Some Arithmetic Properties of Eulerian Numbers

by Arnold Knopfmacher
Centre for Applicable Analysis and Number Theory
University of the Witwatersrand
Johannesburg, South Africa
e-mail: arnoldk@gauss.cam.wits.ac.za

and Neville Robbins
Mathematics Department
San Francisco State University
San Francisco, CA 94132
e-mail: robbins@math.sfsu.edu

Abstract Eulerian numbers may be defined recursively and have applications to many branches of mathematics. We derive some congruence and divisibility properties of Eulerian numbers.

JCMCC 36 (2001), pp. 31-42

1. Introduction

Consider the triangular array:

1

1 1

1 4 1

1 11 11 1

1 26 66 26 1

1 57 302 302 57 1

1 120 1191 2416 1191 120 1

etc.

The numbers that appear in this array were first discovered by Euler [2] and are known as *Eulerian numbers*. Following Knuth [3], we denote the kth entry in row n by $\left\langle {n \atop k} \right\rangle$, where $1 \leq k \leq n$. The following are two contexts in which Eulerian numbers arise:

(*i*) Let $f(x) = (1 - e^x)^{-1}$. If $n \geq 1$, then

$$f^{(n)}(x) = (1 - e^x)^{-(n+1)} \sum_{k=1}^{n} \left\langle {n \atop k} \right\rangle e^{kx}$$

(*ii*) Let $\sigma \in S_n$, the group of permutations of n distinct objects. Specifically, let $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$. Define a "rise" (also known as a "run" or a "reading") to be a strictly increasing subsequence of $\{\sigma(1), \sigma(2), \sigma(3), \dots, \sigma(n)\}$. Then $\left\langle {n \atop k} \right\rangle$ is the number of such permutations that have exactly k rises , where $1 \leq k \leq n$.

Eulerian numbers are the subject of an extensive literature, and have applications to combinatorics (see [3] and [7]), commutative algebra (see [4]), number theory (see [8]), and statistics (see [5] and [6]). In this note, we prove some congruence and divisibility properties of Eulerian numbers. We also use Eulerian numbers to derive an alternate proof of a known congruence property of Bernoulli numbers. Note that Eulerian numbers should not be confused with *Euler numbers*. (Euler numbers may be defined by:
$E_n = sech^{(n)}(0)$, where $n \geq 0$.)

2. Preliminaries

Notation:

Let B_n denote the nth Bernoulli number, using even subscript notation, that is, $B_n = g^{(n)}(0)$, where $g(x) = \frac{x}{e^x - 1}$, $g(0) = 1$, and $n \geq 0$.

Let T_n denote the nth tangent number, that is, $T_n = tanh^{(n)}(0)$.

Definition 1: if $n \geq 1$ is a natural number and if p is prime, let $n = p^k m$, where $k \geq 0$, $m \geq 1$, and $p \not| m$. Then $o_p(n) = k$.

Identities

(1) $$o_p(ab) = o_p(a) + o_p(b)$$

(2) $$o_p(a/b) = o_p(a) - o_p(b)$$

(3) $$o_p(a^r) = r(o_p(a))$$

(4) If $0 \leq j \leq k$ and $p \not| ab$, then $o_p\left(\binom{p^k a}{p^j b}\right) = o_p\left(\binom{p^{k-j} a}{b}\right)$

(5) (Recursive Property of Eulerian Numbers)

$$\left\langle {n \atop 1} \right\rangle = \left\langle {n \atop n} \right\rangle = 1 \text{ for all } n \geq 1;$$

If $n \geq 3$ and $2 \leq k \leq n-1$, then

$$\left\langle {n \atop k} \right\rangle = k\left\langle {n-1 \atop k} \right\rangle + (n+1-k)\left\langle {n-1 \atop k-1} \right\rangle$$

(6) (Symmetry Property of Eulerian Numbers)

If $1 \leq k \leq n$, then

$$\left\langle {n \atop k} \right\rangle = \left\langle {n \atop n+1-k} \right\rangle$$

(7) $$\sum_{n=1}^{k} \left\langle {n \atop k} \right\rangle = n!$$

(8) $$\left\langle {n \atop k} \right\rangle = \sum_{j=0}^{k-1} (-1)^j (k-j)^n \binom{n+1}{j}$$

(9) $$\sum_{k=1}^{n} (-1)^{k-1} \left\langle {n \atop k} \right\rangle = T_n$$

(10) $$T_{2n-1} = 2^{2n-1}(2^{2n}-1)B_{2n}/n$$

Remarks: (1) through (4) are elementary; (5) may be found in [3]; (6) follows from (5); (7) may be proved by induction, using (5); (8) appears in [1] and [2]; (9) was proved in [9]; (10) appears in [10].

