

Elementary proof of W. Schulte’s conjecture

Djamel Himane 

LA3C Laboratory, Faculty of Mathematics, USTHB

P. O. Box 32, El Alia, 16111, Bab Ezzouar, Algiers, Algeria

e-mails: dhimane@usthb.dz, djamel17himane@gmail.com

Received: 14 November 2024

Accepted: 8 May 2025

Online First: 9 May 2025

Abstract: In the On-Line Encyclopedia of Integer Sequences, we find the sequence 1, 1, 3, 18, 180, 2700, 56700, 1587600, 57153600, \dots , which is given by the formula $A_n = n!(n-1)!/2^{n-1}$. On the same page, Werner Schulte conjectured that for all $n > 1$, n divides $2A_{n-1} + 4$ if and only if n is prime. In this paper, we employ elementary methods to provide a simple proof of this conjecture.

Keywords: Legendre’s formula, Wilson’s theorem, Fermat’s Little Theorem.

2020 Mathematics Subject Classification: 11A41, 11A51.

1 Introduction and statement of results

Consider the sequence defined by the relation:

$$A_n = 1 \cdot (1 + 2) \cdot (1 + 2 + 3) \cdots (1 + 2 + \cdots + (n - 1)).$$

We pose the question: *Does this sequence of positive integers hold any particular significance?*

In the course of analyzing this sequence, we consider the triangular number:

$$T_s = 1 + 2 + \cdots + s = \frac{s(s+1)}{2}.$$

Using this formula, we can express the sequence A_n as follows:



$$A_n = \prod_{j=1}^{n-1} T_j = \prod_{j=1}^{n-1} \frac{j(j+1)}{2} = \frac{(n-1)! \cdot n!}{2^{n-1}}. \quad (1)$$

The first terms of this sequence are 1, 1, 3, 18, 180, 2700, 56700, ... (sequence A006472 in the OEIS, also listed as sequence M3052 in [5]).

In the OEIS database entry A006472, we encountered a conjecture attributed to W. Schulte regarding this sequence, for which we will provide an elementary proof.

The main result we aim to prove is the following:

Theorem 1.1 (W. Schulte's Conjecture). *For any positive integer $n > 1$, n divides*

$$\frac{(n-2)!(n-1)!}{2^{n-3}} + 4. \quad (2)$$

if and only if n is a prime number.

2 Preliminaries

For any prime p and any non-negative integer n , we define $v_p(n)$ as the exponent of the largest power of p that divides n (i.e., the p -adic valuation of n). We can express this using the following formula:

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor, \quad (3)$$

where $\lfloor x \rfloor$ denotes the floor function of x .

Legendre's formula (3) provides an expression for the largest power of a prime p that divides the factorial $n!$ [2]. Although this formula is an infinite sum, for each pair of values n and p , only a few terms are non-zero: for each i such that $p^i > n$, we have $\left\lfloor \frac{n}{p^i} \right\rfloor = 0$.

We also have the following recurrence relation:

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + v_p\left(\left\lfloor \frac{n}{p} \right\rfloor!\right). \quad (4)$$

Legendre's formula can also be rewritten in terms of the base- p expansion of n . If $s_p(n)$ denotes the sum of the digits in the base- p representation of n , then we have:

$$v_p(n!) = \frac{n - s_p(n)}{p - 1}. \quad (5)$$

It is easy to verify the following relations: For any positive integers a, b and any prime p [1]:

1. $v_p(a \times b) = v_p(a) + v_p(b)$.
2. $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$.
3. If $a \mid b$, then $v_p(a) \leq v_p(b)$, with $v_p(a) < a$.

The proof of the following lemma is well-known and straightforward, but we include it here for completeness.

Lemma 2.1. *For any positive integer $m > 4$, we have $m < 2^{m/2}$.*

Proof. We prove this inequality by induction. Note that in the induction step, the left-hand side grows additively, whereas the right side grows multiplicatively. In particular, we have:

$$m < 2^{m/2},$$

which is equivalent to

$$m \left(\frac{m+1}{m} \right) < 2^{m/2} \left(\frac{m+1}{m} \right).$$

Simplifying, we obtain:

$$m+1 < 2^{m/2} \left(\frac{m+1}{m} \right). \quad (6)$$

We define the following auxiliary function:

$$g(t) = \sqrt{2} - \frac{t+1}{t} = (\sqrt{2} - 1) - \frac{1}{t}.$$

Evaluating, we find $g(5) = (\sqrt{2} - 1) - \frac{1}{5} \approx 0.2142$. Moreover, since $g'(t) = \frac{1}{t^2} > 0$, we see that $g(t)$ is a strictly increasing function for $t \geq 5$. Thus, for $t \geq 5$, we have

$$\sqrt{2} - \frac{t+1}{t} > 0 \quad \Rightarrow \quad \sqrt{2} > \frac{t+1}{t}.$$

This implies that, for $m \geq 5$,

$$\frac{m+1}{m} < 2^{1/2} \quad \Rightarrow \quad 2^{m/2} \left(\frac{m+1}{m} \right) < 2^{(m+1)/2}.$$

