http://math-sci.ui.ac.ir

Journal of Mathematics and Society
ISSN (print): 2345-6493, ISSN (on-line): 2345-6507
Vol. 10 No. 4 (2025), pp. 105–131.

http://www.ui.ac.ir

NEW RESULTS ON WOLSTENHOLMES THEOREM AND ITS APPLICATIONS

DANIEL YAQUBI* AND MADJID MIRZAVAZIRI

ABSTRACT. In 1862, Wolstenholme proved that for primes $p \geq 5$, $\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$. This theorem is equivalent to the divisibility of the coefficients of the harmonic series

$$1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$$

by p^2. The far-reaching implications of Wolstenholme's theorem ignited the curiosity of mathematicians in the 19th century, leading to a surge of investigations into the divisibility properties of coefficients in rational fractions and binomial coefficients involving powers of primes. The emergence of Bernoulli numbers in this theorem and their intricate connection to binomial coefficients firmly established the roots of this mathematical domain in analytic number theory. In this paper, we embark on a journey to explore Wolstenholme's theorem for higher powers of primes and delve into the intricacies of these diverse proofs. The converse of Wolstenholme's theorem, first proposed by Jones, asserts that a natural number n satisfying the congruence $\binom{2n-1}{n-1} \equiv 1 \pmod{p^3}$ must be prime. We conclude our exploration by examining the conditions of the converse of Wolstenholme's theorem and presenting several intriguing problems that beckon further investigation.

1. Introduction

Number theory is one of the oldest branches of mathematics. The earliest records of number theory can be traced back to the Babylonians in the mid-third millennium BC, where lists of Pythagorean triples have been found. This branch of mathematics is dedicated to the study of the properties of

Keywords: Wolstenholme's theorem, Harmonic numbers, Euler's theorem, Bernoulli numbers, Binomial coefficient.

Article Type: Review Paper.

Communicated by Javad Asadollah.

Received: 10-06-2024, Accepted: 27-01-2025, Published Online: 29-06-2025.

Cite this article: D. Yaqubi and M. Mirzavaziri,New results on Wolstenholmes theorem and its applications, *Journal of Mathematics and Society*, **10** no. 4 (2025) 105–131. http://dx.doi.org/10.22108/msci.2025.141789.1669 .

numbers. One of the most significant concepts in number theory is the divisibility of binomial coefficients, a subject that has fascinated many renowned mathematicians, including *Joseph Wolstenholme*, born in Eccles, England in 1829. Wolstenholme is known for the following theorem:

Theorem 1.1 (Wolstenholme's Theorem)**.** *Let $p \geq 5$ be a prime number. The numerator of the harmonic sum*

$$1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$$

is divisible by p^2.

Since the 19th century, eminent mathematicians such as *Babbage, Cauchy, Cayley, Gauss, Kummer, and Lucas* have extensively studied the divisibility properties of coefficients of rational fractions and binomial coefficients to powers of primes. The primary focus of this paper is to present and prove Wolstenholme's theorem and its generalizations. The second section introduces the necessary definitions and preliminaries. We will prove the Wolstenholme's theorem is equivalence with the congruence $\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$. It is straightforward to show that the congruence $\binom{2p-1}{p-1} \equiv 1 \pmod{p}$ holds for all primes p. In 1819, Babbage proved the congruence $\binom{2p-1}{p-1} \equiv 1 \pmod{p^2}$ for all $p \geq 2$ [2].

Section three delves into the generalization of Wolstenholme's theorem to higher powers of the prime p. In the fourth section, we explore the converse of Wolstenholme's theorem and investigate specific cases.

Finally, we conclude by presenting several conjectures and open problems that arise from our investigation.

2. Main Results

Definition 2.1. *Let p be a prime number. For any positive integer $1 \leq n \leq p-1$, we define the generalized harmonic number $H_n(p-1)$ and the generalized Riemann zeta function $R_n(p-1)$ as follows:*

$$R_n(p-1) = \sum_{k=1}^{p-1} \frac{1}{k^n} \qquad \text{and} \qquad H_n(p-1) = \sum_{1 \leq i_1 < i_2 < \cdots < i_n \leq p-1} \frac{1}{i_1 i_2 \cdots i_n}.$$

Theorem 2.2 (Wolstenholme's Theorem)**.** *Let $p \geq 5$ be a prime number. The numerator of the harmonic sum*

$$1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$$

is divisible by p^2.

