CERIAS Tech Report 2010-01

The period of the Bell numbers modulo a prime

by Peter Montgomery, Sangil Nahm, Samuel Wagstaff Jr
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

MATHEMATICS OF COMPUTATION
Volume 00, Number 0, Pages 000–000
S 0025-5718(XX)0000-0

THE PERIOD OF THE BELL NUMBERS MODULO A PRIME

PETER L. MONTGOMERY, SANGIL NAHM, AND SAMUEL S. WAGSTAFF, JR.

Abstract. We discuss the numbers in the title, and in particular whether the minimum period of the Bell numbers modulo a prime p can be a proper divisor of $N_p = (p^p - 1)/(p - 1)$. It is known that the period always divides N_p. The period is shown to equal N_p for most primes p below 180. The investigation leads to interesting new results about the possible prime factors of N_p. For example, we show that if p is an odd positive integer and m is a positive integer and $q = 4m^2p + 1$ is prime, then q divides $p^{m^2p} - 1$. Then we explain how this theorem influences the probability that q divides N_p.

1. Introduction

The Bell exponential numbers $B(n)$ are positive integers that arise in combinatorics. They can be defined by the generating function

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

See [5] for more background. Williams [11] proved that for each prime p, the Bell numbers modulo p are periodic and that the period divides $N_p = (p^p - 1)/(p - 1)$. In fact the minimum period equals N_p for every prime p for which this period is known.

Theorem 1.1. *The minimum period of the sequence $\{B(n) \bmod p\}$ is N_p when p is a prime < 126 and also when $p = 137$, 149, 157, 163, 167 or 173.*

Theorem 1.1 improves the first part of Theorem 3 of [10]. The statements about the primes p = 103, 107, 109, 137, 149 and 157 are new here and result from calculations we did using the same method as in [10]. These calculations are possible now because new prime factors have been discovered for these N_p. Table 1 lists all new prime factors discovered for N_p since [10], even when the factorization remains incomplete. Table 1 uses the same notation and format as Table 1 of [10]. The "L" and "M" in the table represent pieces of algebraic factorizations explained in [10].

1991 *Mathematics Subject Classification.* 11B73, 11A05, 11A07, 11A51.
Key words and phrases. Bell numbers, period modulo p.
This work was supported in part by the CERIAS Center at Purdue University.

Table 1. Some new prime factors

p	New prime factors of N_p
103	66372424944116825940401913193.
103	167321256949237716863040684441514323749790592645938001.P98
107	847261197784821583381604854855693.P165
109L	7080226051839942554344215177418365113791664072203.P58
137L	14502230930480689611402075474137987.P85
149L	14897084928588789671974072568141537826492971.P115
149M	24356237167368011037018270166971738740925336580189261.P84
151	7606586095815204010302267401765907353.C277
157L	26924627624276327689812\
	23371662397585576503452818526793420773.P99
179	618311908211315583991314548081149.C369

Theorem 1.1 is proved by showing that the period does not divide N_p/q for any prime divisor q of N_p. (We made this check for each new prime q in Table 1, including those written as "Pxxx," and not just those for the p for which N_p is completely factored.) In [10], this condition was checked also for all pairs (p, q) of primes for which $p < 1100$, $q < 2^{31}$ and q divides N_p. It was conjectured there that the minimum period is always N_p. As early as 1979 [6] others wondered whether the minimum period is always N_p. See [3] for a summary of work on this conjecture up to 2008. We present a heuristic argument below supporting the conjecture.

Touchard's [8] congruence $B(n+p) \equiv B(n)+B(n+1) \bmod p$, valid for any prime p and for all $n \geq 0$, shows that any p consecutive values of $B(n) \bmod p$ determine the sequence modulo p after that point.

If N divides N_p, then one can test whether the period of the Bell numbers modulo p divides N by checking whether $B(N + i) \equiv B(i) \bmod p$ for $0 \leq i \leq p - 1$. The period divides N if and only if all p of these congruences hold.

A polynomial time algorithm for computing $B(n) \bmod p$ has been known at least since 1962 [5]. Pseudocode for the algorithm appears in [10].

In the last section of this note we give a heuristic argument for the probability that the conjecture holds for a prime p and estimate the expected number of primes $p > 126$ for which the conjecture fails. The most difficult piece of this heuristic argument is determining the probability that a given prime q divides N_p. We investigate this probability in the next section. The assumptions made in the heuristic argument are clearly labeled with the words "assume" or "assuming."

