Mathematics and Society
University of Isfahan
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.
© 2025 The Author(s)
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 $1\leq i\leq\frac{p-1}{2}$, i.e., $r\equiv\frac{(p-1)!}{i(p-i)} \pmod p$. Using Wilson's theorem, for each $1\leq i\leq\frac{p-1}{2}$ 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 $\begin{bmatrix} n \\ k \end{bmatrix}$, 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

$$\begin{bmatrix} n \\ k \end{bmatrix} = (n-1)\begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} \tag{2.1}$$

with the initial conditions $\begin{bmatrix} n \\ 0 \end{bmatrix} = 0$ and $\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1$. Applying this recurrence for the special case $k = 2$, we obtain

$$\begin{bmatrix} n+1 \\ 2 \end{bmatrix} = n!H_n = n!\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right). \tag{2.2}$$

Carlitz [5] investigated congruence properties of these numbers and showed that $\begin{bmatrix} p \\ k \end{bmatrix} \equiv 0 \pmod{p}$.

Signed Stirling numbers of the first kind are defined as $\overline{\begin{bmatrix} n \\ k \end{bmatrix}} = (-1)^{n-k}\begin{bmatrix} n \\ k \end{bmatrix}$ and satisfy the relation

$$\sum_{k=0}^{n} \overline{\begin{bmatrix} n \\ k \end{bmatrix}} x^k = x(x-1)(x-2)\cdots(x-n+1).$$

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

$$\sum_{k=0}^{n} \overline{\begin{bmatrix} p \\ k \end{bmatrix}} p^k = p!.$$

Expanding the series, we have

$$p! = p\begin{bmatrix} p \\ 1 \end{bmatrix} - p^2\begin{bmatrix} p \\ 2 \end{bmatrix} + \cdots + p^{p-1}\begin{bmatrix} p \\ p-1 \end{bmatrix} - p^p\begin{bmatrix} p \\ p \end{bmatrix}.$$

Since $p\begin{bmatrix} p \\ 1 \end{bmatrix} = p(p-1)!$, dividing both sides by p^2 gives

$$\begin{bmatrix} p \\ 2 \end{bmatrix} = p\begin{bmatrix} p \\ 3 \end{bmatrix} + \cdots + p^{p-4}\begin{bmatrix} p \\ p-2 \end{bmatrix} - p^{p-3}\begin{bmatrix} p \\ p-1 \end{bmatrix} + p^{p-2}\begin{bmatrix} p \\ p \end{bmatrix}. \tag{2.3}$$

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

$$H_{p-1} = \frac{1}{(p-1)!}\begin{bmatrix} p \\ 2 \end{bmatrix} \equiv 0 \pmod{p^2}.$$

□

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 $1 \leq i \leq p^{\ell+2}$, we have

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

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

ریاضی و جامعه
شاپا (چاپی): ۲۳۴۵-۶۴۹۳، شاپا(الکترونیکی): ۲۳۴۵-۶۵۰۷
جلد ۱۰، شماره ۴ (۱۴۰۴)، صص. ۱۰۵-۱۳۱
© ۱۴۰۴ دانشگاه اصفهان

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

نتایجی پیرامون قضیه ولستن‌هولم و کاربردهای آن

دانیال یعقوبی* و مجید میرزاوزیری

چکیده. در سال ۱۸۶۲ ولستن‌هولم ثابت کرد، $\binom{۲p-۱}{p-۱} \equiv ۱ \pmod{p^۳}$ که در آن $p \geq ۵$ عددی اول است. این قضیه هم‌ارز با بخش پذیری صورت کسر مجموع هارمونیک

