

Minimum Periods, Modulo p , of First-Order Bell Exponential Integers

By Jack Levine and R. E. Dalton

1. Introduction. The integers of the title, $B(n)$, can be defined by the generating function, given by Bell [1, 2],

$$(1.1) \quad e^{e^x-1} = \sum_{n=0}^{\infty} B(n) \frac{x^n}{n!}.$$

These numbers have been known for a long time and have a variety of interesting interpretations which include:

- (a) $B(n)$ = the number of rhyming schemes in a stanza of n lines (attributed to Sylvester by Becker [3],
- (b) $B(n)$ = the number of pattern sequences for words of n letters, as used in cryptology, Levine [4],
- (c) $B(n)$ = number of ways n unlike objects can be placed in 1, 2, 3, \dots , or n like boxes (allowing blank boxes), Whitworth [5, p. 88],
- (d) $B(n)$ = number of ways a product of n (distinct) primes may be factored, Jordan [6, p. 179], Williams [7].

Epstein [8] extended the definition of $B(n)$ to include all real and complex numbers n by means of the representation

$$(1.2) \quad B(n) = \frac{1}{e} \sum_{t=0}^{\infty} \frac{t^n}{t!}.$$

He also gave several asymptotic formulas for $B(n)$ in addition to the numerical values of $B(n)$ for $n = 1, \dots, 20$. This paper, as well as [2], contains numerous references dealing with these numbers.

For computational purposes, various defining relations are known, for example,

$$(1.3) \quad B(n) = \sum_{r=1}^n \sum_{k=0}^r \frac{(-1)^k}{r!} \binom{r}{k} (r-k)^n,$$

given by Bell [1], and Mendelsohn and Riordan [9]. This formula, (1.3), is equivalent to

$$(1.4) \quad B(n) = \sum_{r=1}^n S(n, r),$$

where $S(n, r)$ are Stirling numbers of the second kind, and which was obtained by Broggi [10] and Becker and Riordan [11]. Other references relative to (1.3) and (1.4) are found in Epstein [8].

$$(1.5) \quad B(n+1) = (B+1)^n,$$

where on the right, B^m is to be replaced by $B(m)$ after expansion, was given by d'Ocogne [12]. (See also [1, 2, 11]).

The difference formula,

$$(1.6) \quad B(n) = \Delta^n B(1),$$

Becker and Browne [3], was found to be the simplest for a digital computer, and was used in the computation of the $B(n)$ given in the present paper.

For a study of arithmetic properties of $B(n)$, the congruence of Touchard [13],

$$(1.7) \quad B(n + p) \equiv B(n) + B(n + 1), \quad \text{mod } p,$$

for p a prime, is basic.

In addition, for our purposes, we mention the following congruence given by Hall [14], Touchard [13], and Williams [7],

$$(1.8) \quad B(n + p^m) \equiv B(n + 1) + mB(n), \quad \text{mod } p.$$

It is known that the (minimum) period of the sequence (reduced mod p)

$$(1.9) \quad B(0), B(1), B(2), \dots, B(n), \dots$$

is a divisor of

$$(1.10) \quad N_p = \frac{p^p - 1}{p - 1};$$

and Williams [7] has shown this minimum period is precisely N_p for $p = 2, 3, 5$.

In this paper we extend these results to primes $p > 5$. The results obtained are stated in the theorem below.

THEOREM. *The minimum period, mod p , of the sequence $B(0), B(1), \dots, B(n)$, of first-order Bell exponential integers is N_p for $p = 7, 11, 13$, and 17. For the remaining primes $p < 50$, $p = 19, 23, 29, 31, 37, 41, 43, 47$, no known proper divisor, N , of N_p , with $N \leq 10^{40}$ can be a period.*

In the course of the computations connected with this theorem the results of Cunningham [15] on factoring N_p have been extended to include several new factors for certain p . These are exhibited in Table 3.