2. How often does $2kp + 1$ divide N_p as p varies?

It is well known that every prime factor of N_p has the form $2kp + 1$ when p is an odd prime. According to page 381 of Dickson [4], Euler proved this fact in 1755. On the following page Dickson writes that Legendre proved it again in 1798. A recent proof of a slightly more general result appears on page 642 of Sabia and Tesauri [7]. Here is a short proof. Suppose q is prime and $q \mid N_p$. The radix-p expansion

$$N_p = 1 + \sum_{i=1}^{p-1} p^i \equiv 1 + \sum_{i=1}^{p-1} p = 1 + p(p-1) \equiv 1 \bmod (p^2 - p)$$

shows $\gcd(N_p, p^2 - p) = 1$, whence $\gcd(q, p^2 - p) = 1$. In particular q is odd, $q \neq p$, and $q \nmid (p-1)$.

We have $p^p \equiv 1 \bmod q$ because $q \mid N_p$. Let d be the smallest positive integer for which $p^d \equiv 1 \bmod q$. We cannot have $d = 1$ because q does not divide $p-1$. But $d \mid p$, so $d = p$. By Fermat's little theorem, $p^{q-1} \equiv 1 \bmod q$, so $p \mid (q-1)$. The quotient $(q-1)/p$ must be even because both p and q are odd. Thus, $q = 2kp + 1$.

For each $1 \leq k \leq 50$ and for all odd primes $p < 100000$, we computed the fraction of the primes $q = 2kp + 1$ that divide N_p. For example, when $k = 5$ there are 1352 primes $p < 100000$ for which $q = 2kp + 1$ is also prime, and 129 of these q divide N_p, so the fraction is $129/1352 = 0.095$. This fraction is called "Prob" in Table 2 because it approximates the probability that q divides N_p, given that p and $q = 2kp + 1$ are prime, for fixed k.

Table 2. Probability that $(2kp+1) \mid N_p$

Odd k			Even k		
k	$1/(2k)$	Prob	k	$1/k$	Prob
1	0.500	0.503	2	0.500	1.000
3	0.167	0.171	4	0.250	0.247
5	0.100	0.095	6	0.167	0.173
7	0.071	0.076	8	0.125	0.496
9	0.056	0.047	10	0.100	0.096
11	0.045	0.042	12	0.083	0.082
13	0.038	0.051	14	0.071	0.068
15	0.033	0.033	16	0.063	0.064
17	0.029	0.032	18	0.056	0.111
19	0.026	0.021	20	0.050	0.050
21	0.024	0.016	22	0.045	0.054
23	0.022	0.021	24	0.042	0.042
25	0.020	0.021	26	0.038	0.052
27	0.019	0.021	28	0.036	0.036
29	0.017	0.022	30	0.033	0.031
31	0.016	0.019	32	0.031	0.055
33	0.015	0.021	34	0.029	0.032
35	0.014	0.015	36	0.028	0.030
37	0.014	0.014	38	0.026	0.024
39	0.013	0.011	40	0.025	0.020
41	0.012	0.010	42	0.024	0.023
43	0.012	0.010	44	0.023	0.020
45	0.011	0.012	46	0.022	0.022
47	0.011	0.011	48	0.021	0.025
49	0.010	0.014	50	0.020	0.043

The first observation is that usually Prob is approximately $1/k$ when k is even and $1/(2k)$ when k is odd. The greatest anomalies to this observation in the table are that Prob is about $2/k$ when $k = 2$, 18, 32 and 50, and that Prob is about $4/k$ when $k = 8$. Note that these exceptional values of k have the form $2m^2$ for $1 \leq m \leq 5$. (These numbers arise also in chemistry as the row lengths in the periodic table of elements.)

We will now explain these observations. Suppose k is a positive integer and that both p and $q = 2kp+1$ are odd primes. Let g be a primitive root modulo q.

If $p \equiv 1 \bmod 4$ or k is even (so $q \equiv 1 \bmod 4$), then by the Law of Quadratic Reciprocity

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \left(\frac{2kp+1}{p}\right) = \left(\frac{1}{p}\right) = +1,$$

so p is a quadratic residue modulo q. In this case $g^{2s} \equiv p \bmod q$ for some s. Now, by Euler's criterion for power residues, $(2kp+1) \mid (p^p - 1)$ if and only if p is a $(2k)$-ic residue of $2kp+1$, that is, if and only if $(2k) \mid (2s)$. It is natural to assume that $k \mid s$ with probability $1/k$ because k is fixed and s is a random integer.

