JOURNAL OF COMBINATORIAL THEORY, Series A 40, 161–168 (1985)

Note

Maximum Zero Strings of Bell Numbers Modulo Primes

J. W. LAYMAN

Department of Mathematics,
Virginia Polytechnic Institute and State University,
Blacksburg, Virginia 24061

Communicated by the Managing Editors

Received September 13, 1983

For any prime p, the sequence of Bell exponential numbers B_n is shown to have $p-1$ consecutive values congruent to zero (mod p), beginning with B_m, where $m \equiv 1 - (p^p-1)/(p-1)^2 \pmod{(p^p-1)/(p-1)}$. This is an improvement over previous results on the maximal strings of zero residues of the Bell numbers. Similar results are obtained for the sequence of generalized Bell numbers A_n generated by $e^{-(e^x-1)} = \sum_{n=0}^{\infty} A_n x^n/n!$.

1. INTRODUCTION AND HISTORICAL BACKGROUND

We consider the linear congruence

$$a_{n+p}(s) \equiv a_{n+1}(s) + s a_n(s) \pmod{p}, \tag{1.1}$$

where p is a prime and s is an integer. The congruence is satisfied by the numbers $a_n(s)$ generated by

$$e^{s(e^x-1)} = \sum_{n=0}^{\infty} a_n(s) \frac{x^n}{n!}. \tag{1.2}$$

When $s=1$, the numbers $B_n = a_n(1)$ are the Bell exponential numbers studied by Bell [2, 3] and many others. For integer values of s ($s \neq 1$) we will refer to the numbers $a_n(s)$ as generalized Bell numers. The congruence properties of the Bell numbers and generalized Bell numbers have been investigated by several authors [4, 8, 11, 12].

One aspect of these investigations has been the determination of the congruence periods l such that

$$a_{n+l}(s) \equiv a_n(s) \pmod{p}. \tag{1.3}$$

0097-3165/85 $3.00

Hall [6] showed that the Bell numbers have the periodicity

$$B_{n+N_p} \equiv B_n \pmod{p}, \tag{1.4}$$

where

$$N_p = \frac{p^p - 1}{p - 1}, \tag{1.5}$$

a result rediscovered by Williams [12]. Chinthayama and Gandhi [4] showed that a period for $a_n(s)$ is given by

$$l = (N_p)\,\mathrm{ord}_p(s). \tag{1.6}$$

Since the minimality of these periods was not established, Levine and Dalton [8] searched for periods of the Bell numbers among the divisors of N_p and found that for $p \leqslant 17$ the minimum period is exactly N_p and that for $p \leqslant 47$ no known proper divisior N of N_p, with $N \leqslant 10^{40}$, can be a period.

The rather extreme length of the periods makes the congruence (1.1) of interest as a possible pseudorandom number generator. Zierler [13] has investigated the autocorrelation functions of the residues in an m-sequence, that is, a sequence with the maximum possible minimum period $p^p - 1$. Since the Bell numbers have a period which divides $N_p = (p^p - 1)/(p - 1)$, they clearly do not constitute an m-sequence. However, if s is a primitive root of p, so that the order of $s \pmod{p}$ is $p - 1$, then by (1.6) the only known period is $l = p^p - 1$ and thus an m-sequence solution of (1.1) is an open possibility in this case.

Of interest in connection with the problem of the minimal periods of the generalized Bell numbers (modulo p) is the problem of the determination and location of maximal strings of zero residues. In Section 3, we give a new approach to this problem and obtain stronger results than known previously.

For combinatorial interpretations of the B_n, see [7]. A large bibliography is given in Rota [10].

In addition to the special case $s = 1$, which yields the Bell numbers, the case $s = -1$ holds considerable interest. The author, with Prather, has shown [7] a connection between the $a_n(-1)$ and several problems in complex function theory. Results on the maximal strings of zeros of the $a_n(-1) \pmod{p}$ are obtained in Section 4.

