

AURIFEULLIAN FACTORIZATIONS AND THE PERIOD OF THE BELL NUMBERS MODULO A PRIME

SAMUEL S. WAGSTAFF, JR.

ABSTRACT. We show that the minimum period modulo p of the Bell exponential integers is $(p^p - 1)/(p - 1)$ for all primes $p < 102$ and several larger p . Our proof of this result requires the prime factorization of these periods. For some primes p the factoring is aided by an algebraic formula called an Aurifeullian factorization. We explain how the coefficients of the factors in these formulas may be computed.

1. INTRODUCTION

The first-order Bell exponential integers $B(n)$ may be defined by the generating function

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

These integers appear in many combinatorial problems. For example, $B(n)$ is the number of ways a product of n different primes may be factored. See [6] and its references for more background.

Williams [13] proved that for each prime p the sequence $\{B(n) \bmod p; n = 0, 1, \dots\}$ is periodic and that the minimum period divides

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

He showed that the minimum period is precisely N_p for $p = 2, 3$ and 5 . Levine and Dalton [6] showed 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 . We show that the minimum period is exactly N_p for each prime < 102 and for several larger primes. Our technique is the same one used by Levine and Dalton. We show that the period is not N_p/q for any prime factor q of N_p . We were able to extend their work so far because of great advances in integer factoring methods since 1962.

In the next two sections we describe our attempts to factor N_p for primes $p < 180$. The final section explains how we investigated the period of $\{B(n) \bmod p\}$.

Received by the editor August 24, 1993 and, in revised form, January 26, 1995.

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, Lucas' identities, Aurifeullian 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.

2. FACTORIZATION OF N_p

As we tried to factor N_p for the odd primes $p < 180$, we also tried to factor the important related numbers $K_p = (p^p + 1)/(p + 1)$ for the same primes p . It is well known that all prime factors of N_p and K_p have the form $2kp + 1$, where k is a positive integer. After just a little trial division we used the Elliptic Curve Method [5]. We used the Quadratic Sieve Method [9] to factor the occasional integer of modest size which did not succumb to the Elliptic Curve Method. Before we did any of this work, however, we used the fact that for each odd prime p , one of N_p , K_p admits an algebraic factorization into two nearly equal factors. In fact, if p is squarefree, then the numbers $(p^{hp} - 1)/(p - 1)$ when $p \equiv 1 \pmod{4}$ and $(p^{hp} + 1)/(p + 1)$ when $p \equiv 2$ or $3 \pmod{4}$ have algebraic factorizations for all odd h . Although we describe these factorizations in general in Theorem 2, in this paper we use only the case $h = 1$ and p prime. The algebraic factorizations are called *Aurifeuillian* because some of these formulas were discovered by Aurifeuille (see page 276 of [7]).

The known factors of N_p and K_p are given in Tables 1 and 2. The notations Pxx and Cxx denote prime and composite numbers of xx digits. An L or M following p refers to the Aurifeuillian factor of Theorem 2 below.

Levine and Dalton [6] copied some factors from the table in Cunningham [4] including the erroneous “factor” 6709 of N_{43} , and found more factors by trial division. But they did not use the Aurifeuillian factorizations from [4]. If they had, they could have finished factoring N_{29} and probably also N_{37} .

TABLE 1: Factorization of $N_p = (p^p - 1)/(p - 1)$ for primes $p < 180$

p	Known prime factors of N_p
3	13
5L	11
5M	71
7	29.4733
11	15797.1806113
13L	1803647
13M	53.264031
17L	2699538733
17M	10949.1749233
19	109912203092239643840221
23	461.1289.831603031789.1920647391913
29L	84449.2428577.549334763
29M	59.16763.14111459.58320973
31	568972471024107865287021434301977158534824481
37L	149.41903425553544839998158239
37M	1999.7993.16651.17317.10192715656759
41L	1752341.20567159.1876859311090803007
41M	83.5926187589691497537793497756719
43	173.120401.P62
47	1693.255742492896763511474638530188876017.P39