$$۱ + \frac{۱}{۲} + \cdots + \frac{۱}{p-۱}$$

بر عدد $p^۲$ می‌باشد. با پی‌بردن به کاربردهای متفاوت قضیه ولستن‌هولم در قرن نوزدهم، باعث گردید ریاضیدان‌های برجسته زیادی مسائل مرتبط با بخش‌پذیری ضرایب کسرهای گویا و ضرایب دوجمله‌ای بر توان‌های اعداد اول را مورد مطالعه قرار دادند. ظاهر شدن اعداد برنولی در این قضیه و ارتباط آن با ضرایب دوجمله‌ای، پای این بخش از ریاضیات را در نظریه اعداد تحلیلی نیز بازکرد. اثبات‌های متفاوتی از قضیه ولستن‌هولم توسط ریاضیدان‌ها مطرح شده است. در این مقاله ما به بررسی قضیه ولستن‌هولم برای توان‌های بیشتر عدد اول p و همچنین بررسی این اثبات‌های متفاوت می‌پردازیم. عکس قضیه ولستن‌هولم برای نخستین بار توسط جونز مطرح گردید که بیان می‌کند اگر عدد طبیعی n در رابطه $\binom{۲n-۱}{n-۱} \equiv ۱ \pmod{n^۳}$ صدق کند آنگاه n عددی اول می‌باشد. ما این مقاله را با بررسی شرایط عکس قضیه ولستن‌هولم و همچنین بیان چند مسئله به پایان می‌رسانیم.

۱. مقدمه

نظریه اعداد یکی از قدیمی‌ترین شاخه‌های علم ریاضیات می‌باشد. اولین آثار نظریه اعداد را می‌توان در میان بابلی‌ها از اواسط هزاره سوم قبل از میلاد یافت. فهرستی از اعداد که به سه‌گانه فیثاغورثی [۱] شهرت دارند در آن زمان پیدا شده است. این شاخه از ریاضیات به مطالعه خواص اعداد می‌پردازد. یکی از مهمترین مفاهیم در نظریه اعداد مفهوم بخش‌پذیری ضرایب دوجمله‌ای [۲] می‌باشد که از مسائل جذاب در شاخه نظریه اعداد و ترکیبیات می‌باشد و توسط بسیاری از ریاضیدان‌های مشهور مورد بررسی قرار گرفته است. از جمله این ریاضیدان‌ها می‌توان به جوزف ولستن‌هولم [۳] که در سال ۱۸۲۹ در شهر اِکلز [۴] انگلیس متولد شده است اشاره کرد. بیشتر شهرت ولستن‌هولم به‌خاطر بیان قضیه زیر می‌باشد.

عبارات و کلمات کلیدی: قضیه ولستن‌هولم، اعداد هارمونیک، قضیه اویلر، اعداد برنولی، ضریب دوجمله‌ای.
نوع مقاله: مروری
دبیرتخصصی رابط: جواد اسدالهی
* نویسنده مسئول
تاریخ دریافت: ۱۴۰۳/۰۳/۲۱ تاریخ پذیرش: ۱۴۰۳/۱۱/۰۸ تاریخ انتشار آنلاین: ۱۴۰۴/۰۴/۰۸
ارجاع به مقاله: د. یعقوبی و م. میرزاوزیری، نتایجی پیرامون قضیه ولستن‌هولم و کاربردهای آن، نشریه ریاضی و جامعه، ۱۰ شماره ۴ (۱۴۰۴) ۱۰۵-۱۳۱.
http://dx.doi.org/10.22108/msci.2025.141789.1669 .

[1]Pythagorean triples [2]binomial cofficents [3]Joseph Wolstenholme [4]Eccles

قضیه ۱.۱ (قضیه ولستن‌هولم). فرض کنید $p \geq ۵$ عددی اول باشد. در این‌صورت صورت کسر

$$۱ + \frac{۱}{۲} + \cdots + \frac{۱}{p-۱}$$

بر $p^۲$ بخش پذیر می‌باشد.