3. The Main Results

Lemma 1: If p is prime, $m \geq 1$, and $1 \leq k \leq p^m - 1$,
then $\binom{p^m}{k} \equiv 0 \pmod{p}$.

Proof: Let $k = p^h c$ where $h \geq 0$, $c \geq 1$, and $p \nmid c$. By hypothesis, $h < m$. Now (4) implies $o_p\left(\binom{p^m}{h}\right) = m - h \geq 1$, from which the conclusion follows. QED

Lemma 2: If p is prime, $m \geq 1$, and $1 \leq k \leq p^m - 1$, then

$$\binom{p^m + 1}{k} \equiv \begin{cases} 1 \pmod{p} \text{ if } k = 0, 1, p^m, p^m + 1 \\ 0 \pmod{p} \text{ if } 2 \leq k \leq p^m - 1 \end{cases}$$

Proof: By the symmetry property of the binomial coefficients, it suffices to consider $0 \leq k \leq [\frac{1}{2}(p^m + 1)]$. Now

$$\binom{p^m + 1}{0} = 1 \equiv 1 \pmod{p} ;$$

$$\binom{p^m + 1}{1} = p^m + 1 \equiv 1 \pmod{p}.$$

If $2 \leq k \leq [\frac{1}{2}(p^m + 1)]$, then

$$\binom{p^m + 1}{k} = \binom{p^m}{k} + \binom{p^m}{k - 1} \equiv 0 + 0 \equiv 0 \pmod{p}$$

by Lemma 1. QED

Theorem 1: If p is prime, $m \geq 1$, and $1 \leq k \leq p^m - 1$, then

$$\left\langle \begin{matrix} p^m - 1 \\ k \end{matrix} \right\rangle \equiv \begin{cases} 1 \pmod{p} \text{ if } p \nmid k \\ 0 \pmod{p} \text{ if } p \mid k \end{cases}$$

Proof: By (8), we have:

$$\left\langle \begin{matrix} p^m - 1 \\ k \end{matrix} \right\rangle = \sum_{j=0}^{k-1} (-1)^j (k-j)^{p^m - 1} \binom{p^m}{j}.$$

Now Lemma 1 implies $\left\langle \begin{matrix} p^m - 1 \\ k \end{matrix} \right\rangle \equiv k^{p^m - 1} \pmod{p}$. If $p \mid k$, then $k \equiv 0 \pmod{p}$, hence $\left\langle \begin{matrix} p^m - 1 \\ k \end{matrix} \right\rangle \equiv 0 \pmod{p}$. If $p \nmid k$, then by Fermat's Little Theorem, we have $\left\langle \begin{matrix} p^m - 1 \\ k \end{matrix} \right\rangle \equiv (k^{p-1})^{\frac{p^m - 1}{p-1}} \equiv 1 \pmod{p}$. QED

Theorem 2: n is prime iff $\left\langle \begin{matrix} n - 1 \\ k \end{matrix} \right\rangle \equiv 1 \pmod{n}$ for all k such that $1 \leq k \leq n - 1$.

Proof: Sufficiency follows from Theorem 1. To prove necessity, suppose that $\left\langle \begin{matrix} n - 1 \\ k \end{matrix} \right\rangle \equiv 1 \pmod{n}$ for all k such that $1 \leq k \leq n - 1$. Then

$$\sum_{k=1}^{n-1} \left\langle \begin{matrix} n - 1 \\ k \end{matrix} \right\rangle \equiv \sum_{k=1}^{n-1} 1 \equiv n - 1 \equiv -1 \pmod{n}.$$

By (7), we have $(n-1)! \equiv -1 \pmod{n}$. The strong form of Wilson's Theorem implies n is prime. QED

Remark: In [8], the second author used Eulerian numbers to provide an alternate proof of Wilson's Theorem.

Theorem 3 If p is prime, $m \geq 1$, and $1 \leq k \leq p^m$, then

$$\left\langle \begin{matrix} p^m \\ k \end{matrix} \right\rangle \equiv 1 \pmod{p}$$

Proof: In view of (5) and (6), it suffices to consider $2 \leq k \leq [\frac{1}{2}p^m]$. By (8), we have

$$\left\langle \begin{matrix} p^m \\ k \end{matrix} \right\rangle = \sum_{j=0}^{k-1} (-1)^j (k-j)^n \binom{p^m+1}{j}.$$

Now Lemma 2 implies $\left\langle \begin{matrix} p^m \\ k \end{matrix} \right\rangle \equiv k^{p^m} - (k-1)^{p^m} \equiv 1^{p^m} \equiv 1 \pmod{p}$. QED

Lemma 3: Let $n = p^k m$ where p is prime, $k \geq 1$, $m \geq 1$, and $p \nmid m$. Then $k < n$.