2. Preliminaries

We will need certain additional properties of the generalized Bell numbers and their congruences. Comtet [5] gives

$$sa_n(s) = [\Delta^n a_k(s)]_{k=1}, \tag{2.1}$$

where Δ^n is the nth difference taken with respect to k. It follows easily from (2.1) and (1.1) that

$$a_{n+1}(s) = s \sum_{k=0}^{n} \binom{n}{k} a_k(s), \qquad a_0(s) = 1, \tag{2.2}$$

and

$$a_{n+kp}(s) \equiv \sum_{i=0}^{k} \binom{k}{i} s^i a_{n+k-i}(s) \pmod{p}. \tag{2.4}$$

In the next section we make use of the following result.

Lemma 1. $B_{n+1} \equiv B_{pn} \pmod{p}$, *for* $n = 0, 1, 2, \ldots$, *where* p *is any prime.*

Proof. From (2.4), with $s = 1$, we have

$$B_{pn} \equiv \sum_{i=0}^{n} \binom{n}{i} B_i,$$

and the desired conclusion follows from (2.2).

3. Maximal Strings of Consecutive Zeros

The maximum possible number of consecutive zeros of $a_n(s) \pmod{p}$ is obviously $p-1$ since, for any greater number, the recurrence (1.1) would generate the trivial sequence consisting entirely of zero residues. It is not immediately clear, however, that such a maximal string of $p-1$ zeros actually occurs for each p. Proof of the existence of such maximal strings for B_n and, in addition, the determination of their precise location in the sequence, is therefore of interest. Radoux [9] has shown that, for those p for which the minimal period is N_p, one period of the sequence $B_n \pmod{p}$ contains exactly one string of $p-1$ consecutive zeros. He also obtains the location of such a string. In this section we show by an entirely different method that this result holds without the hypothesis that N_p is the minimal period.

THEOREM 1. *Let M be an integer and p a prime. Then a necessary and sufficient condition that $B_{M+k} \equiv 0 \pmod{p}$ for $k = 0, 1, \ldots, p-2$, is that $B_{M+k} \equiv B_{M+pk} \pmod{p}$ for $k = 1, 2, \ldots, p-1$.*

Proof. By (2.4) we have

$$B_{M+kp} \equiv \sum_{i=0}^{k} \binom{k}{i} B_{M+i} \pmod{p} \qquad \text{for } k = 0, 1, 2, \ldots. \tag{3.1}$$

Therefore, if $B_{M+k} \equiv 0$ for $k = 0, 1, \ldots, p-2$, we clearly have $B_{M+pk} \equiv 0$ and hence, trivially, $B_{M+k} \equiv B_{M+pk}$. When $k = p-1$ and $B_{M+k} \equiv 0$ for $k = 0, 1, \ldots, p-2$, (3.1) reduces to $B_{M+p-1} \equiv B_{M+(p-1)p}$.

Conversely, if $B_{M+k} \equiv B_{M+pk} \pmod{p}$ for $k = 1, 2, \ldots, p-1$, (3.1) is equivalent to

$$B_{M+k} \equiv B_{M+k} + \sum_{i=0}^{k-1} \binom{k}{i} B_{M+i} \pmod{p} \qquad \text{for } k = 1, 2, \ldots, p-1,$$

which reduces to

$$0 \equiv \sum_{i=0}^{k-1} \binom{k}{i} B_{M+i} \pmod{p} \qquad \text{for } k = 1, 2, \ldots, p-1. \tag{3.2}$$

The system (3.2) is triangular with diagonal coefficients $\binom{k}{1}$. The coefficient matrix is therefore nonsingular with determinant $(p-1)! \equiv -1 \pmod{p}$, by Wilson's theorem. Thus the only solution is given by

$$B_{M+i} \equiv 0 \pmod{p}, \qquad i = 0, 1, \ldots, p-2.$$

THEOREM 2. *For each prime p the sequence B_n contains $p-1$ consecutive zeros*

$$B_{m_p+k} \equiv 0 \pmod{p}, \qquad k = 0, 1, \ldots, p-2, \tag{3.3}$$

where

$$m_p \equiv 1 - \frac{p^p - p}{(p-1)^2} \pmod{N_p}. \tag{3.4}$$

Proof. In Lemma 1, let $n = M + k$ for $k = 0, 1, 2, \ldots$, where M is an integer to be determined, to obtain