از قرن نوزدهم به بعد، ریاضیدان‌های برجسته زیادی مسائل مرتبط با بخش‌پذیری ضرایب کسرهای گویا و ضرایب دوجمله‌ای بر توان‌های اعداد اول را مورد مطالعه قرار دادند. از جمله این ریاضیدان‌ها می‌توان به باباج[۵]، کوشی[۶]، کیلی[۷]، گاوس[۸]، کومر[۹]، و لوکاس[۱۰] اشاره‌کرد. هدف از نگارش این مقاله، بیان و اثبات قضیه ولستن‌هولم و صورت‌های توسیع یافته آن می‌باشد. بخش ۲ این مقاله به تعاریف و مقدمات مورد نیاز اختصاص پیدا کرده است. در این بخش، نشان می‌دهیم قضیه ولستن‌هولم هم‌ارز با همنهشتی $\binom{۲p-۱}{p-۱} \equiv ۱ \pmod{p^۳}$ می‌باشد. به راحتی می‌توان نشان داد همنهشتی $\binom{۲p-۱}{p-۱} \equiv ۱ \pmod{p}$ برای همه اعداد اول برقرار می‌باشد. در سال ۱۸۱۹، باباج همنهشتی $\binom{۲p-۱}{p-۱} \equiv ۱ \pmod{p^۲}$ را برای تمام $p \geq ۲$ به‌دست آورد [۲]. بخش ۳ به بررسی قضیه ولستن‌هولم برای توان‌های بیشتر عدد اول p پرداخته و در بخش ۴، عکس قضیه ولستن‌هولم را مطرح کرده و به حالت‌های خاص آن می‌پردازیم و در بخش ۵، به بیان چند حدس و مسئله می‌پردازیم.

۲. مقدمات و تعاریف اولیه

در این بخش، ابتدا به بیان بعضی از قضیه‌ها و تعاریف در نظریه اعداد و ترکیبیات که در ادامه مقاله مورد استفاده قرار می‌گیرد اشاره می‌کنیم. سپس اثبات‌های متفاوتی از قضیه ولستن‌هولم را بیان می‌کنیم.

تعریف ۱.۲ (دستگاه کامل مانده‌ها). مجموعه $\mathbf{S} = \{x_۱, x_۲, \ldots, x_m\}$ از باقی‌مانده‌ها به پیمانه m را یک دستگاه کامل مانده‌ها[۱۱] به پیمانه m گویند هرگاه برای هر $y \in \mathbb{Z}$ عضوی مانند $x_j \in \mathbf{S}$ وجود داشته باشد به‌طوری‌که $y \equiv x_j \pmod{m}$. به بیان ساده‌تر اگر از هر کلاس باقی‌مانده به پیمانه m یک عضو را انتخاب کنیم، آنگاه مجموعه این اعضاء انتخاب شده تشکیل یک دستگاه کامل مانده به پیمانه m خواهد داد.

مجموعه $\mathbf{S} = \{x_۱, x_۲, \ldots, x_m\}$ را یک دستگاه مخفّف مانده‌ها[۱۲] به پیمانه m گویند در صورتی‌که این مجموعه از هر کلاس باقی‌مانده به پیمانه m که نسبت به m اول باشد یک و تنها یک عضو داشته باشد. تمامی دستگاه‌های مخفّف مانده‌ها به پیمانه m دارای تعداد اعضای یکسانی می‌باشند. این تعداد برابر با تابع اویلر[۱۳] $\phi(m)$ می‌باشد.

قضیه ۲.۲ (قضیه کوچک فرما[۱۴]). فرض کنیم p عددی اول و متباین با عدد $a \in \mathbb{Z}$ باشد. بنابراین $a^p \equiv a \pmod{p}$.

قضیه کوچک فرما برای حالت $p = ۲, ۳$ واضح می‌باشد. زیرا حاصل‌ضرب دوعدد متوالی بر دو و سه عدد متوالی بر سه بخش‌پذیر می‌باشد. این الگو برای اعداد اول بزرگتر از ۵ جواب نمی‌دهد. قضیه کوچک فرما با استقرا به راحتی قابل اثبات می‌باشد.

قضیه ۳.۲ (قضیه ویلسون[۱۵]). فرض کنیم p عددی اول باشد. در این‌صورت $(p-۱)! \equiv -۱ \pmod{p}$.

