}{n!} = \exp\left(\alpha_1 t + \alpha_2 \frac{t^2}{2!} + \alpha_3 \frac{t^3}{3!} + \cdots\right). \tag{2.1}$$

Indeed this may be taken as the definition of ϕ_n. Differentiating with respect to t we get

$$\sum_{n=0}^{\infty} \phi_{n+1} \frac{t^n}{n!} = \sum_{n=0}^{\infty} \phi_n \frac{t^n}{n!} \sum_{r=0}^{\infty} \alpha_{r+1} \frac{t^r}{r!} ,$$

so that

$$\phi_{n+1} = \sum_{r=0}^{n} \binom{n}{r} \phi_{n-r} \alpha_{r+1} . \tag{2.2}$$

Since the binomial coefficient

$$\binom{pn}{r} \equiv 0 \pmod{p}$$

unless $p|r$ and

$$\binom{pn}{pr} \equiv \binom{n}{r} \pmod{p}$$

it follows from (2.2) that

$$\phi_{pn+1} \equiv \sum_{r=0}^{n} \binom{n}{r} \phi_{p(n-r)} \alpha_{pr+1} \pmod{p} . \tag{2.3}$$

If for brevity we put

$$A(t) = \sum_{r=1}^{\infty} \alpha_r t^r / r! ,$$

so that

$$\sum_{n=0}^{\infty} \phi_n \frac{t^n}{n!} = \exp A(t) ,$$

it is easily seen by repeated differentiation and by (1.3) that

$$\sum_{n=0}^{\infty} \phi_{n+p} \frac{t^n}{n!} \equiv \{(A'(t))^p + A^{(p)}(t)\}e^{A(t)} \pmod{p} . \tag{2.4}$$

(By the statement

$$\sum_{n=0}^{\infty} A_n \frac{t^n}{n!} \equiv \sum_{n=0}^{\infty} B_n \frac{t^n}{n!} \pmod{m} ,$$

where A_n, B_n are polynomials with integral coefficients, is meant the system of congruences

$$A_n \equiv B_n \pmod{m} \qquad (n = 0, 1, 2, \cdots)) .$$

Hurwitz [4, p. 345] has proved the lemma that if $a_1, a_2, a_3, \cdots$ are arbitrary integers then

$$\left(\sum_{n=1}^{\infty} a_n \frac{x^n}{n!}\right)^k \equiv 0 \pmod{k!} .$$

The proof holds without change when the a_n are indeterminates. Since

$$A'(t) = \sum_{n=0}^{\infty} \alpha_{n+1} \frac{t^n}{n!} ,$$

it follows easily from Hurwitz's lemma that

$$(A'(t)^p = \left(\alpha_1 + \sum_{n=1}^{\infty} \alpha_{n+1} \frac{t^n}{n!}\right)^p \equiv \alpha_1^p \pmod{p} .$$

Thus (2.4) becomes

$$\sum_{n=0}^{\infty} \phi_{n+p} \frac{t^n}{n!} \equiv \left(\alpha_1^p + \sum_{r=0}^{\infty} \alpha_{r+p} \frac{t^r}{r!}\right) \sum_{n=0}^{\infty} \phi_n \frac{t^n}{n!} ,$$

which yields

$$\phi_{n+p} \equiv (\alpha_1^p + \alpha_p)\phi_n + \sum_{r=1}^{n} \binom{n}{r} \alpha_{r+p} \phi_{n-r} \pmod{p} . \tag{2.5}$$

In particular, for $n = 0$, (2.5) reduces to Bell's congruence (1.3). Similarly

$$\phi_{p+1} \equiv (\alpha_1^p + \alpha_p)\alpha_1 + \alpha_{p+1} \equiv \phi_p \alpha_1 + \alpha_{p+1} ,$$
$$\phi_{p+2} \equiv \phi_p \phi_2 + 2\alpha_{p+1}\alpha_1 + \alpha_{p+2} ,$$

and so on.

We remark that (2.5) is equivalent to Bell's congruence involving a determinant [2, p. 267, formula (6.5)]. Also for $s = \alpha_1 = \alpha_2 = \cdots$, (2.5) reduces to

$$
\begin{aligned}
(2.5)' \qquad a_{n+p}(s) &\equiv (s^p + s)a_n(s) + s\sum_{r=1}^{n}\binom{n}{r}a_{n-r}(s) \\
&\equiv a_{n+1}(s) + s^p a_n(s) \qquad (\text{mod } p)\,,
\end{aligned}
$$

where [5, p. 76]

$$
a_n(s) = \phi_n(s, s, \cdots) = \sum_k S(n, k)s^k
$$

and $S(n, k)$ denotes the Stirling number of the second kind. The congruence (2.5)′ is due to Touchard [6].