Proof: By hypothesis, $p^k \leq n$, so $k \leq \frac{\log n}{\log p} < n$. QED

Theorem 4: n is prime iff $\left\langle \begin{matrix} n \\ k \end{matrix} \right\rangle \equiv 1 \pmod{n}$ for all k such that $1 \leq k \leq n$.

Proof: Sufficiency follows from Theorem 3, taking $m = 1$. To prove necessity, it suffices, in view of (5), to consider $n \geq 3$, $2 \leq k \leq n-1$. Suppose that n is composite and that p is the least prime factor of n. We will show that $\left\langle \begin{matrix} n \\ p+1 \end{matrix} \right\rangle \not\equiv 1 \pmod{n}$.

Let $n = p^k m$ where p is prime, $k \geq 1$, $m \geq 1$, and $p \nmid m$. By (8), we have

$$\left\langle \begin{matrix} n \\ p+1 \end{matrix} \right\rangle = (p+1)^n - (n+1)p^n + \binom{n+1}{2}(p-1)^n + \ldots$$

$$+(-1)^{p-1}\binom{n+1}{p-1}2^n + (-1)^p \binom{n+1}{p}$$

Therefore $\left\langle \begin{matrix} n \\ p+1 \end{matrix} \right\rangle \equiv (p+1)^n - p^n + (-1)^p \binom{n+1}{p} \pmod{n}$, so that

$$\left\langle \begin{matrix} n \\ p+1 \end{matrix} \right\rangle \equiv (p+1)^n - p^n + (-1)^p \binom{n+1}{p} \bmod (p^k)$$

This yields

$$\left\langle \begin{matrix} n \\ p+1 \end{matrix} \right\rangle \equiv \sum_{j=0}^{n-1} \binom{n}{j} p^j + (-1)^p \binom{n+1}{p} \pmod{p^k}$$

By Lemma 3 and hypothesis, we have $k \leq n-1$, so that

$$\langle \begin{matrix} n \\ p+1 \end{matrix} \rangle \equiv \sum_{j=0}^{k} \binom{n}{j} p^j + (-1)^p \binom{n+1}{p} \pmod{p^k}$$

Now (4) implies that $o_p(\binom{n}{j}) = o_p(\binom{p^k m}{j} = k - o_p(j)$. If $j > 0$, then Lemma 3 implies $o_p(j) < j$, so $o_p(\binom{n}{j} > k - j$. Then (1) implies $o_p(\binom{n}{j} p^j) > k$. Therefore we have $\langle \begin{matrix} n+1 \\ p \end{matrix} \rangle \equiv (-1)^p \binom{n+1}{p} \pmod{p^k}$. Now $\binom{n+1}{p} = (n+1)n(n-1)(n-2)\cdots(n-2+p)/p!$, so that $o_p(\binom{n+1}{p}) = o_p(n) - 1 = k - 1$. This implies that $\binom{n+1}{p} \not\equiv 0 \bmod(p^k)$, hence $\langle \begin{matrix} n \\ p+1 \end{matrix} \rangle \not\equiv 1 \pmod{p^k}$, and $\langle \begin{matrix} n \\ p+1 \end{matrix} \rangle \not\equiv 1 \pmod{n}$, so we are done. QED

Remark: As we have seen in the proof of Theorem 4, if n is composite and if p is the least prime factor of n (so that $p \leq [n^{\frac{1}{2}}]$), then $\langle \begin{matrix} n \\ p+1 \end{matrix} \rangle \not\equiv 1 \pmod{n}$. This suggests the following algorithm: Compute $\langle \begin{matrix} n \\ k \end{matrix} \rangle$ for all k such that $2 \leq k \leq [n^{\frac{1}{2}}]$. If $\langle \begin{matrix} n \\ k \end{matrix} \rangle \equiv 1 \pmod{n}$ for all such k, then n is prime; otherwise n is composite. Note that $[n^{\frac{1}{2}}] - 1$ computations would be required to verify that n is prime. Thus our algorithm provides an inefficient method to verify primality. On the other hand, if n is composite, then it may well be that $\langle \begin{matrix} n \\ k \end{matrix} \rangle \not\equiv 1 \pmod{n}$ for some $k < p+1$, where p is the least prime factor of n. Still, our algorithm would not be an efficient way to verify that n is composite, for reasons that we will demonstrate below.