$$B_{M+k+1} \equiv B_{pM+pk} \pmod{p}, \qquad k = 0, 1, \ldots. \tag{3.5}$$

By (1.4), (1.5), and Theorem 1, it follows that $p-1$ consecutive zeros of $B_n \pmod{p}$ will occur, beginning with B_{M+1}, if

$$M + 1 \equiv pM \pmod{N_p}, \tag{3.6}$$

or, in other words, if

$$M+1=pM+rN_p$$

for some integer r. Using $N_p=(p^p-1)/(p-1)$, straightforward calculation leads to

$$M=-r\frac{p^p-p}{(p-1)^2}-\frac{r-1}{p-1}.$$

Now it can be easily verified that $(p^p-p)/(p-1)^2$ is always an integer; in fact, for $p\geqslant 3$,

$$\frac{p^p-p}{(p-1)^2}=p+\sum_{k=0}^{p-3}(k+1)\,p^{p-k-2}.$$

Since M must be an integer we must have $r=1+t(p-1)$ for some integer t, from which it follows that

$$M=-\frac{p^p-p}{(p-1)^2}-tN_p.$$

Since the $p-1$ consecutive zeros begin with B_{M+1}, the proof is complete.

4. The numbers $a_n(-1)$

For convenience in this section we write $A_n=a_n(-1)$. The A_n are generated by (1.2) with $s=-1$:

$$e^{-(e^x-1)}=\sum_{n=0}^{\infty}A_n\frac{x^n}{n!}. \tag{4.1}$$

The combinatorial and congruence properties given in Sections 1 and 2 may be written as follows for the A_n

$$A_{n+p}\equiv A_{n+1}-A_n \pmod p, \tag{4.2}$$

$$A_{n+N_p}\equiv -A_n \pmod p \qquad \text{where } N_p=\frac{p^p-1}{p-1}, \tag{4.3}$$

$$A_n=\sum_{k=0}^{n}\binom{n}{k}A_k,\ A_0=1, \tag{4.4}$$

$$A_n=-\Delta^n A_1. \tag{4.5}$$

The location of maximal runs of consecutive zeros of $A_n \pmod p$ and the minimal period can be established in a manner similar to that used above for the B_n.

THEOREM 3. *For any prime p, there occur* $p-1$ *consecutive zeros of* $A_n \pmod p$, *beginning at* $n = n_p$, *where*

$$n_p \equiv \frac{p^p - p}{(p-1)^2} \pmod{N_p}.$$

Proof. By (4.5) and (4.2) we have

$$A_n \equiv -(E^p)^n A_1 \equiv -A_{np+1} \pmod p,$$

where E is the shift operator defined by $EA_k = A_{k+1}$. Let $n = M + k$ to obtain

$$\begin{aligned} A_{M+k} &\equiv -A_{Mp+pk+1} \\ &\equiv A_{N_p+Mp+pk+1} \qquad \text{by (4.3).} \end{aligned}$$

A straightforward modification of Theorem 1 for the case $s = -1$ provides that $p-1$ consecutive zeros of $A_n \pmod p$ will occur, beginning with A_M, if

$$M \equiv N_p + pM + 1 \pmod{N_p}.$$

Proceeding as in the proof of Theorem 1, we find that

$$M = -r\frac{p^p - p}{(p-1)^2} - \frac{r+1}{p-1}$$

for some integer r satisfying $r \equiv -1 \pmod{p-1}$. If we write $r = t(p-1) - 1$, calculation shows that

$$M = \frac{p^p - p}{(p-1)^2} - t\frac{p^p - 1}{p-1},$$

which completes the proof.

Theorem 3, together with (4.3), shows that the sequence of the $A_n \pmod p$ contains at least two strings of $p-1$ consecutive zeros. We now investigate whether other such strings are possible. Following Radoux, we obtain the following useful result:

THEOREM 4. *Let p be a prime and let t be an integer such that* $tA_{i+r} \equiv A_{j+r} \pmod p$, *for* $r = 0, 1, \ldots, p-1$. *Then* $t^2 \equiv 1 \pmod p$.