If in (2.5) we replace n by pn we get

$$
(2.6) \qquad \phi_{p(n+1)} \equiv \phi_p\phi_{np} + \sum_{r=1}^{n}\binom{n}{r}\alpha_{p(r+1)}\phi_{p(n-r)} \qquad (\text{mod } p)
$$

for all $n = 0, 1, 2, \cdots$. Thus ϕ_{pn} is congruent to a polynomial in ϕ_p, $\alpha_{2p}, \alpha_{3p}, \cdots$ alone. Moreover, comparing (2.6) with (2.2), it is clear that

$$
(2.7) \qquad \phi_{pn} \equiv \phi_n(\phi_p, \alpha_{2p}, \alpha_{3p}, \cdots) \qquad (\text{mod } p)\,,
$$

so that we have proved (1.5).

Replacing n by pn in (2.7) we get

$$
\phi_{p^2n} \equiv \phi_{pn}(\phi_p, \alpha_{2p}, \alpha_{3p}, \cdots) \equiv \phi_n(\phi_p^p + \alpha_{p^2}, \alpha_{2p^2}, \alpha_{3p^2}, \cdots)\,.
$$

In particular for $n = 1$

$$
\phi_{p^2} \equiv \phi_p^p + \alpha_{p^2} \equiv \alpha_1^{p^2} + \alpha_p^p + \alpha_{p^2}\,.
$$

Again replacing n by pn we get

$$
\phi_{p^3n} \equiv \phi_n(\phi_{p^2}^p + \alpha_{p^3}, \alpha_{2p^3}, \alpha_{3p^3}, \cdots)\,,
$$

so that in particular

$$
\phi_{p^3} \equiv \phi_{p^2}^p + \phi_{p^3} \equiv \alpha_1^{p^3} + \alpha_p^{p^2} + \alpha_{p^2}^p + \alpha_{p^3}\,.
$$

Continuing in this way we see that

$$
(2.8) \qquad \phi_{p^rn} \equiv \phi_n(\phi_{p^r}, \alpha_{2p^r}, \alpha_{3p^r}, \cdots) \qquad (\text{mod } p)
$$

and

$$
(2.9) \qquad \phi_{p^r} \equiv \phi_{p^{r-1}}^p + \alpha_{p^r} \equiv \alpha_1^{p^r} + \alpha_p^{p^{r-1}} + \cdots + \alpha_{p^r} \qquad (\text{mod } p)\,.
$$

We have therefore proved (1.4) as well as the more general congruence (2.8).

Since

$$\phi_2 = \alpha_1^2 + \alpha_2 ,$$
$$\phi_3 = \alpha_1^3 + 3\alpha_1\alpha_2 + \alpha_3 ,$$
$$\phi_4 = \alpha_1^4 + 6\alpha_1^2\alpha_2 + 4\alpha_1\alpha_3 + 3\alpha_2^2 + \alpha_4 ,$$

it follows from (2.8) that

$$\begin{cases} \phi_{2p^r} \equiv \phi_{p^r}^2 + \alpha_{2p^r} , \\ \phi_{3p^r} \equiv \phi_{p^r}^3 + 3\phi_{p^r}\alpha_{2p^r} + \alpha_{3p^r} , \\ \phi_{4p^r} \equiv \phi_{p^r}^4 + 6\phi_{p^r}^2\alpha_{2p^r} + 4\phi_{p^r}\alpha_{3p^r} + 3\alpha_{2p^r}^2 + \alpha_{4p^r} , \end{cases} \tag{2.10}$$

and so on.

We note also that (2.3) implies

$$\begin{cases} \phi_{p^r+1} \equiv \phi_{p^r}\alpha_1 + \alpha_{p^r+1} , \\ \phi_{2p^r+1} \equiv \phi_{2p^r}\alpha_1 + 2\phi_{p^r}\alpha_{p^r+1} + \alpha_{2p^r+1} , \\ \phi_{3p^r+1} \equiv \phi_{3p^r}\alpha_1 + 3\phi_{2p^r}\alpha_{p^r+1} + 3\phi_{p^r}\alpha_{2p^r+1} + \alpha_{3p^r+1} . \end{cases} \tag{2.11}$$

