Contemporary Mathematics
Volume **00**, 0000

The period of the Bell exponential integers modulo a prime

SAMUEL S. WAGSTAFF, JR.

Abstract. We show that the minimum period of the Bell exponential integers reduced modulo p is $(p^p - 1)/(p - 1)$ for all primes $p < 82$ and several larger p. Our proof of this result requires the prime factorization of these periods. For about one-half of the primes p the factoring is aided by an algebraic formula.

The first-order Bell exponential integer $B(n)$ is the number of ways of placing n distinguishable objects into 1 to n indistinguishable cells so that no cell is empty. The Bell numbers may be expressed as a sum $B(n) = \sum_{r=1}^{n} S(n,r)$ of Stirling numbers of the second kind. See [**4**] and its references.

The first few Bell numbers may be computed easily from the difference formula $B(n) = \Delta^n B(1)$ of Cesàro [**2**]. The first few values are $B(0) = 1$ (by definition), $B(1) = 1$, $B(2) = 2$, $B(3) = 5$, $B(4) = 15$, $B(5) = 52$ and $B(6) = 203$.

Consider the sequence of Bell numbers reduced modulo a prime p. After one computes $B(n) \bmod p$ for $0 \le n < p$ by Cesàro's formula, one may compute further terms quickly by the congruence

$$B(n+p) \equiv B(n) + B(n+1) \pmod{p} \tag{1}$$

1991 *Mathematics Subject Classification.* Primary 11-04, 11B73; Secondary 11Y05, 12-04, 12E10, 12Y05.

Key words and phrases. Bell numbers, period modulo p, integer factorization, Aurifeuillian factorization.

Some of the computing reported in this work was performed on a MasPar computer at Purdue University which was supported in part by NSF Infrastructure Grant CDA-9015696.

The final version of this paper will be submitted for publication elsewhere.

of Touchard [7]. It is clear from (1) that the sequence $\{B(n) \bmod p; n = 0, 1, \dots\}$ is eventually periodic. Williams [8] proved that for each prime p the sequence is periodic from the beginning and that the minimum period divides

$$N_p = \frac{p^p - 1}{p - 1}.$$

By hand compuation, he showed that the minimum period is precisely N_p for $p = 2$, 3 and 5. Levine and Dalton [4] used a computer to show that the minimum period is exactly N_p for $p = 7$, 11, 13 and 17. They also investigated the period for the other primes < 50. Using the same general technique, we show that the minimum period is exactly N_p for each prime < 82 and for several larger primes. Great advances in integer-factoring methods since 1962 allowed us to extend their work so far.

Given a prime p, to test whether the period of $\{B(n) \bmod p\}$ divides some factor N of N_p, it suffices because of (1) to compare $B(N+i) \bmod p$ with $B(i) \bmod p$ for $0 \le i < p$. For primes $p < 180$, we factored N_p as much as possible, using techniques described below. The factorization of N_p was complete for all primes $p < 82$ and for the six larger primes mentioned in Theorem 1. For each prime $p < 180$ and each known prime divisor q of N_p we tested whether the period divides $N = N_p/q$. It never did, and we have proved

THEOREM 1. *The minimum period of the sequence* $\{B(n) \bmod p\}$ *is* N_p *when* p *is a prime* < 82 *and also when* $p = 89$*,* 97*,* 101*,* 163*,* 167 *or* 173*.*

We conjecture that the minimum period of the sequence $\{B(n) \bmod p\}$ is N_p for every prime p.

We computed $B(N) \bmod p$ for large N via the congruence $B(n + p^m) \equiv B(n+1) + mB(n) \pmod p$ of Touchard [7], which generalizes (1). Starting from the block $B(i) \bmod p$, $0 \le i \le p$, we computed successive blocks of length $p + 1$, using the digits of N in radix p to direct our choice of the blocks towards the final block $B(N + i) \bmod p$, $0 \le i \le p$. See Levine and Dalton [4] for details.

We now describe our efforts to factor N_p for primes $p < 180$. The Table shows the factorization of those N_p which we could factor completely. We use Pxx in the Table to mean a prime of xx digits. Some trial division was done first, using the fact that all prime factors of N_p have the form $2kp + 1$ for some positive integer k. Most of the larger factors in the Table were found by the Elliptic Curve Method [3], using a program written by Peter Montgomery. This work was aided greatly by the use of Aurifeuillian factorizations. That is, when p is prime and $\equiv 1 \pmod 4$, N_p splits algebraically into two nearly equal factors (called pL and pM in the Table). We computed these two Aurifeuillian factors from Theorem 2.

We would be happy to send our partial factorizations of the N_p not shown in the Table to any reader. The first p for which we could not factor N_p completely was $p = 83$, which has a composite cofactor of 147 digits. The smallest remaining composite cofactor of an N_p was the 100-digit divisor of $113M$. For the primes $p < 180$ not listed in the Table, we checked that no known proper divisor of N_p can be a period.

For integers $n > 0$ let $\Phi_n(x)$ denote the cyclotomic polynomial. When p is an odd prime, $N_p = \Phi_p(p)$. Let (m, n) be the greatest common divisor of m and n. Let $\phi(n)$ denote Euler's totient function. Let $(m|n)$ be the Jacobi symbol. Theorem 2 follows from Theorem 1 of Schinzel [**6**].