If $p \equiv 3 \bmod 4$ and k is odd (so $q \equiv 3 \bmod 4$), then

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) = -\left(\frac{2kp+1}{p}\right) = -\left(\frac{1}{p}\right) = -1,$$

so p is a quadratic nonresidue modulo q. Now $g^{2s+1} \equiv p \bmod q$ for some s. Reasoning as before, $(2kp+1) \mid (p^p - 1)$ if and only if $(2k) \mid (2s+1)$, which is impossible. Therefore q does not divide N_p. (This statement is equivalent to Lemma 1.1(c) of [3].)

Thus, if we fix k and let p run over all primes, then the probability that $q = 2kp+1$ divides N_p is $1/k$ when k is even and $1/(2k)$ when k is odd because, when k is odd only those $p \equiv 1 \bmod 4$ (that is, half of the primes p) offer a chance for q to divide N_p.

In fact, when $k = 1$ and $p \equiv 1 \bmod 4$, q always divides N_p. This theorem must have been known long ago, but we could not find it in the literature.

Theorem 2.1. *If p is odd and $q = 2p+1$ is prime, then q divides N_p if and only if $p \equiv 1 \bmod 4$.*

Proof. We have just seen that q does not divide N_p when $p \equiv 3 \bmod 4$. If $p \equiv 1 \bmod 4$, then p is a quadratic residue modulo q, as was mentioned above, so $p^p = p^{(q-1)/2} \equiv +1 \bmod q$ by Euler's criterion. Finally, q is too large to divide $p-1$, so q divides N_p.

We now explain the anomalies, beginning with $k = 2$.

Theorem 2.2. *If $q = 4p+1$ is prime, then q divides N_p.*

This result was an old problem posed and solved more than 100 years ago. In [2] it was proposed as Problem 13058 by C. E. Bickmore and solved by him, by Nath Coondoo, and by others. Here is a modern proof.

Proof. Since $q \equiv 1 \bmod 4$, there exists an integer I with $I^2 \equiv -1 \bmod q$. Then

$$(1+I)^4 \equiv (2I)^2 \equiv -4 \equiv \frac{1}{p} \bmod q.$$

Hence

$$p^p \equiv \left(\frac{1}{p}\right)^{-p} \equiv (1+I)^{-4p} \equiv (1+I)^{1-q} \equiv 1 \bmod q$$

by Fermat's theorem. Thus, q divides $p^p - 1$. But $q = 4p+1$ is too large to divide $p-1$, so q divides N_p.

Lemma 2.3. *Suppose q is prime and $q \equiv 1 \bmod 4$. If the integer ℓ divides $(q-1)/4$, then ℓ is a quadratic residue modulo q.*

Proof. The hypothesis implies $\gcd(q,\ell)=1$. In particular $\ell \neq 0$. Factor

$$\ell = \pm \ell_1 \dots \ell_\nu \tag{2.1}$$

where each ℓ_j is prime.

The hypotheses that q is prime and $q \equiv 1 \bmod 4$ imply that ± 1 are quadratic residues modulo q.

We claim each ℓ_j is a quadratic residue modulo q, so their product (2.1) (or its negative) is also a quadratic residue.

If $\ell_j = 2$, then ℓ is even and $q \equiv 1 \bmod 8$. Since q is prime, 2 is a quadratic residue modulo q.

If instead ℓ_j is odd, then we can use quadratic reciprocity:

$$\left(\frac{\ell_j}{q}\right) = \left(\frac{q}{\ell_j}\right) = \left(\frac{1}{\ell_j}\right) = +1,$$

which completes the proof.

Theorem 2.4. *Let p be an odd positive integer and m be a positive integer. If $q = 4m^2p+1$ is prime, then q divides $p^{m^2p} - 1$.*

Proof. As in the proof of Theorem 2.2, $q \equiv 1 \bmod 4$, so there is an integer I with $I^2 \equiv -1 \bmod q$ and $(1+I)^4 \equiv -4 \bmod q$. By Lemma 2.3, m is a quadratic residue modulo q, so

$$-4m^2 \equiv (1+I)^4 m^2 \bmod q$$

is a fourth power modulo q, say $r^4 \equiv -4m^2 \bmod q$. Then

$$p^{m^2p} = \left(\frac{q-1}{4m^2}\right)^{(q-1)/4} \equiv ((-4m^2)^{-1})^{(q-1)/4} = r^{1-q} \equiv 1 \bmod q,$$

which proves the theorem.