Proof.

http://dx.doi.org/10.22108/msci.2025.141789.1669

First proof [3]. We can rewrite the given sum as follows:

$$1+\frac{1}{2}+\cdots+\frac{1}{p-1}=(1+\frac{1}{p-1})+(\frac{1}{2}+\frac{1}{p-2})+\cdots+(\frac{1}{\frac{p-1}{2}}+\frac{1}{\frac{p+1}{1}})$$
$$=p(\frac{1}{1(p-1)})+(\frac{1}{2(p-2)}+\cdots+(\frac{1}{\frac{p-1}{2}\frac{p+1}{2}})=p\frac{A}{(p-1)!}.$$

It suffices to show that

$$A=\sum_{i=1}^{\frac{p-1}{2}}\frac{(p-1)!}{i(p-i)}$$

is divisible by the prime p. Consider the multiplicative group $\mathbb{Z}_p$, consisting of all non-zero elements modulo p. Let $\overline{r}$ be the element corresponding to $\frac{(p-1)!}{i(p-i)}$ for each $1\le i\le\frac{p-1}{2}$, i.e., $r\equiv\frac{(p-1)!}{i(p-i)} \pmod p$. Using Wilson's theorem, for each $1\le i\le\frac{p-1}{2}$ we have $-ri^2\equiv-1 \pmod p$. Thus, $\overline{i^2}$ is the inverse of the element $\overline{r}$. Since, there is a bijection between the squares in $\mathbb{Z}_p$ and the set $\{1,\overline{2},\ldots,\overline{\frac{p-1}{2}}\}$. Therefore, we can rewrite A as

$$A=1^2+2^2+\cdots+(\frac{p-1}{2})^2=(\frac{p-1}{2})(\frac{p+1}{2})(\frac{p}{6})\equiv 0 \pmod p.$$

Second Proof (By the Author). Using elementary properties of congruences modulo a prime p, we can write

$$2\sum_{i=1}^{p-1}\frac{1}{i}=\sum_{i=1}^{p-1}\frac{1}{i}+\sum_{i=1}^{p-1}\frac{1}{p-i}=p\sum_{i=1}^{p-1}\frac{1}{i(p-i)}=p\sum_{i=1}^{p-1}\frac{1}{i^2}.$$

It suffices to show that $\sum_{i=1}^{p-1}\frac{1}{i^2}\equiv 0 \pmod p$. By the previous proof, the elements of the set $\{\frac{1}{1^2},\frac{1}{2^2},\ldots,\frac{1}{(p-1)^2}\}$ have the same residues modulo p as the elements of the set $\{1^2,2^2,\ldots,(p-1)^2\}$. Therefore, it is sufficient to show that

$$\sum_{i=1}^{p-1}i^2\equiv 0 \pmod p.$$

Let $p>5$ and let a be a natural number such that $p\nmid a^2$. The set $\{1,2,\ldots,p-1\}$ is a reduced residue system modulo p, and hence the set $\{1a,2a,\ldots,(p-1)a\}$ is also a reduced residue system modulo p. Therefore, we have

$$\sum_{i=1}^{p-1}i^2=\sum_{i=1}^{p-1}(ai)^2=a^2\sum_{i=1}^{p-1}i^2.$$

Since $p\nmid a^2$, it follows that $\sum_{i=1}^{p-1}i^2\equiv 0 \pmod p$.

Third Proof Inspired by Theorem 5.25 on page 116 of Apostol's book [1], we consider the polynomial

$$f(x)=(x-1)(x-2)\cdots(x-p+1)-(x^{p-1}-1).$$

Since the degree of $f(x)$ is at most $p-2$, we can write it as

$$f(x)=a_{p-2}x^{p-2}+a_{p-3}x^{p-3}+\cdots+a_1x+a_0.$$

We will now show that all coefficients of $f(x)$ are divisible by the prime p. Let

$$g(x) = (x-1)(x-2)\cdots(x-p+1) \quad \text{and} \quad h(x) = x^{p-1} - 1.$$

The roots of the polynomial $g(x)$ are the numbers $1, 2, \ldots, p-1$, and hence $g(x) \equiv 0 \pmod{p}$. By Fermat's little theorem, these numbers are also roots of the polynomial $h(x)$, i.e., $h(x) \equiv 0 \pmod{p}$. The polynomial $f(x) = g(x) - h(x)$ has degree $p-2$ but the congruence $f(x) \equiv 0 \pmod{p}$ has $p-1$ roots: $1, 2, \ldots, p-1$. Hence, by Lagrange's theorem, each coefficient of $f(x)$ is divisible by p.