3. By means of (1.5) we can obtain certain congruences for the coefficient $A(k_1, k_2, k_3, \cdots)$. Indeed by (1.1) and (1.3)

$$\begin{aligned} &\phi_n(\phi_p, \alpha_{2p}, \alpha_{3p}, \cdots) \\ &\equiv \sum A_n(k_1, k_2, k_3, \cdots)(\alpha_1^p + \alpha_p)^{k_1}\alpha_{2p}^{k_2}\alpha_{3p}^{k_3} \cdots \pmod{p} , \end{aligned} \tag{3.1}$$

where the summation is over nonnegative k_j such that

$$k_1 + 2k_2 + 3k_3 + \cdots = n .$$

The right member of (3.1) is equal to

$$\sum_{(k_j)} A_n(k_1, k_2, k_3, \cdots) \sum_{r=0}^{k_1} \binom{k_1}{r} \alpha_1^{p(k_1-r)}\alpha_p^r\alpha_{2p}^{k_2}\alpha_{3p}^{k_3} \cdots . \tag{3.2}$$

On the other hand

$$\phi_{pn} = \sum A_{pn}(h_1, h_2, h_3, \cdots)\alpha_1^{h_1}\alpha_2^{h_2}\alpha_3^{h_3} \cdots , \tag{3.3}$$

summed over

$$h_1 + 2h_2 + 3h_3 + \cdots = p_n . \tag{3.4}$$

It follows from (1.5) that

$$A_{pn}(h_1, h_2, h_3, \cdots) \equiv 0 \pmod{p}$$

except possibly when

$$h_j = 0 \qquad (j > 1,\ p \nmid j) . \tag{3.5}$$

When this condition is satisfied (3.4) becomes

$$h_1 + p(h_p + 2h_{2p} + \cdots) = pn\ ;$$

consequently $h_1 = pk_1$ and (3.3) becomes

$$\phi_{pn} \equiv \sum A_{pn}(pk_1, 0, \cdots, 0, h_p, \cdots)\alpha_1^{pk_1}\alpha_h^{h_p}\alpha_{2p}^{h_{2p}} \cdots .$$

We have therefore proved the following result:

THEOREM 1. *The coefficient $A_{pn}(h_1, h_2, h_3, \cdots)$ occurring in* (3.3) *is certainly divisible by p unless* (3.5) *is satisfied and $h_1 = pk_1$. If these conditions are satisfied then*

$$A_{pn}(h_1, h_2, h_3, \cdots) \equiv \binom{k_1}{h_p} A_n(k_1 - h_p, h_p, h_{2p}, \cdots) \pmod{p} .$$

If we make use of (1.4) we obtain the following simpler

THEOREM 2. *Let*

$$h_1 + 2h_2 + 3h_3 + \cdots = p^r .$$

Then the coefficient $A_{p^r}(h_1, h_2, h_3, \cdots)$ is divisible by p except when

$$h_i = 0 \qquad (i \neq j) , \qquad h_j = p^s ,$$

for some j, in which case

$$A_{p^r}(h_1, h_2, h_3, \cdots) \equiv 1 \pmod{p} .$$

Using (2.10) and (2.11) we can obtain additional results. For example take

$$h_1 + 2h_2 + 3h_3 + \cdots = 2p^r .$$

Then $A_{2p^r}(h_1, h_2, h_3, \cdots)$ is divisible by p unless (i) all $h_s = 0$ $(s \neq j)$, $h_j = 1$ or 2; (ii) all $h_s = 0$ $(s \neq i, j)$, $h_i = h_j = 1$. In case (i) $A \equiv 1$, in case (ii) $A \equiv 2 \pmod{p}$.

For $n = 3p^r$ the corresponding results are more complicated.

4. We turn now to the polynomial $C_n(\alpha_1, \alpha_2, \alpha_3, \cdots)$, the cycle indicator of the symmetric group [5, p. 68]:

$$\begin{aligned} C_n &= C_n(\alpha_1, \alpha_2, \alpha_3, \cdots) = \phi_n(\alpha_1, \alpha_2, 2!\alpha_3, \cdots) \\ &= \sum \frac{n!}{k_1!k_2!k_3 \cdots} \left(\frac{\alpha_1}{1}\right)^{k_1}\left(\frac{\alpha_2}{2}\right)^{k_2}\left(\frac{\alpha_3}{3}\right)^{k_3} \cdots , \end{aligned} \tag{4.1}$$

where the summation is over all nonnegative k_j such that

$$k_1 + 2k_2 + 3k_3 + \cdots = n .$$

It is convenient to define $C_0 = 1$.

