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],

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

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, $\cdots$, 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

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

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

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

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

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

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

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].

$$B(n+1) = (B+1)^n, \tag{1.5}$$

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]).

Received February 16, 1962.

The difference formula,

$$B(n) = \Delta^n B(1), \tag{1.6}$$

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],

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

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],

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

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

$$B(0), B(1), B(2), \cdots, B(n), \cdots \tag{1.9}$$

is a divisor of

$$N_p = \frac{p^p - 1}{p - 1}; \tag{1.10}$$

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* $B(0), B(1), \cdots, B(n)$, *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* $N \leqq 10^{40}$ *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 $B(n)$, $n \leqq 74$, have been computed, and are given in Table 1. This extends results of Gupta [16] for $n \leqq 50$. Also, the values of $B(n)$, mod p, ($n \leqq p, p < 50$) 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 1

The Exponential Integers $B(n)$, $0 \leqq n \leqq 74$

			n
		1	0
		1	1
		2	2
		5	3
		15	4
		52	5
		203	6
		877	7
		4140	8
		21147	9
		115975	10
		678570	11
		4213597	12
		27644437	13
		190899322	14
		1382958545	15
	1	0480142147	16
	8	2864869804	17
	68	2076806159	18
	583	2742205057	19
	5172	4158235372	20
	47486	9816156751	21
	450671	5738447323	22
	4415200	5855084346	23
	44595886	9294805289	24
	463859033	2229999353	25
	4963124652	3618756274	26
5	4571704793	6059989389	27
61	6053940459	9934652455	28
713	3980193886	0275191172	29
8467	4901451180	9332450147	30
102933	5894622637	6485095653	31
1280646	7004990871	3818925644	32
16295958	9284600760	6764728147	33
211950393	8864036046	2388656799	34
2816002030	1956026656	3340426570	35

				3	8197147298	9481833997	5525681317	36
				52	8683662085	5044790194	5575624941	37
				746	2898920956	2533052309	9540639146	38
				10738	8233307746	9283276885	7986425209	39
				157450	5883912049	3128932434	4702531067	40
				2351152	5077406176	2820069407	7243788988	41
				35742549	1988726172	9135350865	6626642567	42
				552950118	7971654843	2171469328	0737767385	43
				8701963427	3870550890	2360053185	5797148876	44
			13	9258505266	2636696023	4705399365	4079693415	45
			226	5418219334	4940029284	8444470539	2276158355	46
			3745	0059502461	5111965053	4209643151	0120174682	47
			62891	9796303118	4154202104	5407184953	7746015761	48
			1072613	7154573358	4003422155	1859000263	3917247281	49
			18572426	8771078270	4382577671	8190891749	9221852770	50
			326398387	0004111524	8569518301	9158252441	9255819477	51
			5820533802	4195872785	4646270632	1859914950	3972126463	52
		10	5292851801	4714166107	7812980215	8353492840	2714242132	53
		193	1728758914	5618265728	9500692855	0325734983	2850302011	54
		3593	3408596862	2831041960	1885980436	6106538872	6959079837	55
		67756	8532064582	4322581483	0683714197	4597905321	6268760300	56
		1294826	6194750696	4462616580	6338060009	1749160260	9372517195	57
		25071363	5898429611	4560786627	4375749422	5301562344	5622326263	58
		491767433	3630962165	9000944152	6248968535	9101824891	9168867818	59
		9769393074	6700755298	6994066961	6754555502	4634775747	4482558637	60
	19	6523644715	4794148211	4228389322	7899633456	7346067337	0562378245	61
	400	2373048214	5478623052	2819234667	5449355269	6306024008	2269259738	62
	8250	7717004056	2488991245	6724304738	0284501901	3433711094	3817172961	63
	172134	1433573588	5093436996	3665272571	1255575751	8404975804	5339873395	64
	3633778	7854578993	2241525768	2767737441	4100369945	6043598236	5219287372	65
	77605907	2388436694	8215593085	7960017792	7780598875	1927803800	0759795263	66
	1676501284	3015234533	6721288085	4005182365	7483175898	8866047702	1013719409	67
3	6628224206	6961354788	3464061802	8539032699	1748479319	0948067172	5803995436	68
80	9212768387	9478363368	4627770706	6239391942	3239986492	7377173674	4420003007	69
1807	5003898340	5112375567	8442449836	9141305841	2344680979	0822799303	5088029195	70
40813	0093410464	2742599456	0096213470	6689859323	6369225324	4336559472	6056131962	71
931452	8182092653	2882514514	8352734180	6516792394	6744967255	7893570602	9134658745	72
21483462	3568478894	4527656055	1192833336	7140719361	2910039971	6139004370	1285425833	73
500690802	4247925379	7070764709	5772222046	3116781409	6591601595	3698116129	8714301202	74