In addition, the values of $B(n)$, $n \leq 74$, have been computed, and are given in Table 1. This extends results of Gupta [16] for $n \leq 50$. Also, the values of $B(n)$, mod p , ($n \leq p$, $p < 50$) are given in Table 2. Such values are needed in testing for periods.

2. Computation of $B(n)$. The symbolic binomial expansion (1.5), though useful in the computation of the first several $B(n)$, becomes bulky and time-consuming as n increases, since each successive $B(n)$ computed by this iterative scheme requires $n - 2$ multiplications and n additions involving larger numbers at each iteration. Formula (1.6), together with the initial values $B(0) = 1$, $B(1) = 1$, by contrast, requires but $n - 1$ additions for each new $B(n)$. (See Becker and Browne [3]). Such a difference formula as (1.6) is ideally suited for a digital computer, since it substitutes fixed-point addition for multiplication in which accuracy to the unit's digit must always be maintained. The only limitation which presented itself was the increasing size of the integers and differences involved. Using an octuple-precision addition subroutine, the numbers were generated on the difference table until a $B(n)$ or a difference exceeded 80 digits, the capacity of a standard IBM card. This

TABLE I
The Exponential Integers $B(n)$, $0 \leq n \leq 74$

n		
0	1	
1	1	
2	2	
3	5	
4	15	
5	52	
6	203	
7	877	
8	4140	
9	21147	
10	115975	
11	678370	
12	4213397	
13	27644137	
14	190899322	
15	1382958515	
16	0480142147	1
17	2864869804	8
18	20768061159	68
19	2742205057	583
20	4158235372	5172
21	9816156751	47486
22	5738447323	450671
23	5855084346	4415200
24	9294805289	44595886
25	2229999353	463859033
26	3618756274	4963124652
27	6059989389	4571704793
28	9934652455	6053940459
29	0275191172	3880193886
30	9332450147	4901451180
31	6485095653	5894622637
32	3818925644	7004990871
33	6704728147	9284600760
34	2388656799	8864036046
35	3340426570	1956026656
		5
		102933
		1280646
		16295958
		211950393
		2816002030
		61
		713
		8467

condition occurred during the computation of $B(75)$. The program, which used the SOAP I assembly program, was used on an IBM 650 to compute the 75 numbers in 73 minutes. A check was made with Gupta's highest value, $B(50)$, and the numbers were found to be identical.

3. Factorization of N_p , ($p < 50$). From a result of Fontene [17], it follows that all factors of N_p are of the form $2kp + 1$, when p is an odd prime. Using this information, a program was developed for the Univac 1105 in the USE compiler language. This simply involved successive division of N_p by divisors of the form

$$P_k = 2pk + 1, \quad k = 1, 2, 3, \dots$$

until a zero remainder was reached. Since the routine was single-precision for the divisors, the P_k 's were limited in magnitude to one accumulator length on the Univac 1105, or to values $P_k < 2^{35}$.

Table 3 gives the N_p and the factors thus obtained.

The following is a summary of new prime factors and other information not contained in Cunningham [15, p. 72].

Case $p = 17$. N_{17} is completely factored into the three prime factors 10949, 1749233, 2699538733.

Case $p = 19$. No factors of N_{19} have been found, but N_{19} contains no factor $< 17,005,305$