THEOREM 2. *Let* $p \equiv 1 \pmod 4$ *be squarefree. Then there exist polynomials* $C_p(x)$ *and* $D_p(x)$ *with integer coefficients and degrees* $\phi(p)/2$ *and* $\phi(p)/2 - 1$, *respectively, with the following properties. For any odd positive integer* h,

$$\Phi_p(p^h) = (C_p(p^h) - p^{(h+1)/2} D_p(p^h))(C_p(p^h) + p^{(h+1)/2} D_p(p^h)).$$

The coefficients of $C_p(x)$ *and* $D_p(x)$ *may be computed from the identity*

$$C_p(x^2) - \sqrt{p}\, x D_p(x^2) = \prod_{\substack{s=1 \\ (s,p)=1}}^{(p-1)/2} (x^2 - 2(s|p) \cos \frac{2\pi s}{p} x + 1).$$

Brent [**1**] gives an algorithm for computing the coefficients of $C_p(x)$ and $D_p(x)$, which uses integer arithmetic throughout.

A table of coefficients of $C_p(x)$ and $D_p(x)$ for $p < 120$ may be found in Table 34 on page 453 ff. of Riesel [**5**].

To prove Theorem 1, we used Theorem 2 only when p is prime and $h = 1$.

Acknowledgements

I thank John W. Wrench, Jr. for suggesting this research and R. P. Brent for sending me a preprint of [**1**]. I am grateful to P. L. Montgomery for the use of his ECM program and for several factors which I missed. I thank A. K. Lenstra and B. Dixon for letting me use their ECM program for the MasPar computer. It found several factors in the Table.

REFERENCES

1. Richard P. Brent, *On computing factors of cyclotomic polynomials*, Math. Comp. **61** (1993), 131–149.
2. E. Cesàro, *Sur une équation aux différences mèlées*, Nouvelles Annales de Math. (3) **4** (1885), 36–40.
3. H. W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. of Math. **126** (1987), 649–673.
4. Jack Levine and R. E. Dalton, *Minimum periods, modulo p, of first-order Bell exponential integers*, Math. Comp. **16** (1962), 416–423.
5. Hans Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, 1985.
6. A. Schinzel, *On the primitive prime factors of* $a^n - b^n$, Proc. Cambridge Philos. Soc. **58** (1962), 555–562.

Table. Factors of $N_p = (p^p - 1)/(p - 1)$ for some primes p in $10 < p < 180$

p	Prime factorization of N_p
11	$15797 \cdot 1806113$
$13L$	1803647
$13M$	$53 \cdot 264031$
$17L$	2699538733
$17M$	$10949 \cdot 1749233$
19	$1099122030922396438402 21$
23	$461 \cdot 1289 \cdot 831603031789 \cdot 1920647391913$
$29L$	$84449 \cdot 2428577 \cdot 549334763$
$29M$	$59 \cdot 16763 \cdot 14111459 \cdot 58320973$
31	$568972471024107865287021434301977158534824481$
$37L$	$149 \cdot 4190342555354483999815 8239$
$37M$	$1999 \cdot 7993 \cdot 16651 \cdot 17317 \cdot 10192715656759$
$41L$	$1752341 \cdot 20567159 \cdot 1876859311090803007$
$41M$	$83 \cdot 5926187589691497537793497756719$
43	$173 \cdot 120401 \cdot P62$
47	$1693 \cdot 25574249289676351147463853018887601 7 \cdot P39$
$53L$	$107 \cdot 16505521259654533 \cdot 1434707204785893132883134 73$
$53M$	$141829 \cdot 1303396057963132488045544988140899439 2143$
59	$709 \cdot 141579233 \cdot P92$
$61L$	$977 \cdot 343625872243632312073 \cdot 3988532864560717926099179959 07$
$61M$	$1000403244183535565720394723140528028235711874491322863$
67	$269 \cdot 4021 \cdot 730837 \cdot 10960933 \cdot$ $\cdot 151495488509660402356228791573004 9 \cdot P69$
71	$105649 \cdot 3388409395214741 \cdot 17882954877203881 \cdot P93$
$73L$	$1414741 \cdot 1295720382587 \cdot 1192167517020392933 \cdot P31$
$73M$	$293 \cdot 439 \cdot 25239167 \cdot 56377463 \cdot 3611379501352361 \cdot P32$
79	$317 \cdot 1558537597 \cdot 171355071830508389477 \cdot$ $\cdot 5449313290804337826320291 3 \cdot P91$
$89L$	$179 \cdot 8009862103557709 \cdot 5964844210432006407836201 \cdot P43$
$89M$	$3730759891225349089330219913 3 \cdot P58$
$97L$	$P95$
$97M$	$389 \cdot 363751 \cdot 684640163 \cdot 1194372873374129476439060215 3 \cdot P51$
$101L$	$1213 \cdot 9931988588681 \cdot 102208068907493 \cdot 393101595766008847 \cdot P53$
$101M$	$607 \cdot 5657 \cdot 157561 \cdot P89$
163	$653 \cdot 2609 \cdot 41729 \cdot 31943437 \cdot 3727539197017 \cdot 391683908074297 \cdot$ $\cdot 8224734227858383253 \cdot P294$
167	$16033 \cdot 1001953110409 \cdot 6698062506786295140456261 89 \cdot P326$
$173L$	$347 \cdot 685081 \cdot P184$
$173M$	$161297590410850151 \cdot P176$

7. J. Touchard, *Propriétés arithmétiques de certains nombres récurrents*, Ann. Soc. Sci. Bruxelles **53A** (1933), 21–31.
8. G. T. Williams, *Numbers generated by the function* e^{e^x-1}, Amer. Math. Monthly **52** (1945), 323–327.

Department of Computer Sciences, Purdue University, West Lafayette, IN 47907

E-mail address: ssw@cs.purdue.edu