TABLE 2

$B(n)$ *mod* p, $0 \leqq n \leqq p$, $p \leqq 50$

n	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	0	2	2	2	2	2	2	2	2	2	2	2	2	2	2
3		2	0	5	5	5	5	5	5	5	5	5	5	5	5
4			0	1	4	2	15	15	15	15	15	15	15	15	15
5			2	3	8	0	1	14	6	23	21	15	11	9	5
6				0	5	8	16	13	19	0	17	18	39	31	15
7				2	8	6	10	3	3	7	9	26	16	17	31
8					4	6	9	17	0	22	17	33	40	12	4
9					5	9	16	0	10	6	5	20	32	34	44
10					2	2	1	18	9	4	4	17	27	4	26
11					2	9	15	4	1	28	11	27	20	30	31
12						11	11	5	20	13	15	0	27	27	0
13						2	6	7	1	13	1	35	23	38	24
14							15	14	12	7	20	5	1	5	33
15							11	16	9	20	30	36	9	27	42
16							14	15	5	28	16	2	4	42	38
17							2	1	6	17	8	29	19	19	12
18								10	6	16	1	21	17	1	22
19								2	9	20	21	28	16	20	44
20									4	20	3	23	3	26	43
21									16	15	25	32	22	27	5
22									22	5	26	32	33	39	25
23									2	25	19	6	3	36	29
24										7	16	34	23	42	3
25										24	2	0	3	27	20
26										11	15	26	38	41	10
27										21	16	19	13	42	0
28										18	17	12	13	27	23
29										2	12	21	35	1	30
30											3	10	23	11	22
31											2	1	4	35	44
32												35	2	21	18
33												35	37	3	35
34												26	34	28	46
35												17	14	33	11
36												6	35	32	37
37												2	40	28	45
38													31	3	25
39													6	7	16
40													5	12	17
41													2	41	5
42														17	13
43														2	9
44															23
45															37
46															19
47															2

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

$$P_k = 2pk + 1, \qquad k = 1, 2, 3, \cdots$$

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	$N_p = \dfrac{p^p - 1}{p - 1}$
5	N_5 = 781 = 11*·71*
7	N_7 = 1 37257 = 29*·4733*
11	N_{11} = 2 85311 67061 = 15797*·1806113*
13	N_{13} = 2523 95922 16021 = 53*·264031*·1803647*
17	N_{17} = 51702 51636 78960 47761 = 10949*·1749233*·2699538733*
19	N_{19} = 1099 12203 09223 96438 40221 No known prime factors
23	N_{23} = 94911 21818 11268 72883 43196 77753 = 461*·1289*· 1597216194112486480522357
29	N_{29} = 9 17030 76898 61468 33772 08150 52610 77188 02981 = 59*·16763*·84449*·2428577*·14111459*·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*·1999*·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*·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 $B(1)$, $B(2)$, $\cdots$, $B(p)$, (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 $B(N+1)$, $B(N+2)$, $\cdots$, $B(N+p)$, mod p, and compare with $B(1)$, $B(2)$, $\cdots$, $B(p)$, 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 $B(1)$, $B(2)$, $\cdots$, $B(p)$, 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,

$$N = a_n p^n + a_{n-1} p^{n-1} + \cdots + a_1 p + a_0 . \tag{4.1}$$

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

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

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

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

$$B(tp^n + p + 1) = B(tp^n + 1) + B(tp^n + 2), \tag{4.3}$$

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

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

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

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

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

This procedure is continued until we reach

$$B(M+1), B(M+2), \cdots, B(M+p), \tag{4.6}$$

where

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

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

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

which are then compared with

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

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^{e^x-1}," *Amer. Math. Monthly*, v. 52, 1945, p. 323–327.
8. L. F. Epstein, "A function related to the series for e^{e^x}," *J. Math. Phys.*, v. 18, 1939, p. 153–173.
9. N. S. Mendelsohn & 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 recurrents," *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 $X^{XY} \pm Y^{XY}$," *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.