TABLE 1 (continued)

p	Known prime factors of N_p
53L	107.16505521259654533.143470720478589313288313473
53M	141829.13033960579631324880455449881408994392143
59	709.141579233.P92
61L	977.343625872243632312073.398853286456071792609917995907
61M	1000403244183535565720394723140528028235711874491322863
67	269.4021.730837.10960933. .1514954885096604023562287915730049.P69
71	105649.3388409395214741.17882954877203881.P93
73L	1414741.1295720382587.1192167517020392933.P31
73M	293.439.25239167.56377463.3611379501352361.P32
79	317.1558537597.171355071830508389477. .54493132908043378263202913.P91
83	2657.11155201.1008505707601323349156769489.P120
89L	179.8009862103557709.5964844210432006407836201.P43
89M	37307598912253490893302199133.P58
97L	P95
97M	389.363751.684640163.11943728733741294764390602153.P51
101L	1213.9931988588681.102208068907493.393101595766008847.P53
101M	607.5657.157561.P89
103	1237.16706917226363953216841.C180
107	137122213.10508824813.C197
109L	2617.C107
109M	6196098743139082891438631.P86
113L	3391.8363.785192800256197898644431714786031.P75
113M	227.34314816732569. .70739255769077616674066085318030811655932920203.P53
127	509.22861.1320675600886906675359917.C234
131	1049.1742643541410742623061.C251
137L	54142883557383383180139791.C120
137M	1097.124123.1918644449.12779722229.574894288613. .271329112787027.1759429467460935879916775610180659.P59
139	557.119833345601.C282
149L	1193.C158
149M	51784951.450090559.465814231.C137
151	2417.15101.1234577.C314
157L	1356984109417.C159
157M	86351.P167
163	653.2609.41729.31943437.3727539197017.391683908074297. .8224734227858383253.P294
167	16033.1001953110409.669806250678629514045626189.P326
173L	347.685081.P184
173M	161297590410850151.P176
179	C402

TABLE 2. Factorization of $K_p = (p^p + 1)/(p + 1)$ for primes $p < 180$

p	Known prime factors of K_p
3	7
5	521
7L	113
7M	911
11L	58367
11M	23.89.199
13	13417.20333.79301
17	45957792327018709121
19L	108301.1049219
19M	870542161121
23L	47.139.1013.52626071
23M	1641281.1522029233
29	233.6864997.9487923853.5639663878716545087233
31L	1613.145577.35789156484227
31M	373.62869.2706690202468649
37	593.134135213.4356032201.6190006021.P27
41	18041.20396681.P53
43L	947.6709.1140834804168935454622067377
43M	1291.86689.485926008972226664331036683
47L	65519.10519189757.60963223421.2506611914519
47M	659.15511.21179047.3543413924249049822089893
53	991313.2644277.5324593.14443842647093.19604216783737.P45
59L	27759619.6806872605199.4393717192308664068865841443741
59M	4466419.11821911653180627.114888627555970745944996436263
61	2441.1191941.9229762307875553.560622532089629629. .28523716939675891427869.P42
67L	P60
67M	141907.4002983.5759607944561.P37
71L	4872163.7270495362831024364754355287.P30
71M	17467.59743093.P54
73	4596369165585291112352829637852339157090144708807832677.P80
79L	P74
79M	34919.188021.45780868646549.P51
83L	499.9463.P72
83M	167.997.17929.472168956426245957.860785395874331487431.P32
89	169573582127857.11188457211131513436831539501.P130
97	1553.1631871607681574053.C170
101	10741549365517.266345719946724536329.C167
103L	2267.18541.237313.43577750158649183. .1133217861836283429782583969130809253.P37
103M	1031.692779.36733862315539624797022993014846462017.P57
107L	1061227.46242619.304535269. .3211610951880144183669785219693807857.P49
107M	643.2121939803795871061.2286620265240211377877.P66
109	1236165024989.10341388749337445617033.P186