Of course, Theorem 2.2 is the case $m=1$ of Theorem 2.4.

We now apply Theorem 2.4. As before, let g be a primitive root modulo q and let $a = g^{(q-1)/m^2} \bmod q$. Then a^j, $0 \le j < m^2$, are all the solutions to $x^{m^2} \equiv 1 \bmod q$. Let $b = p^p \bmod q$. By the theorem, $b^{m^2} \equiv 1 \bmod q$, so $b \equiv a^j \bmod q$ for some $0 \le j < m^2$. It is natural to assume that the case $j=0$, that is, $q \mid N_p$, happens with probability $1/m^2$.

In the case $m=2$, that is, $k=8$, we can do even better.

Theorem 2.5. *If $q = 16p+1$ is prime, then q divides $p^{2p}-1$.*

Proof. As in the proof of Theorem 2.2, there is an integer I with $I^2 \equiv -1 \bmod q$ and $(1+I)^4 \equiv -4 \bmod q$. Therefore, $(1+I)^8 \equiv 16 \equiv -1/p \bmod q$ and so

$$p^{2p} \equiv \left(\frac{-1}{p}\right)^{-2p} \equiv (1+I)^{-16p} \equiv (1+I)^{1-q} \equiv 1 \bmod q,$$

which proves the theorem.

Thus, a prime $q = 2kp+1$ divides $(p^p-1)(p^p+1)$ when $k=8$. Assuming that q has equal chance to divide either factor, the probability that q divides p^p-1 is $1/2$.

So far, we have explained all the behavior seen in Table 2. Further experiments with $q = 2m^2p+1$ lead us to the following result, which generalizes Theorems 2.4 and 2.5.

Theorem 2.6. *Suppose p, m, t are positive integers, with t a power of 2 and $t > 1$. Let $k = (2m)^t/2$ and $q = 2kp+1 = (2m)^t p+1$. If q is prime, then (a) p is a $(2t)$-th power modulo q, and (b) $p^{kp/t} \equiv 1 \bmod q$.*

Proof. To prove part (a), note that since $q \equiv 1 \bmod 2^t$, the cyclic multiplicative group $(\mathbf{Z}/q\mathbf{Z})^*$ of order $q-1$ has an element ω of order 2^t. Then $\omega^{2^{t-1}} \equiv -1 \bmod q$ so $I = \omega^{2^{t-2}}$ satisfies $I^2 \equiv -1 \bmod q$.

Now $m^t = (q-1)/(p2^t)$, so m is a quadratic residue modulo q by Lemma 2.3. We will show that $p^{-1} \equiv (1-q)/p = -(2m)^t \bmod q$ is a $(2t)$-th power modulo q.

If $t = 2$, then $-(2m)^t \equiv (2Im)^2 = (1+I)^4 m^2 \bmod q$ is a fourth power modulo q.

If $t > 2$, then $t \geq 4$ because t is a power of 2. Then $(q-1)/4 = 2mp((2m)^{t-1}/4)$ is divisible by $2m$. Hence $2m$ is a quadratic residue modulo q by Lemma 2.3. Therefore, $(2m)^t$ is a $(2t)$-th power modulo q. Finally, -1 is a (2^{t-1})-th power modulo q because 2^{t-1} divides $(q-1)/2$. Hence -1 is a $(2t)$-th power modulo q because $2t \leq 2^{t-1}$ when $t \geq 4$.

For part (b), apply part (a) and choose r with $r^{2t} \equiv p \bmod q$. Observe that $2t$ divides 2^t which divides $q-1 = 2kp$. Hence,

$$1 \equiv r^{q-1} \equiv (r^{2t})^{2kp/2t} \equiv p^{kp/t} \bmod q.$$

This completes the proof.

When $t = 2$, the theorem is just Theorem 2.4.

When $t = 4$, Theorem 2.6 says that if $q = (2m)^4 p + 1 = 16m^4 p + 1$ is prime, then q divides $p^{2m^4 p} - 1$. Theorem 2.5 is the case $m = 1$ of this statement.