Put

$$(4.2)\qquad c_n(k_1, k_2, k_3, \cdots) = \frac{n!}{k_1!k_2!k_3 \cdots 1^{k_1}2^{k_2}3^{k_3}\cdots},$$

the general coefficient of C_n. Clearly $c_n(k_1, k_2, k_3, \cdots)$ is integral and indeed a multiple of $A_n(k_1, k_2, k_3, \cdots)$.

From (4.1) we get the generating function

$$(4.3)\qquad G(t) = \sum_{n=0}^{\infty} G_n \frac{t^n}{n!} = \exp\left(\alpha_1 t + \frac{1}{2}\alpha_2 t^2 + \frac{1}{3}\alpha_3 t^3 + \cdots\right).$$

For brevity put

$$C(t) = \sum_{n=1}^{\infty} \frac{1}{n} \alpha_n t^n .$$

Differentiating (4.3) with respect to t we get

$$G'(t) = C'(t)G(t) ,$$

that is

$$\sum_{n=0}^{\infty} C_{n+1}\frac{t^n}{n!} = \sum_{r=0}^{\infty} \alpha_{r+1}t^r \sum_{n=0}^{\infty} C_n\frac{t^n}{n!} .$$

This implies

$$(4.4)\qquad C_{n+1} = \sum_{r=0}^{n} \frac{n!}{r!}\alpha_{n-r+1}C_r ,$$

so that

$$(4.5)\qquad C_{n+1} \equiv \alpha_1 C_n \pmod{n} .$$

By repeated differentiation of (4.3) we get (compare (2.4))

$$(4.6)\qquad \frac{d^p}{dt^p}G(t) \equiv \{(C'(t))^p + C^{(p)}(t)\}G(t) \pmod{p} .$$

Now since

$$C'(t) = \sum_{n=0}^{\infty} \alpha_{n+1}t^n , \quad C^{(p)}(t) = \sum_{n=0}^{\infty} (n + p - 1)!\alpha_{n+1}\frac{t^n}{n!} ,$$

it is clear that

$$(C'(t))^p \equiv \alpha_1^p, \quad C^{(p)}(t) \equiv - \alpha_p \pmod{p} ;$$

at the last step we have used Wilson's theorem. Thus (4.6) becomes

$$\sum_{n=0}^{\infty} C_{n+p}\frac{t^n}{n!} \equiv (\alpha_1^p - \alpha_p)\sum_{n=0}^{\infty} C_n\frac{t^n}{n!} ,$$

so that

$$C_{n+p} \equiv (\alpha_1^p - \alpha_p)C_n \pmod p . \tag{4.7}$$

In particular we have

$$C_p \equiv \alpha_1^p - \alpha_p \pmod p \tag{4.8}$$

and

$$C_{n+rp} \equiv (\alpha_1^p - \alpha_p)^r C_n \pmod p \tag{4.9}$$

We remark that for $p = 3, 5, 7$, (4.8) is in agreement with the explicit values of C_n given in [5, p. 69].

By (4.9) with $n = 0$ we find that the coefficient

$$c_{rp}(k_1, k_2, k_3, \cdots) \equiv 0 \pmod p$$

unless all k_j except k_1 and k_p vanish and k_1 is a multiple of p; in this case we have

$$c_{rp}(pk, 0, \cdots, 0, k_p, \cdots) \equiv (-1)^{k_p}\binom{r}{k} \pmod p . \tag{4.10}$$

References

1. P. Bachmann, *Niedere Zahlentheorie*, vol. 1, Leipzig, 1902.
2. E. T. Bell, *Exponential polynomials*, Annals of Math., **35** (1934), 258-277.
3. L. E. Dickson, *Theorems on the residues of multinomial coefficients with respect to a prime modulus*, Quarterly J. Math., **33** (1902), 378-384.
4. A. Hurwitz, *Über die Entwickelungscoeffizienten der lemniscatischen Functionen*, Mathematische Werke, Basel, **2**, (1933), 342-373.
5. J. Riordan, *An Introduction to combinatorial analysis*, New York, 1958.
6. J. Touchard, *Propriétés arithmétiques de certains nombres recurrents*, Ann. Soc. Sci. Bruxelles, **A53** (1933), 21-31.

DUKE UNIVERSITY

PACIFIC JOURNAL OF MATHEMATICS

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, L. J. Paige at the University of California, Los Angeles 24, California.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. The price per volume (4 numbers) is $12.00; single issues, $3.50. Back numbers are available. Special price to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues, $1.25.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley 8, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 6, 2-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Reprinted 1966 in the United States of America

Pacific Journal of Mathematics
Vol. 11, No. 4 , 1961