TABLE 2 (continued)

p	Known prime factors of K_p
113	2713.108637220969.76199628846557168921. $C196$
127 L	921259.1525238541798558622809202213. $P99$
127 M	5932933.26759010325255571935109471. $P101$
131 L	263.8123.23581.128119.509192023.5434194401.118531075451349793. .2274827737024993390020446837627. $P56$
131 M	3407.16003103839.8425818148421874530481343817. .405970466949758035428707456821. $P67$
137	136453.164095915779277. $C272$
139 L	25577. $C144$
139 M	21374190911672122661.1977185134537749396577. $P108$
149	3513009953.4907466108140806981.915115125488764974144697. .2809439870825424714368565313. $C242$
151 L	53593223.20110202953.322631539451020618739. .21410447638232281941934857667. $P97$
151 M	7853. $C160$
157	$P343$
163 L	$P179$
163 M	6521.185821.2272547.21163569551. $C154$
167 L	3760684691.14974117420259. $C162$
167 M	8017.3295913.465247639.4386303138831827. $C151$
173	$C385$
179 L	359.1433.909679.113069992151013739136227. $P166$
179 M	1597039.5864420639771327037769. $C173$

3. AURIFEULLIAN FACTORIZATIONS

For integers $n > 0$ let $\Phi_n(x)$ denote the cyclotomic polynomial

$$\Phi_n(x) = \prod_{\substack{j=1 \\ (j,n)=1}}^n (x - \zeta_n^j),$$

where ζ_n is a primitive n th root of unity. It is well known that $x^n - 1 = \prod_{d|n} \Phi_d(x)$. If p is an odd prime, then $(x^p - 1)/(x - 1) = \Phi_p(x)$ and $(x^p + 1)/(x + 1) = \Phi_{2p}(x)$. Thus $N_p = \Phi_p(p)$ and $K_p = \Phi_{2p}(p)$. Although $\Phi_n(x)$ is irreducible over the integers, it may be reducible over certain quadratic fields. Theorem 1 sets the stage for some factorizations of this type. The first two parts of Theorem 1 were proved by Lucas [8]. Schinzel [11] gave a modern proof of the entire theorem. Our Theorem 1 is the case $m = n$ of Theorem 1 of [11]. Let $(m|n)$ be the Jacobi symbol. For \sqrt{c} we make the convention $\sqrt{c} \geq 0$ if $c \geq 0$ and $\sqrt{c} = i\sqrt{-c}$ if $c < 0$.

Theorem 1. *Let $n > 1$ be a squarefree integer. Then there exist polynomials $P_n(x)$ and $Q_n(x)$ with integer coefficients such that*

$$\Phi_n(x) = P_n^2(x) - (-1|n)nxQ_n^2(x) \quad \text{and} \quad \Phi_{2n}(x) = P_n^2(-x) + (-1|n)nxQ_n^2(-x)$$

when n is odd, and

$$\Phi_{2n}(x) = P_n^2(x) - nxQ_n^2(x)$$

when n is even. These polynomials can be computed from the formulas

$$P_n(x^2) - \sqrt{(-1|n)n}xQ_n(x^2) = \prod_s(x - \zeta_n^s) \prod_t(x + \zeta_n^t),$$

$$P_n(-x^2) - i\sqrt{(-1|n)n}xQ_n(-x^2) = \prod_s(x + i\zeta_n^s) \prod_t(x - i\zeta_n^t),$$

where the products are over $0 < s < n, 0 < t < n, (st, n) = 1, (s|n) = 1, (t|n) = -1$ when n is odd, and from the formula

$$P_n(x^2) - \sqrt{n}xQ_n(x^2) = \prod_s(x - \zeta_{4n}^s),$$

where the product is over $0 < s < 4n, (s, 4n) = 1, (n|s) = 1$ when n is even.

It is easy to modify Theorem 1 to use only real numbers. Theorem 2 does this and also restricts the identities to cases when they produce interesting Aurifeuillian factorizations, that is, when the cyclotomic polynomial is expressed as the difference of two squares. Let $\phi(n)$ denote Euler's totient function.