When $t = 8$, Theorem 2.6 says that if $q = (2m)^8 p + 1 = 256m^8 p + 1$ is prime, then q divides $p^{16m^8 p} - 1$. The first case, $m = 1$, of this statement is for $k = 128$, which is beyond the end of Table 2.

We now apply Theorem 2.6. As above, let g be a primitive root modulo q and let $a = g^{(q-1)t/k} \bmod q$. Then a^j, $0 \leq j < k/t$, are all the solutions to $x^{k/t} \equiv 1 \bmod q$. Let $b = p^p \bmod q$. By the theorem, $b^{k/t} \equiv 1 \bmod q$, so $b \equiv a^j \bmod q$ for some $0 \leq j < k/t$. It is natural to assume that the case $j = 0$, that is, $q \mid N_p$, happens with probability $1/(k/t) = t/k$.

When k is an odd positive integer, define $c(k) = 1/2$. When k is an even positive integer, define $c(k)$ to be the largest power of 2, call it t, for which there exists an integer m so that $k = (2m)^t/2$. Note that $c(k) = 1$ if k is even and not of the form $2m^2$. Also, $c(k) \geq 2$ whenever $k = 2n^2$ because if $k = (2m)^t/2$ with $t \geq 2$, then $k = 2n^2$ with $n = 2^{(t-2)/2} m^{t/2}$. Note that

$$c(k) = \begin{cases} 1/2 & \text{if } k \text{ is odd,} \\ 1 & \text{if } k \text{ is even and not of the form } 2m^2, \\ O(\log k) & \text{if } k = 2m^2 \text{ for some positive integer } m. \end{cases}$$

Hence the average value of $c(k)$ is $3/4$ because the numbers $2m^2$ are rare.

We have given heuristic arguments which conclude that, for fixed k, when p and $q = 2kp+1$ are both prime, the probability that q divides N_p is $c(k)/k$. Empirical evidence in Table 2 supports this conclusion. We have explained all the behavior shown in Table 2. We tested many other values of k and found no further anomalies beyond those listed in this section.

3. Is the conjecture about the period of the Bell numbers true?

We follow, in principle, the heuristic argument on page 386 of [9]. According to the Bateman-Horn conjecture [1], for each positive integer k the number of $p \le x$ for which both p and $2kp+1$ are prime is asymptotically

$$2C_2 f(2k) \frac{x}{(\log x)\log(2kx)},$$

where

$$C_2 = \prod_{q \text{ odd prime}} \left(1-(q-1)^{-2}\right), \qquad f(n) = \prod_{\substack{q|n \\ q \text{ odd prime}}} \frac{q-1}{q-2}.$$

Thus, by the Prime Number Theorem, if p is known to be prime and k is a positive integer, then the probability that $2kp+1$ is prime is $2C_2 f(2k)/\log(2kp)$.

Now we apply the results of the previous section. If p is prime and k is a positive integer, then the probability that $2kp+1$ is prime and divides N_p is $(2C_2 f(2k)/\log(2kp)) \times (c(k)/k)$. For a fixed prime p and real numbers $A < B$, let $F_p(A,B)$ denote the expected number of prime factors of N_p between A and B. Then

$$F_p(A,B) \approx \sum_{\substack{k \\ A<2kp+1\le B}} \frac{2C_2 f(2k)c(k)}{k\log(2kp)}.$$

The anomalous values of $c(k)$ occur when k is twice a square, and these numbers are rare. The denominator $k\log(2kp)$ changes slowly with k. If $B-A$ is large, so that there are many k in the sum, then we may ignore the anomalies and replace $c(k)$ by its average value $3/4$. This change makes little difference in the sum. Thus,

$$F_p(A,B) \approx \sum_{\substack{k \\ A<2kp+1\le B}} \frac{3C_2 f(2k)}{2k\log(2kp)}.$$

Just as in the heuristic argument on page 386 of [9] we may replace $C_2 f(2k)$ by 1 and find

$$F_p(A,B) \approx \sum_{\substack{k \\ A<2kp+1\le B}} \frac{3}{2k\log(2kp)} \approx \frac{3}{2}\log\left(\frac{\log B}{\log A}\right).$$

We can now estimate the expected value of the number d_p of distinct prime factors of N_p. (Question: Is N_p always square free?) The expected value of d_p is

$$F_p\left(2p, N_p\right) \approx \frac{3}{2}\log\left(\frac{\log N_p}{\log(2p)}\right) = \frac{3}{2}\log\left(\frac{\log_p N_p}{\log_p(2p)}\right) \approx \frac{3}{2}\log p.$$

Now we are ready to compute the probability that the conjecture holds for a prime p. If the conjecture fails for p, then there is a prime factor q of N_p such that the period of the Bell numbers modulo p divides $N = N_p/q$. The period will divide N if and only if $B(N+i) \equiv B(i) \bmod p$ for all i in $0 \le i \le p-1$.