Note that by setting $x = 0$, we easily obtain Wilson's theorem , since

$$f(0) = (-1)(p-1)! + 1 = a_0.$$

Since $a_0 \equiv 0 \pmod{p}$, we have $(p-1)! \equiv -1 \pmod{p}$.

Now, by setting $x = p$, we compute the value of $f(p)$. Thus,

$$f(p) = (p-1)! - p^{p-1} + 1 = a_{p-2}p^{p-2} + a_{p-3}p^{p-3} + \cdots + a_1 p + (p-1)! + 1.$$

Therefore,

$$p^{p-1} + a_{p-2}p^{p-2} + a_{p-3}p^{p-3} + \cdots + a_1 p = 0.$$

Dividing both sides by the prime number p, we get

$$p^{p-2} + a_{p-2}p^{p-3} + a_{p-3}p^{p-4} + \cdots + a_2 p + a_1 = 0.$$

Since $p^2 \mid (p^{p-2} + a_{p-2}p^{p-3} + a_{p-3}p^{p-4} + \cdots + a_3 p^2)$ and $p^2 \mid a_2 p$, it follows that $p^2 \mid a_1$.

By the definition of the polynomial $f(x)$, we have $a_1 = f'(0)$. Taking the logarithm of the function $g(x)$ and differentiating, we get

$$(\ln g(x))' = \frac{g'(x)}{g(x)} = \frac{[(x-1)(x-2)\cdots(x-p+1)]'}{(x-1)(x-2)\cdots(x-p+1)} = \sum_{k=1}^{p-1} \frac{1}{x-k}.$$

Thus, by substitution, we have

$$f'(x) = g'(x) - h'(x) = (x-1)(x-2)\cdots(x-p+1)\sum_{k=1}^{p-1} \frac{1}{x-k} - (p-1)x^{p-2}.$$

Setting $x = 0$, we get

$$a_1 = f'(0) = (-1)^{p-1}(p-1)!\sum_{k=1}^{p-1} \frac{-1}{k}.$$

Since $p^2 \mid a_1$ and, by Wilson's theorem, $p \nmid (p-1)!$, it follows that

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p^2}.$$

This completes the proof of Wolstenholme's theorem.

http://dx.doi.org/10.22108/msci.2025.141789.1669

Fourth Proof In this approach, we utilize the relationship between Stirling numbers of the first kind, denoted by $\left[{n \atop k}\right]$, which count the number of permutations of n elements with k cycles, and harmonic numbers. It can be easily shown that Stirling numbers of the first kind satisfy the recurrence relation

$$\left[{n \atop k}\right] = (n-1)\left[{n-1 \atop k}\right] + \left[{n-1 \atop k-1}\right] \tag{2.1}$$

with the initial conditions $\left[{n \atop 0}\right] = 0$ and $\left[{0 \atop 0}\right] = 1$. Applying this recurrence for the special case $k = 2$, we obtain

$$\left[{n+1 \atop 2}\right] = n!H_n = n!\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right). \tag{2.2}$$

Carlitz [5] investigated congruence properties of these numbers and showed that $\left[{p \atop k}\right] \equiv 0 \pmod{p}$.

Signed Stirling numbers of the first kind are defined as $\overline{\left[{n \atop k}\right]} = (-1)^{n-k}\left[{n \atop k}\right]$ and satisfy the relation

$$\sum_{k=0}^{n} \overline{\left[{n \atop k}\right]} x^k = x(x-1)(x-2)\cdots(x-n+1).$$

(See Theorem A, page 213 of [6]). Setting $n = x = p$ in the above equation yields

$$\sum_{k=0}^{n} \overline{\left[{p \atop k}\right]} p^k = p!.$$

Expanding the series, we have

$$p! = p\left[{p \atop 1}\right] - p^2\left[{p \atop 2}\right] + \cdots + p^{p-1}\left[{p \atop p-1}\right] - p^p\left[{p \atop p}\right].$$

Since $p\left[{p \atop 1}\right] = p(p-1)!$, dividing both sides by p^2 gives

$$\left[{p \atop 2}\right] = p\left[{p \atop 3}\right] + \cdots + p^{p-4}\left[{p \atop p-2}\right] - p^{p-3}\left[{p \atop p-1}\right] + p^{p-2}\left[{p \atop p}\right]. \tag{2.3}$$

Carlitz's congruence implies that $p\left[{p \atop 3}\right] \equiv 0 \pmod{p^2}$. Thus, all terms on the right-hand side of the above equation are congruent to zero modulo p^2. Therefore,

$$H_{p-1} = \frac{1}{(p-1)!}\left[{p \atop 2}\right] \equiv 0 \pmod{p^2}.$$

□

3. Summary of Proofs/Conclusions

In [16], the author proposed the following conjectures, which we prove in [19].