قضیه ۴.۲ (قضیه لاگرانژ[۱۶]). فرض کنیم p عددی اول و $f(x)$ چندجمله‌ای با ضرایب صحیح از درجه n باشد که هیچ‌یک از ضرایبش بر p بخش‌پذیر نمی‌باشد. در این‌صورت معادله $f(x) \equiv ۰ \pmod{p}$ نمی‌تواند بیش n جواب ناهمنهشت داشته باشد.

[5]Babbage [6]Cauchy [7]Cayley [8]Gauss [9]Kummer [10]Lucas [11]complete residue system [12]reduced residue system
[13]Euler function [14]Little Fermat's theorem [15]Wilson's theorem [16]Lagrange's theorem

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

بی‌تردید یکی از زیباترین و پرکاربردترین نتایج در مسائل تقسیم‌پذیری ضرایب دوجمله‌ای قضیه لوکا [17] می‌باشد. این قضیه برای نخستین‌بار توسط ادوارد لوکا در سال ۱۸۷۸ مطرح گردید.

قضیه ۵.۲ (قضیه لوکا). فرض کنیم p عددی اول باشد. در این‌صورت برای اعداد طبیعی n, k داریم

$$\binom{\sum_{i=0}^{k} a_i p^i}{\sum_{i=0}^{k} b_i p^i} \equiv \prod_{i=0}^{k} \binom{a_i}{b_i} \pmod{p};$$

که در آن $a_i, b_i \in \{0, 1, \ldots, p-1\}$.

در سال ۱۸۶۲ تقریباً ۱۶۲ سال پیش، ولستن‌هولم [۱۷] قضیه زیر را که با نام خودش شناخته می‌شود عنوان کرد. این قضیه سرآغازی بر پژوهش ریاضیدان‌ها در این شاخه از نظریه اعداد بود. اثبات‌های متفاوتی برای قضیه ولستن‌هولم بیان گردیده است که در زیر به بیان چند نمونه از آن‌ها می‌پردازیم.

تعریف ۶.۲. فرض کنید p عددی اول باشد. برای هر عدد صحیح مثبت $1 \leq n \leq p-1$ اعداد هارمونیک توسیع یافته $H_n(p-1)$ و تابع توسیع‌یافته زتای‌ریمان [18] $R_n(p-1)$ را به‌صورت

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

تعریف می‌کنیم.

قضیه ۷.۲ (قضیه ولستن‌هولم). اگر $p \geq 3$ یک عدد اول باشد، صورت کسر $1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$ بر p^2 بخش پذیر می‌باشد.

اثبات.

اثبات اول [۳]. ابتدا کسر فوق را به‌صورت زیر بازنویسی می‌کنیم

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

کافی‌است نشان دهیم

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

بر عدد اول p تقسیم‌پذیر می‌باشد. گروه ضربی $\mathbb{Z}_p$، تشکیل شده از همه عناصر غیرصفر به پیمانه p را در نظر بگیرید. فرض کنید $\overline{r}$ عضو متناظر با $\frac{(p-1)!}{i(p-i)}$ در گروه $\mathbb{Z}_p$، برای هر $1 \leq i \leq \frac{p-1}{2}$ باشد، یعنی $r \equiv \frac{(p-1)!}{i(p-i)} \pmod{p}$. با استفاده از قضیه ویلسون ۳.۲، برای هر $1 \leq i \leq \frac{p-1}{2}$ داریم $-ri^2 \equiv -1 \pmod{p}$. بنابراین $\overline{i^2}$ معکوس عضو $\overline{r}$ می‌باشد.