Theorem 5: Suppose that n is composite and that $(n, j) = 1$ for all $j \leq k-1$. Then $\langle {n \atop j} \rangle \equiv 1 \pmod{n}$ for all $j \leq k$ iff n is a pseudoprime to base j for all j such that $2 \leq j \leq k$.

Proof: (8) implies

$$\langle {n \atop j} \rangle = j^n + (n+1)(j-1) + \sum_{i=2}^{j-1} (-1)^i \binom{n+1}{i} (j-i)^n$$

Since $(n, j) = 1$ for all$j \leq k-1$ by hypothesis, we have $\binom{n+1}{i} \equiv 0 \pmod{n}$ for $2 \leq i \leq j-1$, hence $\langle {n \atop j} \rangle \equiv j^n - (j-1)^n \pmod{n}$ for $1 \leq j \leq k$. If n is a pseudoprime to base j for all j such that $2 \leq j \leq k$, then $\langle {n \atop j} \rangle \equiv j - (j-1) \equiv 1 \pmod{n}$ for $2 \leq j \leq k$. Since $\langle {n \atop 1} \rangle = 1$, we have $\langle {n \atop j} \rangle \equiv 1 \pmod{n}$ for $1 \leq j \leq k$. Conversely, if $\langle {n \atop j} \rangle \equiv 1 \pmod{n}$ for all $j \leq k$, then $j^n - (j-1)^n \equiv 1 \pmod{n}$ for all $j \leq k$. It is easily seen by induction on j that $j^n \equiv j \pmod{n}$, that is, n is a pseudoprime to the base j, for all $j \leq k$. QED

Remark: Suppose that n is a Carmichael number, that is, n is composite, yet $b^n \equiv b \pmod{n}$ for all b such that $(b, n) = 1$. Let p be the least prime factor of n. Since n has at least three distinct prime factors, we must have $p \leq [n^{\frac{1}{3}}]$. By Theorem 5, we have $\langle {n \atop k} \rangle \equiv 1 \pmod{n}$ for $1 \leq k \leq p-1$. Thus our algorithm could require as many as $1 + [n^{\frac{1}{3}}]$ iterations to verify that n is composite. This would not be computationally feasible.

Theorem 6: If p is prime, $m \geq 1$, and $2 \leq k \leq p^m$, then $\langle {p^m + 1 \atop k} \rangle \equiv 2 \pmod{p}$.

Proof: By (5), we have $\langle {p^m + 1 \atop k} \rangle = (p^m + 1)\langle {p^m \atop k-1} \rangle + k\langle {p^m \atop k} \rangle$. Theorem 3 implies $\langle {p^m + 1 \atop k} \rangle = (p^m + 2 - k)1 + k(1) \equiv 2 \pmod{n}$ QED

We now turn our attention to the divisibility properties of the Eulerian numbers $\langle {n \atop 2} \rangle$.

Theorem 7: If $m \geq 2$, then $\langle {2^m - 1 \atop 2} \rangle = 2^m(2^{\langle {m \atop 2} \rangle} - 1)$.

Proof: By (8), we have $\langle {n \atop 2} \rangle = 2^n - (n+1)$. Thus

$$\langle {2^m - 1 \atop 2} \rangle = 2^{2^m - 1} - 2^m = 2^m(2^{2^m - (m+1)} - 1) = 2^m(2^{\langle {m \atop 2} \rangle} - 1)$$

QED

Corollary 1: $2^m | \langle {2^m - 1 \atop 2} \rangle$

Proof: This follows directly from Theorem 7. QED

Theorem 8: For each prime, p, and for each $k \geq 1$, there exist infinitely many n such that $p^k | \langle {n \atop 2} \rangle$.

Proof: In view of Corollary 1, we may assume that p is odd. First note that $2^j = j + 1$ iff $j = 0$ or 1. Let 2 have order d (mod p^k), where $d | \phi(p^k)$. Let $m = [d, p^k]$. Let $n = j + tm$, where $j = 0$ or 1 and t is an arbitrary natural number. Then $2^n = 2^{j+tm} = 2^j 2^{tm} = 2^j(2^d)^{tm/d}$, so that $2^n \equiv 2^j \bmod(p^k)$, and also $n \equiv j \pmod{p^k}$. Now $\langle {n \atop 2} \rangle = 2^n - (n+1) \equiv 2^j - (j+1) \equiv 0 \bmod(p^k)$, that is, $p^k | \langle {n \atop 2} \rangle$. QED

Remark: If p is a given prime, let n be the least positive integer such that $p | \langle {n \atop 2} \rangle$. By Theorem 8, n exists, and $n \leq [d, p]$, where 2 has order d (mod p). It may well occur that $n < dp$. For example, if $p = 5$, then $d = 4$, but $n = 7$.