Conjecture 3.1 ([16, Conjecture 1]). *Let $p \geq 3$ be a prime. Then, for any positive integer n, we have*

$$\binom{pn-1}{p} \equiv n-1 \pmod{p^3}.$$

Conjecture 3.2 ([16, Conjecture 2])**.** *For positive integers n, ℓ, and $k \equiv 0, 1 \pmod 3$, we have*

$$\binom{3^\ell n - k}{3} \equiv \left\lfloor \frac{3^\ell n - k}{3} \right\rfloor \pmod{3^2}.$$

The second conjecture can be easily generalized as follows.

Conjecture 3.3 ([16, Conjecture 3])**.** *For positive integers n, ℓ, and $k \equiv 0, 1 \pmod p$, we have*

$$\binom{p^\ell n - k}{p} \equiv \left\lfloor \frac{p^\ell n - k}{p} \right\rfloor \pmod{p^3}.$$

We prove the second and third conjectures, which are consequences of

$$\binom{n}{p} \equiv \left\lfloor \frac{n}{p} \right\rfloor \pmod p.$$

This result can be easily proved using Lucas' theorem. Alternatively, we can provide an elementary proof. Let $n = pq + r$ where $0 \le r < p$. Then $\lfloor \frac{n}{p} \rfloor = q$. Thus,

$$\begin{aligned}
\binom{n}{p} &= \frac{(pq+r)!}{p!(pq+r-p)!} \\
&= \frac{1}{p!} \prod_{t=0}^{p-1} (pq+r-t) \\
&= \frac{pq}{p!} \prod_{\substack{0 \le t \le p \\ t \ne r}} (pq+r-t) \\
&= \frac{q}{(p-1)!} \prod_{\substack{0 \le t \le p \\ t \ne r}} (pq+r-t).
\end{aligned}$$

The set $\{pq + r - i \mid 0 \le i < p; i \ne r\}$ forms a complete residue system modulo p. Therefore,

$$\prod_{\substack{0 \le t \le p \\ t \ne r}} (pq+r-t) \equiv (p-1)! \pmod p.$$

By Wilson's theorem , $\binom{n}{p} \equiv q(-1)(-1) \equiv q \pmod p$.

The second conjecture, Conjecture 3.2, can be easily proved by a simple calculation:

$$\begin{aligned}
\binom{n3^\ell - k}{3} &= \frac{(n3^\ell - k)(n3^\ell - k - 1)(n3^\ell - k - 2)}{1 \times 2 \times 3} \\
&= \left(\frac{n3^\ell - k}{3}\right) \sum_{i=0}^{2} (-1)^i (n3^\ell - k)^i H_i(2) \qquad (3.1) \\
&\equiv \left\lfloor \frac{3^\ell n - k}{3} \right\rfloor \pmod{3^2}.
\end{aligned}$$

 http://dx.doi.org/10.22108/msci.2025.141789.1669

In [19], the authors have investigated Conjecture 3.3 for the case p^4 using Mathematica but have not been able to find a general formula. For example, for $p = 7, \ell = 3$, and $k = 14$, we have

$$\binom{np^\ell - k}{p} - \left\lfloor \frac{np^\ell - k}{p} \right\rfloor \equiv 1715 \pmod{p^4}.$$

Apparently, the value of the above expression depends on the prime factorization of n. This question can be extended to higher powers of p.

The Stirling numbers of the second kind $\left\{ n \atop k \right\}$ represent the number of partitions of an n-set into k non-empty subsets. Investigating Conjecture 3.3 for Stirling numbers of the second and first kind is an interesting research problem:

$$\left\{ n \atop p \right\} \equiv ? \pmod{p} \quad \text{and} \quad \left[n \atop p \right] \equiv ? \pmod{p}.$$

A general form of Wolstenholme's theorem can be stated as follows:

Conjecture 3.4. *For which values of m and n does the congruence*

$$\binom{np-1}{mp-1} \equiv 1 \pmod{p^3} \tag{3.2}$$

hold?

Although a complete solution to this problem is not straightforward, investigating specific cases for n and m may be more tractable.