Using this relation in (6), we obtain:

$$m+1 < 2^{(m+1)/2},$$

which completes the induction step. Therefore, for $m > 4$, it follows that

$$m < 2^{m/2}. \quad \square$$

Lemma 2.2. *If p is prime, then $(p-1)! + 1$ is divisible by p .*

This theorem was proposed by Alhazen (c. 965–1000 AD) and, in the 18-th century, by J. Wilson. Lagrange provided the first proof in 1771. A primality test [3] directly follows from Wilson's theorem: a positive integer $n > 1$ is prime if and only if

$$(n-1)! + 1 \equiv 0 \pmod{n}. \quad (7)$$

Lemma 2.3. *For any positive integer a that is not divisible by a prime p , we have*

$$a^{p-1} \equiv 1 \pmod{p}. \quad (8)$$

This fundamental result in number theory is known as Fermat's Little Theorem. First stated by Pierre de Fermat in 1640, this theorem forms the basis for Fermat's primality test (p. 22, [3]).

3 Proof of the main theorem

Proof. Let n be a positive integer greater than 1. We will prove that n divides

$$\frac{(n-2)!(n-1)!}{2^{n-3}} + 4$$

if and only if n is a prime number. The proof is divided into two parts:

- First part: Assume that n is a prime number. Let $n = p$, where p is an odd prime. By Wilson's theorem (Lemma 2.2), we know that p divides both $(p-1)! + 1$ and $(p-2)! - 1$. Moreover, by Fermat's Little Theorem (Lemma 2.3), we deduce that p divides $2^{p-1} - 1$. Using the relation (1), we obtain:

$$2 \times A_{p-1} \equiv -4 \pmod{p}.$$

Therefore, p divides

$$\frac{(p-2)!(p-1)!}{2^{p-3}} + 4.$$

For $n = 2$, the property holds directly.

- Second part: Now assume that n is a composite number. Let $n = pq$, where $1 < p \leq q < n$. We consider three cases:

- Case 1: If $n = 4$, we have

$$\frac{(n-2)!(n-1)!}{2^{n-3}} + 4 = 10,$$

which is not divisible by 4.

- Case 2: If n is odd and $n > 4$, then $n \mid (n-2)!(n-1)!$ and $\gcd(n, 2^{n-3}) = 1$. We deduce that:

$$n \mid \frac{(n-2)!(n-1)!}{2^{n-3}},$$

which implies that:

$$\frac{(n-2)!(n-1)!}{2^{n-3}} + 4 \equiv 4 \pmod{n}.$$

This means that the expression is not divisible by n .

- Case 3: If n is even, let $n = 2^{v_2(n)} \times k > 4$, where k is odd. We have that $n \mid (n-2)!(n-1)!$. By Euclid's lemma, we know that $k \mid 2 \times A_{n-1}$, which implies that $n \mid 2 \times A_{n-1}$ if and only if

$$v_2(n) \leq v_2(2 \times A_{n-1}).$$

Using properties of the p -adic valuation, we obtain:

$$v_2(2 \times A_{n-1}) = v_2((n-1)!) + v_2((n-2)!) - v_2(2^{n-3}).$$

We use the recurrence relation:

$$v_2((n-1)!) = v_2(n-1) + v_2((n-2)!) = v_2((n-2)!),$$

since $n-1$ is odd, and thus

$$v_2((n-2)!) = \left\lfloor \frac{n-2}{2} \right\rfloor + \left\lfloor \frac{n-2}{4} \right\rfloor + v_2\left(\left\lfloor \frac{n-2}{4} \right\rfloor!\right) \geq \frac{n-2}{2} + \frac{n-2}{4}.$$

Therefore,

$$v_2(2 \times A_{n-1}) \geq \left(\frac{n-2}{2} + \frac{n-2}{4} \right) + \left(\frac{n-2}{2} + \frac{n-2}{4} \right) - (n-3).$$

Simplifying, we find that

$$v_2(2 \times A_{n-1}) \geq \frac{n}{2}.$$

By Lemma 2.1, this implies that

$$\frac{n}{2} > v_2(n).$$

Thus,

$$v_2(2 \times A_{n-1}) \geq v_2(n),$$

which implies that

$$\frac{(n-2)!(n-1)!}{2^{n-3}} + 4 \equiv 4 \pmod{n}.$$

In conclusion,

$$\frac{(n-2)!(n-1)!}{2^{n-3}} + 4$$

is not divisible by n .

Thus, the proof is complete. □

Acknowledgements

I would like to express my sincere appreciation to Professor Boumahdi Rachid at NHSM, who generously offered his advice and guidance. I would also like to extend my deepest gratitude to the reviewers for their voluntary efforts in supporting research and the scientific community.

References

- [1] Cassels, J. W. S., & Fröhlich, A. (1967). *Algebraic Number Theory*. Academic Press, p. 9.
- [2] Legendre, A. M. (1830). *Théorie des Nombres*. Paris, p. 10.
- [3] Ribenboim, P. (1996). *The New Book of Prime Number Records*. Springer Verlag.
- [4] Sloane, N. J. A. A006472 $a(n) = n! \times (n-1)!/2^{(n-1)}$. (Formerly M3052). *The On-Line Encyclopedia of Integer Sequences*. Available online at: <https://oeis.org/A006472>.
- [5] Sloane, N. J. A., & Plouffe, S. (1995). *The Encyclopedia of Integer Sequences*. Academic Press, p. 319.