TABLE 3
 N_p 's and Prime Factors (Indicated by)*

p	$N_p = \frac{p^p - 1}{p - 1}$
5	$N_5 = 781 = 11 \cdot 71^*$
7	$N_7 = 1\ 37257 = 29^* \cdot 4733^*$
11	$N_{11} = 2\ 85311\ 67061 = 15797^* \cdot 1806113^*$
13	$N_{13} = 2523\ 95922\ 16021 = 53^* \cdot 264031^* \cdot 1803647^*$
17	$N_{17} = 51702\ 51636\ 78960\ 47761 = 10949^* \cdot 1749233^* \cdot 2699538733^*$
19	$N_{19} = 1099\ 12203\ 09223\ 96438\ 40221$ No known prime factors
23	$N_{23} = 94911\ 21818\ 11268\ 72883\ 43196\ 77753 = 461^* \cdot 1289^* \cdot 1597216194112486480522357$
29	$N_{29} = 9\ 17030\ 76898\ 61468\ 33772\ 08150\ 52610\ 77188\ 02981 = 59^* \cdot 16763^* \cdot 84449^* \cdot 2428577^* \cdot 14111459^* \cdot 32037737880884399$
31	$N_{31} = 56897\ 24710\ 24107\ 86528\ 70214\ 34301\ 97715\ 85348\ 24481$ No known prime factors
37	$N_{37} = 29\ 31981\ 93216\ 04953\ 92799\ 53613\ 49988\ 42485\ 03538\ 78009\ 36166\ 51181 = 149^* \cdot 1999^* \cdot 7993^*$, (quotient > 40 digits)
41	$N_{41} = 33271\ 94076\ 58177\ 99967\ 83498\ 10240\ 83656\ 39964\ 72332\ 54041\ 27485\ 81284\ 48841 = 83^*$, (quotient > 40 digits)
43	$N_{43} = 4129\ 46984\ 92929\ 20838\ 07232\ 88782\ 88579\ 08531\ 14434\ 61669\ 54570\ 31137\ 54094\ 99893 = 173^* \cdot 6709^*$, (quotient > 40 digits)
47	$N_{47} = 84\ 30270\ 13796\ 61926\ 57970\ 97431\ 77268\ 05988\ 90944\ 54377\ 04795\ 47313\ 54904\ 95405\ 42692\ 40497 = 1693^*$, (quotient > 40 digits)

Case $p = 23$. No new prime factors of N_{23} have been found, but the third factor 1,597,216,194,112,486,480,522,357 contains no factor $< 59,929,399$

Case $p = 29$. Four new prime factors of N_{29} are 16763, 84449, 2428577, 14111459.

4. Determination of minimum periods, mod p . The knowledge of $B(1), B(2), \dots, B(p)$, (or of any p consecutive B 's) will determine the complete set of B 's, mod p . Hence, if N be a factor of N_p , to test for a period of the sequence $\{B(n)\}$ mod p , it is sufficient to calculate $B(N + 1), B(N + 2), \dots, B(N + p)$, mod p , and compare with $B(1), B(2), \dots, B(p)$, mod p .

Furthermore, if N_p can be expressed as a product of r factors, it is not necessary to test all possible combinations of factors for periods, but merely the combinations of $r - 1$ factors. A positive result would indicate what further testings are necessary.

In case the complete factorization of N_p into prime factors is unknown it may not be possible to find the minimum period.

The actual testing of the various factors for the period property was accomplished on an IBM 650. The program requires N , the factor to be tested; p , the particular prime; and $B(1), B(2), \dots, B(p)$, mod p . These B 's were obtained from a modification of the program used to calculate Table 1 and are given in Table 2. The program used could test any factor less than 10^{40} . It would, of course, be impractical to calculate every B through $B(N + p)$, so a process of proceeding in jumps of powers of p by means of (1.8) is used.

The factor N being tested is first expressed to the base p ,

$$(4.1) \quad N = a_n p^n + a_{n-1} p^{n-1} + \dots + a_1 p + a_0.$$

The various steps are then (all calculations mod p):

(1) Calculate $B(p + 1)$ by (1.7).

(2) Calculate $B(a_n p^n + x)$, $x = 1, 2, \dots, p + 1$, by the iterations

$$(4.2) \quad B(tp^n + y) = B((t - 1)p^n + y + 1) + nB((t - 1)p^n + y),$$

$$(4.3) \quad B(tp^n + p + 1) = B(tp^n + 1) + B(tp^n + 2),$$

where $t = 1, 2, \dots, a_n$; $y = 1, 2, \dots, p$. Equation (4.2) follows from (1.8), and (4.3) from (1.7).