Proof. Suppose that $tA_{i+r_k} \equiv A_{j+r} (\mathrm{mod}\, p)$ for $r = 0, 1, \ldots, p-1$. Then, setting $k = j - 1$, we have, for all n:

$$tA_n \equiv A_{n+k} \,(\mathrm{mod}\, p).$$

It follows that, in general,

$$t^s A_n \equiv A_{n+sk} \,(\mathrm{mod}\, p)$$

and, in particular,

$$A_n \equiv A_{n+(p-1)k} \,(\mathrm{mod}\, p).$$

Therefore the minimal period $\prod_p$ must divide $(p-1)k$ and, by (4.3), $\prod_p | 2(p^p - 1)/(p-1)$. But $(p-1, 2(p^p-1)/(p-1) = 2$. Thus $\prod_p | 2k$ and so, for all n,

$$t^2 A_n \equiv A_n \,(\mathrm{mod}\, p),$$

completing the proof.

The following result is an immediate consequence of Theorems 3 and 4 and (4.3).

THEOREM 5. *The sequence* $A_n \,(\mathrm{mod}\, p)$ *contains in one minimal period exactly two strings of* $p-1$ *consecutive zeros, one string starting exactly one-half period after the other.*

The number A_n can be given a combinatorial interpretation. Let $E(n)$ and $O(n)$ be the numbers of partitions of n elements into an even number of congruence classes and an odd number of congruence classes, respectively. Then, following Rota [10], a tedious but straightforward analysis shows that $A_n = E(n) - O(n)$.

Numerical calculations of the exact values of A_n have been made, by using (4.5), for $0 \leqslant n \leqslant 110$. For $0 \leqslant n \leqslant 15$, the values are

1(0); −1(1); 0(2); 1(3); 1(4); −2(5); −9(6); −9(7);
50(8); 267(9); 413(10); −2, 180(11); −17, 731(12);
−50, 533(13); 110, 176(14); 1, 966,797(15).

A calculation of A_n for $0 \leqslant n \leqslant 900$ has also been made using a double-precision algorithm based on (4.5). At $n = 110$ the calculation agrees with the exact calculation to 13 significant places. The value of A_{900} is 3.217×10^{1648}.

The regular sign reversal seen in the first few vaues persists, with a gradual increase in the interval between successive sign changes from 2 or 3

at the beginning values to 6 or 7 for n near 900. For $0 \leqslant n \leqslant 900$, however, only A_2 is zero.

The author wishes to thank H. Rappaport and D. Royster who performed some of the numerical calculations.

References

1. H.W. Becker and J. Riordan, The arithmetic of Bell and Stirling numbers, *Amer. J. Math.* **70** (1948), 385–394.
2. E. T. Bell, Exponential numbers, *Amer. Math. Monthly* **41** (1934), 411–419.
3. E. T. Bell, The iterated exponential integers, *Ann. of Math.* **39** (1938), 539–557.
4. Chinthayama and J. M. Gandhi, On numbers generated by $e^{s(e^x-1)}$, *Canad. Math. Bull.* **10** (1967), 751–754.
5. L. Comtet, "Advanced Combinatorics," Chap. 5, Reidel, Dordrecht, 1974.
6. M. Hall, Arithmetic properties of a partition function, Abstr. 200, *Bull. Amer. Math. Soc.* **40** (1934).
7. J. W. Layman and C. L. Prather, Generalized Bell numbers and zeros of successive derivatives of an entire function, *J. Math. Anal. Appl.* **96** (1983), 42–51.
8. J. Levine and R. E. Dalton, Minimum periods, modulo p, of first-order Bell exponential integers, *Math. Comp.* **16** (1962), 416–423.
9. C. Radoux, Nombres de Bell, modulo p premier, et extensions de degré p de F_p, *C. R. Acad. Sci. Paris Sér. A* **281** (1975), 879–882.
10. G. C. Rota, The number of partitions of a set, *Amer. Math. Monthly* **71** (1964), 498–504.
11. J. Touchard, Propriétés arithmétiques de certain nombres recurrents, *Ann. Soc. Sci. Bruxelles A* **53** (1933), 21–31.
12. G. T. Williams, Numbers generated by the function e^{e^x-1}, *Amer. Math. Monthly* **52** (1945), 323–327.
13. N. Zierler, Linear Recurring Sequences, *J. Soc. Indust. Appl. Math.* **7** (1959), 31–48.