Theorem 2. *Let $n > 1$ be an odd squarefree integer. Then there exist polynomials $C_n(x)$ and $D_n(x)$ with integer coefficients and degrees $\phi(n)/2$ and $\phi(n)/2 - 1$, respectively, with the following properties. Let h be an odd positive integer. If $n \equiv 1 \pmod{4}$, then*

$$\Phi_n(n^h) = (C_n(n^h) - n^{(h+1)/2}D_n(n^h))(C_n(n^h) + n^{(h+1)/2}D_n(n^h)),$$

and if $n \equiv 3 \pmod{4}$, then

$$(1) \quad \Phi_{2n}(n^h) = (C_n(n^h) - n^{(h+1)/2}D_n(n^h))(C_n(n^h) + n^{(h+1)/2}D_n(n^h)).$$

The coefficients of $C_n(x)$ and $D_n(x)$ may be computed from the identity

$$(2) \quad C_n(x^2) - \sqrt{n}xD_n(x^2) = \prod_{\substack{s=1 \\ (s,n)=1}}^{(n-1)/2} (x^2 - 2(s|n)f_n(s)x + 1),$$

where $f_n(s) = \cos \frac{2\pi s}{n}$ if $n \equiv 1 \pmod{4}$ and $f_n(s) = \sin \frac{2\pi s}{n}$ if $n \equiv 3 \pmod{4}$.

Let n be an even squarefree positive integer. Then there exist polynomials $C_n(x)$ and $D_n(x)$ with integer coefficients and degrees $\phi(n)$ and $\phi(n) - 1$, respectively, so that (1) holds when h is an odd positive integer. The coefficients of $C_n(x)$ and $D_n(x)$ may be computed from the identity

$$C_n(x^2) - \sqrt{n}xD_n(x^2) = \prod_{\substack{s=1 \\ (s,n)=1}}^{2n} (x^2 - (1 + (n|s)) \cos \frac{\pi s}{2n}x + 1).$$

Proof. Let $n \equiv 1 \pmod{4}$. Then $(-1|n) = 1$. By Theorem 1, $\Phi_n(x) = P_n^2(x) - nxQ_n^2(x)$, where

$$P_n(x^2) - \sqrt{n}xQ_n(x^2) = \prod_{\substack{s=1 \\ (s,n)=1}}^{n-1} (x - (s|n)\zeta_n^s).$$

In the product combine the factors with s and $n - s$. Note that $(s, n) = 1$ if and only if $(n - s, n) = 1$. Also $(n - s|n) = (s|n)$ and $\zeta_n^s + \zeta_n^{n-s} = 2 \cos \frac{2\pi s}{n}$. The product of the two factors is $x^2 - 2(s|n)2 \cos \frac{2\pi s}{n}x + 1$. Writing $C_n(x) = P_n(x)$, $D_n(x) = Q_n(x)$ and $x = n^h$ gives the result. There are $\phi(n)/2$ quadratic factors in the product in (2), so the degree of the polynomial in (2) is $\phi(n)$. Since this polynomial is $C_n(x^2) - \sqrt{n}x D_n(x^2)$, the degree of C_n is $\phi(n)/2$ and the degree of D_n is $\phi(n)/2 - 1$.

Now let $n \equiv 3 \pmod{4}$. Then $(-1|n) = -1$. By Theorem 1, $\Phi_{2n}(x) = P_n^2(-x) - nxQ_n^2(-x)$, where

$$P_n(-x^2) - i\sqrt{n}xQ_n(-x^2) = \prod_{\substack{s=1 \\ (s,n)=1}}^{n-1} (x + i(s|n)\zeta_n^s).$$

In the product combine the factors with s and $n - s$. Note that $(s, n) = 1$ if and only if $(n - s, n) = 1$. Also $(n - s|n) = -(s|n)$ and $\zeta_n^s - \zeta_n^{n-s} = 2i \sin \frac{2\pi s}{n}$. The product of the two factors is $x^2 - 2(s|n)2 \sin \frac{2\pi s}{n}x + 1$. Writing $C_n(x) = P_n(-x)$, $D_n(x) = Q_n(-x)$ and $x = n^h$ gives the result.