(3) Calculate $B(a_n p^n + a_{n-1} p^{n-1} + x)$, $x = 1, 2, \dots, p + 1$, by

$$(4.4) \quad B(up^{n-1} + z) = B((u - 1)p^{n-1} + z + 1) + (n - 1)B((u - 1)p^{n-1} + z),$$

$$(4.5) \quad B(up^{n-1} + p + 1) = B(up^{n-1} + 1) + B(up^{n-1} + 2),$$

where $u = 1, 2, \dots, a_{n-1}$; $z = a_n p^n + 1, \dots, a_n p^n + p$.

This procedure is continued until we reach

$$(4.6) \quad B(M + 1), B(M + 2), \dots, B(M + p),$$

where

$$M = a_n p^n + a_{n-1} p^{n-1} + \dots + a_1 p.$$

Since one member of (4.6) is $B(N)$, we start from that point and calculate

$$B(N+1), B(N+2), \dots, B(N+p),$$

which are then compared with

$$B(1), B(2), \dots, B(p),$$

for the period property. The results of these calculations have been given in the theorem of Section 1.

North Carolina State College
Raleigh, North Carolina

1. E. T. BELL, "Exponential numbers," *Amer. Math. Monthly*, v. 41, 1934, p. 411-419.
2. E. T. BELL, "The iterated exponential integers," *Ann. of Math.*, v. 39, 1938, p. 539-557.
3. H. W. BECKER & D. H. BROWNE, "Problem E461 and solution," *Amer. Math. Monthly*, v. 48, 1941, p. 701-703.
4. JACK LEVINE, "A binomial identity related to rhyming sequences," *Math. Mag.*, v. 32, 1958, p. 71-74.
5. W. A. WHITWORTH, *Choice and Chance*, Hafner Publ. Co., New York, 1951.
6. C. JORDAN, *Calculus of Finite Differences*, Second Edition, Chelsea Publ. Co., New York, 1950.
7. G. T. WILLIAMS, "Numbers generated by the function e^{x-1} ," *Amer. Math. Monthly*, v. 52, 1945, p. 323-327.
8. L. F. EPSTEIN, "A function related to the series for e^{x^2} ," *J. Math. Phys.*, v. 18, 1939, p. 153-173.
9. N. S. MENDELSON & J. RIORDAN, "Problem 4340 and solution," *Amer. Math. Monthly*, v. 58, 1951, p. 46-48.
10. U. BROGGI, "Su di qualche applicazione dei numeri di Stirling," *Ist. Lombardo Rend.*, II. s., v. 66, 1933, p. 196-202.
11. H. W. BECKER & J. RIORDAN, "The arithmetic of Bell and Stirling numbers," *Amer. J. Math.*, v. 70, 1948, p. 385-394.
12. M. D'OCAGNE, "Sur une classe de nombres remarquables," *Amer. J. Math.*, v. 9, 1887, p. 353-380. (See also 1, 2, 11).
13. J. TOUCHARD, "Propriétés arithmétiques de certains nombres récurrents," *Ann. Soc. Sci. Bruxelles*, v. 53A, 1933, p. 21-31.
14. M. HALL, "Arithmetic properties of a partition function," (Abstract 200), *Bull. Amer. Math. Soc.*, v. 40, 1934.
15. A. CUNNINGHAM, "Factorization of $N = Y^Y \pm 1$ and $X^{X^Y} \pm Y^{X^Y}$," *Messenger of Math.*, v. 45, 1915, p. 49-75.
16. H. GUPTA, *Tables of Distribution*, East Punjab University, Research Bulletin, v. 2, 1950, p. 44.
17. G. FONTENE, "Problem 2137 and solution," *Nouvelle Annales de Math.*, v. 13, 1913, p. 383-384.