Theorem 9: Let p_1, p_2 be distinct primes. Let $k_1 \geq 1, k_2 \geq 1$. Let $h_1 = p_1^{k_1}$, $h_2 = p_2^{k_2}$. Let 2 have order d_1 (mod h_1). Let 2 have order d_2 (mod h_2). Let $n_1 = [d_1, h_1]$, $n_2 = [d_2, h_2]$. then $h_1 h_2 | \binom{[n_1, n_2]}{2}$.

Proof: We wish to show that $2^{[n_1,n_2]} \equiv 1 + [n_1, n_2]$ (mod $h_1 h_2$) . Since $(h_1, h_2) = 1$ by hypothesis, it suffices to show that $2^{[n_1,n_2]} \equiv 1 + [n_1, n_2]$ mod(h_i) for $i = 1, 2$. Since $h_i | n_i$, we have $h_i | [n_1, n_2]$, so $[n_1, n_2] \equiv 0$ (mod h_i) . Furthermore, $d_i | n_i$, so $d_i | [n_1, n_2]$. Therefore we have
$2^{[n_1,n_2]} \equiv 1 \equiv 1 + [n_1, n_2]$ (mod h_i) . QED

Theorem 10: If h is an odd positive integer, then there exists n such that $h | \binom{n}{2}$.

Proof: Without loss of generality, let $h > 1$. Then $h = \prod_{i=1}^{r} h_i$, where each $h_i = p_i^{e_i}$, the p_i are distinct primes, and each $e_i \geq 1$. The case $r = 1$ follows from Theorem 8. The case $r = 2$ follows from Theorem 9. If $r \geq 3$, we complete the proof using induction on r. Specifically, for each index, i, let 2 have order d_i (mod h_i) and let $n_i = [d_i, h_i]$, so that $h_i | \binom{n_i}{2}$. If $n = [n_1, n_2, \ldots, n_r]$, then $h | \binom{n}{2}$. QED

We conclude by using Eulerian numbers to derive an alternate proof of a known result regarding Bernoulli numbers. Note that (9) is a relation between Eulerian and tangent numbers, while (10) is a relation between tangent and Bernoulli numbers. Using (9) and (10) and Theorem 3, we obtain:

Theorem 11: Let $B_n = N_n / D_n$. Let p denote an odd prime. Then $12 N_{p+1} \equiv D_{p+1}$ (mod p) .

Proof: By (9), Theorem 3, and hypothesis, we have $T_p \equiv 1$ (mod p) . Now (10) implies $T_p = 2^p (2^{p+1} - 1) B_{p+1} / (\frac{1}{2}(p+1))$. This yields:
$2^{p+1}(2^{p+1} - 1) B_{p+1} \equiv p + 1$ (mod p) . Applying Fermat's Little Theorem, we get $12 B_{p+1} \equiv 1$ (mod p) . from which the conclusion follows. QED

4. References

1. **L. Carlitz**, Note on a paper of Shanks, Amer. Math. Monthly 59 (1952) 239-241

2. **L. Euler**, Institutiones Calculi Differentialis, (St. Petersburg, 1755); Opera Omnia (1) 10 (1913) 373-375

3. **D. E. Knuth**, The Art of Computer Programming, vol. III (1973) 34-41

4. **J.-L. Loday**, Operations sur l'homologie cyclique des algebres commutatives, Inventiones Math. 96 (1989) 205-230

5. **H. B. Mann**, On a test for randomness based on signs of differences, Annals Math. Stat. 16 (1945) 193-199

6. **G. H. Moore & W. A. Wallis**, Time series significance tests based on signs of differences, J. Amer. Stat. Assn. 38 (1943) 153-165

7. **J. Riordan**, An Introduction to Combinatorial analysis (1958) Princeton University Press, 213-216

8. **N. Robbins**, Wilson's Theorem via Eulerian Numbers, Fibonacci Quart. 36 (1998) 317-318

9. **L. Toscano**, Sui coefficienti della tangente e sui numeri di Bernoulii, Boll. Un. Mat. Ital. 15 (1936) 8-12

10. **J. V. Uspensky & M. A. Heaslet**, Elementary Number Theory (1939) McGraw-Hill