چون $\overline{i^2} = \overline{(p-i)^2}$، بنابراین دوسویی بین اعضای به‌صورت مربع $\mathbb{Z}_p$، و اعضای مجموعه $\{\overline{1}, \overline{2}, \ldots, \overline{\frac{p-1}{2}}\}$ وجود دارد. پس A را می‌توان به‌صورت زیر بازنویسی کرد:

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

[17] Lucas's Theorem [18] generalized zeta function

اثبات دوم (نویسنده). با استفاده از خواص مقدماتی همنهشتی به پیمانه عدد اول p می‌توان نوشت

$$۲\sum_{i=۱}^{p-۱}\frac{۱}{i}=\sum_{i=۱}^{p-۱}\frac{۱}{i}+\sum_{i=۱}^{p-۱}\frac{۱}{p-i}=p\sum_{i=۱}^{p-۱}\frac{۱}{i(p-i)}=p\sum_{i=۱}^{p-۱}\frac{۱}{i^{۲}}.$$

کافی است نشان دهیم $\sum_{i=۱}^{p-۱}\frac{۱}{i^{۲}}\equiv ۰ \pmod p$. با توجه به اثبات قبل، اعضای مجموعه $\{\frac{۱}{۱^{۲}},\frac{۱}{۲^{۲}},\dots,\frac{۱}{(p-۱)^{۲}}\}$ باقی‌مانده‌های یکسانی با مجموعه $\{۱^{۲},۲^{۲},\dots,(p-۱)^{۲}\}$ به پیمانه عدد اول p دارد. پس کافی است نشان دهیم

$$\sum_{i=۱}^{p-۱}i^{۲}\equiv ۰ \pmod p.$$

فرض کنیم $p>۵$ و a عدد طبیعی باشد به‌طوری‌که $p\nmid a^{۲}$. مجموعه $\{۱,۲,\dots,p-۱\}$ یک دستگاه مخفف مانده‌ها [۱۹] به پیمانه p می‌باشد، پس مجموعه $\{۱a,۲a,\dots,(p-۱)a\}$ یک دستگاه مخفف مانده‌ها به پیمانه p می‌باشد. بنابراین داریم

$$\sum_{i=۱}^{p-۱}i^{۲}=\sum_{i=۱}^{p-۱}(ai)^{۲}=a^{۲}\sum_{i=۱}^{p-۱}i^{۲}.$$

چون $p\nmid a^{۲}$ بنابراین $\sum_{i=۱}^{p-۱}i^{۲}\equiv ۰ \pmod p$.

اثبات سوم. در این روش، برای اثبات از ایده قضیه ۵٫۲۵ صفحه ۱۱۶ کتاب آپوستل [۲۰][۱] الهام گرفته‌ایم. چندجمله‌ای

$$f(x)=(x-۱)(x-۲)\cdots(x-p+۱)-(x^{p-۱}-۱)$$

را در نظر بگیرید. درجه $f(x)$ کمتر یا مساوی $p-۲$ می‌باشد. بنابراین می‌توان آن‌را به‌صورت

$$f(x)=a_{p-۲}x^{p-۲}+a_{p-۳}x^{p-۳}+\cdots+a_{۱}x+a_{۰}$$

بازنویسی کرد. ابتدا نشان می‌دهیم که تمام ضرایب $f(x)$ بر عدد اول p بخش‌پذیرند. قرار می دهیم

$$g(x)=(x-۱)(x-۲)\cdots(x-p+۱) \quad و \quad h(x)=x^{p-۱}-۱.$$

ریشه‌های چندجمله‌ای $g(x)$ اعداد $۱,۲,\dots,p-۱$ می‌باشند، از این‌رو $g(x)\equiv ۰ \pmod p$. با توجه به قضیه کوچک فرما ۲.۲، این اعداد ریشه‌های چندجمله‌ای $h(x)$ نیز می‌باشند، یعنی $h(x)\equiv ۰ \pmod p$. چند جمله‌ای $f(x)=g(x)-h(x)$ از درجه $p-۲$ است اما همنهشتی $f(x)\equiv ۰ \pmod p$ دارای $p-۱$ ریشه $۱,۲,\dots,p-۱$ می‌باشد. لذا با توجه به قضیه لاگرانژ ۴.۲، هر یک از ضرایب $f(x)$ بر p تقسیم‌پذیر می‌باشد.

