WILSON'S THEOREM VIA EULERIAN NUMBERS

Neville Robbins
Mathematics Department, San Francisco State University, San Francisco, CA 94132
(Submitted October 1996-Final Revision May 1997)

INTRODUCTION

In 1770, Edward Waring, in a work entitled "Meditationes Algebraicae," announced without proof the following result, which he attributed to his student, John Wilson:

$$\text{If } p \text{ is prime, then } (p-1)! \equiv -1 \pmod{p}.$$

This statement, now known as Wilson's Theorem, was first proved by Lagrange in 1771, and may have been known earlier by Leibniz.

In this note, we present a new proof of Wilson's Theorem, based on properties of Eulerian numbers, which are defined below. Consider the following triangular array, which is somewhat reminiscent of Pascal's triangle.

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 4 & & 1 & & & \\
 & & 1 & & 11 & & 11 & & 1 & & \\
 & 1 & & 26 & & 66 & & 26 & & 1 & \\
1 & & 57 & & 302 & & 302 & & 57 & & 1 \\
 & & & & & \vdots & & & & &
\end{array}$$

The numbers that appear in this array were first discovered by Euler [1] and are known as *Eulerian numbers*. Following Knuth [2], we denote the k^{th} entry in row n by $\langle {n \atop k} \rangle$, where $1 \le k \le n$.

Eulerian numbers may be defined recursively via:

$$\left\langle {n \atop 1} \right\rangle = \left\langle {n \atop n} \right\rangle = 1; \quad \left\langle {n \atop k} \right\rangle = k\left\langle {n-1 \atop k} \right\rangle + (n+1-k)\left\langle {n-1 \atop k-1} \right\rangle \quad \text{if } 2 \le k \le n-1. \tag{1}$$

(See [2], p. 35, eq. (2).)

They enjoy a symmetry property:

$$\left\langle {n \atop k} \right\rangle = \left\langle {n \atop n+1-k} \right\rangle \text{ for all } k \text{ such that } 1 \le k \le n. \tag{2}$$

Adding all the Eulerian numbers in a given row, we get

$$\sum_{k=1}^{n} \left\langle {n \atop k} \right\rangle = n! \tag{3}$$

Furthermore,

$$\left\langle {n \atop k} \right\rangle = \sum_{j=0}^{k} (-1)^j (k-j)^n \binom{n+1}{j}. \tag{4}$$

Remarks: (2) follows easily from (1), (3) follows from (1), using induction on n, and (4) is equation (13) on page 37 in [2].

We will also need

Definition 1: If m and n are integers larger than 1 and k is a nonnegative integer, we say that $O_n(m) = k$ if $n^k \mid m$ but $n^{k+1} \nmid m$.

$$\text{If } p \text{ is prime, } p \nmid a,\ j \le m, \text{ and } 0 < a < p^{m-j}, \text{ then } O_p\left(\binom{p^m}{ap^j}\right) = m - j. \tag{5}$$

Remark: (5) is Theorem 4 in [3].

THE MAIN RESULTS

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

Proof: This follows from the hypothesis and (5).

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

$$\left\langle {p^m - 1 \atop k} \right\rangle \equiv \begin{cases} 0 \pmod p & \text{if } k \equiv 0 \pmod p, \\ 1 \pmod p & \text{if } k \not\equiv 0 \pmod p. \end{cases}$$

Proof: (4) implies

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

Now Lemma 1 implies

$$\left\langle {p^m - 1 \atop k} \right\rangle \equiv k^{p^m - 1} \pmod p.$$

If $k \equiv 0 \pmod p$, then

$$\left\langle {p^m - 1 \atop k} \right\rangle \equiv 0^{p^m - 1} \equiv 0 \pmod p.$$

If $k \not\equiv 0 \pmod p$, then, by Fermat's Little Theorem,

$$\left\langle {p^m - 1 \atop k} \right\rangle \equiv (k^{p-1})^{\left(\frac{p^m - 1}{p-1}\right)} \equiv 1^{\left(\frac{p^m - 1}{p-1}\right)} \equiv 1 \pmod p.$$

Theorem 2 (Wilson's Theorem): If p is prime, then $(p-1)! \equiv -1 \pmod p$.

Proof: (3) implies $(p-1)! = \sum_{k=1}^{p-1} \left\langle {p-1 \atop k} \right\rangle$. Theorem 1 implies $\left\langle {p-1 \atop k} \right\rangle \equiv 1 \pmod p$ for $1 \le k \le p-1$. Therefore, $(p-1)! \equiv \sum_{k=1}^{p-1} 1 \equiv p - 1 \equiv -1 \pmod p$.

REFERENCES

1. L. Euler. *Opera Omnia* (1) **10** (1913):373-75.
2. D. E. Knuth. *The Art of Computer Programming*. Vol. 3. New York: Addison-Wesley, 1973.
3. N. Robbins. "On the Number of Binomial Coefficients Which Are Divisible by Their Row Number." *Canad. Math. Bull.* **25.30** (1982):363-65.

AMS Classification Number: 11A99