Assume that the numbers $B(N+i) \bmod p$ for $0 \le i \le p-1$ are independent random variables uniformly distributed in the interval $[0, p-1]$. Then the probability that the period divides N is p^{-p} because, for each i, there is one chance in p that $B(N+i)$ will have the needed value $B(i) \bmod p$. The probability that the period does not divide N is $1-p^{-p}$.

Assume also that the probabilities that the period divides $N = N_p/q$ for different prime divisors q of N_p are independent. Then the probability that the minimum period is N_p is $(1-p^{-p})^{d_p}$, where d_p is the number of distinct prime factors of N_p. Using our estimate for d_p, we find that this probability is $(1-p^{-p})^{3(\log p)/2}$. When p is large, this number is approximately $1-(3\log p)/(2p^p)$ by the binomial theorem. This shows that the heuristic probability that the minimum period of the Bell numbers modulo p is N_p is exceedingly close to 1 when p is large.

Finally, we compute the expected number of primes $p > x$ for which the conjecture fails. When $x > 2$, this number is

$$\sum_{p>x} \frac{3\log p}{2p^p} < \sum_{p>x} p^{1-x} \leq \int_x^\infty t^{1-x}\,dt = \frac{x^{2-x}}{x-2}.$$

By Theorem 1.1, the conjecture holds for all primes $p < 126$. Taking $x = 126$, the expected number of primes for which the conjecture fails is $< 126^{-124}/124 < 10^{-262}$. Thus, the heuristic argument predicts that the conjecture is almost certainly true.

References

[1] P. T. Bateman and R. A. Horn. A heuristic asymptotic formula concerning the distribution of prime numbers. *Math. Comp.*, 16:363–367, 1962.

[2] C. E. Bickmore. Problem 13058. *Math. Quest. Educ. Times*, 65:78, 1896.

[3] M. Car, L. H. Gallardo, O. Rahavandrainy, and L. N. Vaserstein. About the period of Bell numbers modulo a prime. *Bull. Korean Math. Soc.*, 45(1):143–155, 2008.

[4] L. E. Dickson. *History of the Theory of Numbers, volume 1: Divisibility and Primality.* Chelsea Publishing Company, New York, New York, 1971.

[5] J. Levine and R. E. Dalton. Minimum periods, modulo p, of first-order Bell exponential numbers. *Math. Comp.*, 16:416–423, 1962.

[6] W. F. Lunnon, P. A. B. Pleasants, and N. M. Stephens. Arithmetic properties of Bell numbers to a composite modulus I. *Acta Arith.*, 35:1–16, 1979.

[7] J. Sabia and S. Tesauri. The least prime in certain arithmetic progressions. *Amer. Math. Monthly*, 116:641–643, 2009.

[8] J. Touchard. Propriétés arithmétiques de certains nombres recurrents. *Ann. Soc. Sci. Bruxelles*, 53A:21–31, 1933.

[9] S. S. Wagstaff, Jr. Divisors of Mersenne numbers. *Math. Comp.*, 40:385–397, 1983.

[10] S. S. Wagstaff, Jr. Aurifeuillian factorizations and the period of the Bell numbers modulo a prime. *Math. Comp.*, 65:383–391, 1996.

[11] G. T. Williams. Numbers generated by the function e^{e^x-1}. *Amer. Math. Monthly*, 52:323–327, 1945.

Microsoft Research, One Microsoft Way, Redmond, WA 98052
E-mail address: `pmontgom@cwi.nl`

Department of Mathematics, Purdue University, 150 North University Street, West Lafayette, IN 47907-2067
E-mail address: `snahm@purdue.edu`

Center for Education and Research in Information Assurance and Security, and Departments of Computer Science and Mathematics, Purdue University, 305 North University Street, West Lafayette, IN 47907-2107
E-mail address: `ssw@cerias.purdue.edu`