توجه کنید با قرار دادن $x=۰$ به راحتی اثبات قضیه ویلسون ۳.۲ نتیجه می‌شود، زیرا

$$f(۰)=(-۱)(p-۱)!+۱=a_{۰}.$$

از طرفی $a_{۰}\equiv ۰ \pmod p$، بنابراین $(p-۱)!\equiv -۱ \pmod p$.

حال با قرار دادن $x=p$ مقدار $f(p)$ را محاسبه می‌کنیم. پس

$$f(p)=(p-۱)!-p^{p-۱}+۱=a_{p-۲}p^{p-۲}+a_{p-۳}p^{p-۳}+\cdots a_{۱}p+(p-۱)!+۱.$$

بنابراین

$$p^{p-۱}+a_{p-۲}p^{p-۲}+a_{p-۳}p^{p-۳}+\cdots+a_{۱}p=۰.$$

[19] reduced residue system [20] T. M. Apostol

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

با تقسیم طرفین بر عدد اول p نتیجه می‌شود

$$p^{p-۲}+a_{p-۲}p^{p-۳}+a_{p-۳}p^{p-۴}+\cdots+a_۲p+a_۱=۰.$$

با توجه به اینکه $p^۲|(p^{p-۲}+a_{p-۲}p^{p-۳}+a_{p-۳}p^{p-۴}+\cdots+a_۳p^۲$ و $p^۲|a_۲p$، بنابراین $p^۲|a_۱$.

بنا به تعریف چند جمله‌ای $f(x)$، داریم $a_۱=f'(۰)$. از چند جمله‌ای $f(x)=g(x)-h(x)$ با لگاریتم‌گیری از تابع $g(x)$ مشتق گرفته و داریم

$$(\ln g(x))'=\frac{g'(x)}{g(x)}=\frac{[(x-۱)(x-۲)\cdots(x-p+۱)]'}{(x-۱)(x-۲)\cdots(x-p+۱)}=\sum_{k=۱}^{p-۱}\frac{۱}{x-k}.$$

پس با جایگذاری داریم

$$f'(x)=g'(x)-h'(x)=(x-۱)(x-۲)\cdots(x-p+۱)\sum_{k=۱}^{p-۱}\frac{۱}{x-k}-(p-۱)x^{p-۲}.$$

قرار می‌دهیم $x=۰$. لذا

$$a_۱=f'(۰)=(-۱)^{p-۱}(p-۱)!\sum_{k=۱}^{p-۱}\frac{-۱}{k}.$$

چون $p^۲|a_۱$ و همچنین بنابر قضیه ویلسون $p\nmid(p-۱)!$، نتیجه می‌شود

$$۱+\frac{۱}{۲}+\frac{۱}{۳}+\cdots+\frac{۱}{p-۱}\equiv ۰\pmod p.$$

که این اثبات قضیه ولستن‌هولم را کامل می‌کند.

اثبات چهارم. در این روش از رابطه بین اعداد استرلینگ نوع اول[۲۱] $\begin{bmatrix}n\\k\end{bmatrix}$، که تعداد جایگشت‌های از طول n با k دور می‌باشد با اعداد هارمونیک استفاده می‌کنیم. به راحتی می‌توان نشان داد که اعداد استرلینگ نوع اول در رابطه بازگشتی

$$\begin{bmatrix}n\\k\end{bmatrix}=(n-۱)\begin{bmatrix}n-۱\\k\end{bmatrix}+\begin{bmatrix}n-۱\\k-۱\end{bmatrix}$$

با مقادیر اولیه $\begin{bmatrix}n\\۰\end{bmatrix}=۰$ و $\begin{bmatrix}۰\\۰\end{bmatrix}=۱$ صدق می‌کند. استفاده از این رابطه بازگشتی در حالت خاص $k=۲$ نتیجه می‌دهد

$$\begin{bmatrix}n+۱\\۲\end{bmatrix}=n!H_n=n!(۱+\frac{۱}{۲}+\frac{۱}{۳}+\cdots+\frac{۱}{n}).$$

کارلیتز[۲۲] در [۵] برخی از خواص همنهشتی این اعداد را مورد بررسی قرار داده و نشان داده است $\begin{bmatrix}p\\k\end{bmatrix}\equiv ۰\pmod p$.