Now suppose n is even. Then $n \equiv 2 \pmod{4}$ because n is squarefree. By Theorem 1, $\Phi_{2n}(x) = P_n^2(x) - nxQ_n^2(x)$, where

$$P_n(x^2) - \sqrt{n}xQ_n(x^2) = \prod_{\substack{s=1 \\ (s,4n)=1 \\ (n|s)=1}}^{4n} (x - \zeta_{4n}^s).$$

In the product combine the factors with s and $4n - s$. Note that $(s, 4n) = 1$ if and only if $(4n - s, 4n) = 1$. Also $(n|4n - s) = (n|s)$ and $\zeta_{4n}^s + \zeta_{4n}^{4n-s} = 2 \cos \frac{2\pi s}{4n}$. The product of the two factors is $x^2 - (1 + (n|s)) \cos \frac{\pi s}{2n}x + 1$. Since $(n, s) = 1$, the factor $(1 + (n|s))$ is 2 when $(n|s) = 1$ and is 0 when $(n|s) = -1$. Writing $C_n(x) = P_n(x)$, $D_n(x) = Q_n(x)$ and $x = n^h$ gives the result and proves Theorem 2. \square

The two factors of $\Phi_n(n)$ or $\Phi_{2n}(n)$ in Theorem 2 are denoted nL and nM in Tables 1 and 2. A table of coefficients of $C_n(x)$ and $D_n(x)$ for $n < 120$ may be found in Table 34 on page 453 ff. of Riesel [10].

Ordinary 64-bit double-precision floating-point arithmetic permits the correct calculation in a fraction of a second of these coefficients for odd $n < 180$. The program was tested by comparing the product of nL and nM , computed from $C_n(n)$ and $D_n(n)$, with N_n or K_n , computed independently.

Brent [2] gives an algorithm for computing the coefficients of $C_n(x)$ and $D_n(x)$ which uses integer arithmetic throughout.

4. THE PERIOD OF $\{B(n) \pmod{p}\}$

When p is prime, this period is known to be a divisor of N_p . To test whether the period divides some factor N of N_p , it is enough to compare $B(N + i) \pmod{p}$ with $B(i) \pmod{p}$ for $1 \leq i \leq p$. Only these p pairs need to be compared because the congruence

$$(3) \quad B(n + p) \equiv B(n) + B(n + 1) \pmod{p}$$

of Touchard [12] shows that any p consecutive values of $B(n) \pmod{p}$ determine the sequence after that point. For each prime divisor q of N_p listed in Table 1, the

test just described was performed for $N = N_p/q$. When we could not factor N_p completely, we performed the test also for N_p divided by its remaining composite cofactor q (two of them for N_{149}). In every case the outcome of the test was that the period did not divide N_p/q . We also performed the test with $N = N_p$ to check the program. The not unexpected outcome was that N_p is a period. Finally, we tested some N_p with $p > 180$ to see whether the period might be slightly smaller than N_p . Specifically, for each prime p in $180 < p < 1100$ we computed all primes $q < 2^{31}$ dividing N_p and tested N_p/q for being a period. It never was a period. Thus, we have proved the following result.

Theorem 3. *The minimum period of the sequence $\{B(n) \bmod p\}$ is N_p when p is a prime < 102 and also when $p = 113, 163, 167$ or 173 . For the remaining primes $p < 180$, no proper divisor of N_p whose codivisor appears in Table 1 is a period of the sequence. Furthermore, for each prime $p < 1100$, no proper divisor of N_p whose codivisor has only prime factors $< 2^{31}$ is a period of the sequence.*

Based on the evidence provided by Theorem 3, we conjecture that the minimum period of the sequence $\{B(n) \bmod p\}$ is N_p for every prime p .

It remains to explain how we computed $B(N) \bmod p$ when p is a prime < 1100 and N is large; some N have thousands of decimal digits. First of all, we computed $b_i = B(i) \bmod p$ for $0 \leq i \leq p$ using the formula $B(n+1) = \sum_{j=0}^n \binom{n}{j} B(j)$ of Cesaro [3] (see also Becker and Browne [1]). That is, we used this algorithm:

```

b0 = 1;
b1 = 1;
t0 = 1;
for j = 2 to p do
  begin
    tj-1 = bj-1;
    for i = j - 2 down to 0
      ti = (ti + ti+1) mod p;
    bj = t0;
  end