Conjecture 3.5. *Let n be a natural number and p be a prime number. Then,*

$$\binom{np-1}{(n-1)p} \equiv 1 \pmod{p^3}.$$

Moreover, for any $1 \le i \le p^{\ell+2}$, we have

$$\binom{np^\ell - 1}{p-1} \equiv 1 \pmod{p^i}.$$

References

[1] T. M. Apostol, *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg, 1976.

[2] C. Babbage, Demonstration of a theorem relating to prime numbers, *Edinburgh. Phil. J.*, **1** (1819) 46–49.

[3] M. Bayat, A generalization of Wolstenholme's theorem, *Amer. Math. Monthly*, **104** no. 6 (1997) 557–560.

[4] V. Brun, J. O. Stubban, J. E. Fjeldstad, R. Tambs Lyche, K. E. Aubert, W. Ljunggren and E. Jacobsthal, On the divisibility of the difference between two binomial coefficients, *Den 11te Skandinaviske Matematikerkongress, Trondheim*, (1949), Johan Grundt Tanums Forlag, Oslo, (1952) 42–54.

[5] L. Carlitz, A Note on Stirling Numbers of the First Kind, *Math. Mag.*, **37** no. 5 (1964) 318–321.

[6] L. Comtet, *Advanced Combinatorics: The art of finite and infinite expansions*, Springer Science & Business Media, 2012.

[7] J. W. L. Glaisher, Congruences relating to the sums of products of the first n numbers and to other sums of products, *Quart. J. Math.,* **31** (1900) 1–35.

[8] J. W. L. Glaisher, On the residues of the sums of products of the first $p-1$ numbers, and their powers, to modulus p^2 or p^3, *Quart. J. Math.*, **31** (1900) 321–353.

[9] R. K. Guy, *Unsolved problems in number theory*, Problem Books in Mathematics. Unsolved Problems in Intuitive Mathematics, **1**, Springer-Verlag, New York-Berlin, 1981.

[10] C. Helou and G. Terjanian, On Wolstenholme's theorem and its converse, *J. Number Theory*, **128** no. 3 (2008) 475–499.

[11] K. Ireland and M. Rosen, *classical introduction to modern number theory*, Revised edition of Elements of number theory, Graduate Texts in Mathematics, **84**, Springer-Verlag, New York-Berlin, 1982.

[12] J. P. Jone, Private correspondence, January, 1994.

[13] R. Meštrović, Congruences for Wolstenholme primes, *Czechoslovak Math. J.*, **65(140)** no. 1 (2015) 237–253.

[14] R. J. McIntosh, On the converse of Wolstenholme's theorem, *Acta Arith.*, **71** no. 4 (1995) 381–389.

[15] M. Mirzavaziri, Counting the Countable, *Sokhangostar Publication*, Tehran, Iran, 2008. [InPersion]

[16] M. P. Saikia, Conjectures on congruences of binomial coefficients modulo higher powers of a prime number, *J. Assam Acad. Math.*, **13** (2023) 5–7.

[17] R. Tauraso, More congruences for central binomial coefficients, *J. Number Theory*, **130** no. 12 (2010) 2639–2649.

[18] J. Wolstenholme, On certain properties of prime numbers, *Quart. J. Pure Appl. Math.*, **5** (1862) 35–39.

[19] D. Yaqubi and M. Mirzavaziri, Extending Wolstenholm's theorem: A new perspective, (2024). https://www.researchgate.net/publication/386148476.

[20] D. Yaqubi and M. Mirzavaziri, Some divisibility properties of binomial coefficients, *J. Number Theory*, **183** (2018) 428–441.

[21] J. Zhao, Wolstenholme type theorem for multiple harmonic sums, *Int. J. Number Theory*, **4** no. 1 (2008) 73–106.

[22] Z. Zhi-Hong, Congruences concerning Bernoulli numbers and Bernoulli polynomials, *Discrete Appl. Math.*, **105** no. 1-3 (2000) 193–223.

[23] V. Trevisan, W. Kenneth, Testing the converse of Wolstenholme's theorem. 16th School of Algebra, Part II (Portuguese) (Brasília, 2000), *Mat. Contemp.*, **21** (2001) 275–286.

Daniel Yaqubi

Department of Compute science, University of Torbat e Jam Torbat e Jam, Iran

Email: yaqubi@tjamcaas.ac.ir

Madjid Mirzavaziri

Department of Mathematics, Ferdowsi University of Mashhad, Mashhad, Iran

Email: mirzavaziri@um.ac.ir

http://dx.doi.org/10.22108/msci.2025.141789.1669