```

This algorithm takes $O(N^2)$ operations to compute $B(N) \bmod p$, so it is too slow to use for large N . To compute $B(N) \bmod p$ for large N we use the congruence $B(n+p^m) \equiv B(n+1) + mB(n) \pmod{p}$ of Touchard [12], which generalizes (3). We write N in radix p as $N = \sum_{i=0}^e a_i p^i$, where $0 \leq a_i < p$ and $a_e \neq 0$. Starting from the block $b_i = B(i) \bmod p$, $0 \leq i \leq p$, we use the digits a_i to compute other blocks of length $p+1$ of values of $B(i) \bmod p$. The algorithm, which runs in $O(p^2 \log N)$ steps, is:

```

for i = 0 to p
  ci = bi;
for i = 1 to e
  if ai > 0 then
    begin
      for j = 1 to ai do
        begin
          for k = 0 to p - 1
            dk = (ck+1 + i * ck) mod p
          dp = (d0 + d1) mod p
          for k = 0 to p
            ck = dk
          end
        end
      end
    end

```

At this point, c_{a_0} is $B(N) \bmod p$. Use (3) to shift the window to $B(N+i) \bmod p$ for $0 \leq i \leq p$. Then compare $B(N+i) \bmod p$ with b_i for $0 \leq i \leq p$ to decide whether N is a period. For every proper divisor N of N_p that we examined, either $B(N) \bmod p \neq b_0$ or $B(N+1) \bmod p \neq b_1$.

ACKNOWLEDGEMENTS

I thank John W. Wrench, Jr. for suggesting this research and R. P. Brent for sending me a preprint of [2]. I am indebted to Harvey Cohn and Hugh Edgar for valuable discussions of this research. I discovered many factors using an ECM program written by P. L. Montgomery. He computed Table 1 independently and sent me several factors which I had missed. I am grateful to Marije Huizing of the Centrum voor Wiskunde en Informatica in Amsterdam for factoring K_{73} by the number field sieve. I thank A. K. Lenstra and B. Dixon for letting me use their ECM program for the MasPar computer. It found several factors.

REFERENCES

1. H. W. Becker and D. H. Browne, *Problem E461 and solution*, Amer. Math. Monthly **48** (1941), 701–703.
2. Richard P. Brent, *On computing factors of cyclotomic polynomials*, Math. Comp. **61** (1993), 131–149. MR **93m**:11131
3. E. Cesaro, *Sur une équation aux différences mêlées*, Nouvelles Annales de Math. (3) **4** (1885), 36–40.
4. A. J. C. Cunningham, *Factorisation of $N = y^y \mp 1$ and $x^{xy} \mp y^{xy}$* , Messenger of Math. (2) **45** (1915), 49–75.
5. H. W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) **126** (1987), 649–673. MR **89g**:11125
6. Jack Levine and R. E. Dalton, *Minimum periods, modulo p , of first-order Bell exponential integers*, Math. Comp. **16** (1962), 416–423. MR **26**:6111
7. E. Lucas, *Théorèmes d'arithmétique*, Atti R. Accad. Sci. Torino **13** (1877–78), 271–284.
8. ———, *Sur la série récurrente de Fermat*, Bull. Bibl. Storia Sc. Mat. e Fis. **11** (1878), 783–789.
9. Carl Pomerance, *The quadratic sieve factoring algorithm*, Advances in Cryptology, Proceedings of EUROCRYPT 84 (T. Beth, N. Cot, and I. Ingemarsson, eds.), Springer-Verlag Lecture Notes in Comput. Sci., vol. 209, 1985, pp. 169–182. MR **86m**:94003
10. Hans Riesel, *Prime numbers and computer methods for factorization*, Birkhäuser, Boston, 1985. MR **88k**:11002
11. A. Schinzel, *On the primitive prime factors of $a^n - b^n$* , Proc. Cambridge Philos. Soc. **58** (1962), 555–562. MR **26**:1280
12. J. Touchard, *Propriétés arithmétiques de certains nombres récurrents*, Ann. Soc. Sci. Bruxelles **53A** (1933), 21–31.
13. G. T. Williams, *Numbers generated by the function e^{e^x-1}* , Amer. Math. Monthly **52** (1945), 323–327. MR **7**:47e

DEPARTMENT OF COMPUTER SCIENCES, PURDUE UNIVERSITY, WEST LAFAYETTE, INDIANA 47907

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