اعداد استرلینگ علامت‌دار نوع اول[۲۳] به‌صورت $\overline{\begin{bmatrix}n\\k\end{bmatrix}}=(-۱)^{n-k}\begin{bmatrix}n\\k\end{bmatrix}$ نمایش داده می‌شود و در رابطه

$$\sum_{k=۰}^{n}\overline{\begin{bmatrix}n\\k\end{bmatrix}}x^k=x(x-۱)(x-۲)\cdots(x-n+۱).$$

صدق می‌کنند ([۶، قضیه A صفحه ۲۱۳]). در رابطه فوق قرار می‌دهیم $n=x=p$. بنابراین

$$\sum_{k=۰}^{n}\overline{\begin{bmatrix}p\\k\end{bmatrix}}p^k=p!.$$

[21] stirling numbers of the first kind [22] Carlitz [23] Sign Stirling numbers of the first kind

با باز کردن سری فوق داریم

$$p! = p\begin{bmatrix}p\\۱\end{bmatrix} - p^۲\begin{bmatrix}p\\۲\end{bmatrix} + \cdots + p^{p-۱}\begin{bmatrix}p\\p-۱\end{bmatrix} - p^p\begin{bmatrix}p\\p\end{bmatrix}.$$

از طرفی $p\begin{bmatrix}p\\۱\end{bmatrix} = p(p-۱)!$. بنابراین با تقسیم طرفین رابطه بر $p^۲$ داریم

$$\begin{bmatrix}p\\۲\end{bmatrix} = p\begin{bmatrix}p\\۳\end{bmatrix} + \cdots + p^{p-۴}\begin{bmatrix}p\\p-۲\end{bmatrix} - p^{p-۳}\begin{bmatrix}p\\p-۱\end{bmatrix} + p^{p-۲}\begin{bmatrix}p\\p\end{bmatrix}. \quad (۴)$$

رابطه همنهشتی کارلیتز نتیجه می‌دهد $p\begin{bmatrix}p\\۳\end{bmatrix} \equiv ۰ \pmod{p^۲}$. پس تمامی جملات سمت راست تساوی فوق به پیمانه عدد اول $p^۲$ برابر صفر می‌شود. بنابراین

$$H_{p-۱} = \frac{۱}{(p-۱)!}\begin{bmatrix}p\\۲\end{bmatrix} \equiv ۰ \pmod{p^۲}.$$

□

تبصره ۸.۲. باید دقت داشت که رابطه $\begin{bmatrix}p\\۲\end{bmatrix} \equiv ۰ \pmod{p^۲}$، تنها برای عدد اول $p^۲$ درست نمی‌باشد و ممکن است برای توان‌های بیشتر p نیز برقرار باشد. به‌عنوان مثال $\begin{bmatrix}۱۶۸۴۳\\۲\end{bmatrix} \equiv ۰ \pmod{۱۶۸۴۳^۳}$ و $\begin{bmatrix}۲۱۲۴۶۴۷\\۲\end{bmatrix} \equiv ۰ \pmod{۲۱۲۴۶۷۹^۳}$. بنابراین برای این دوعدد داریم $H_{p-۱} \equiv ۰ \pmod{p^۳}$. تا کنون تنها همین دو عدد بدست آمده که در رابطه فوق صدق می‌کند. اعدادی که در رابطه $H_{p-۱} \equiv ۰ \pmod{p^۳}$ صدق کنند را اعداد اول ولستن‌هولم[۲۴] گویند. خیلی از ریاضیدان‌ها اعتقاد دارند که تعداد این اعداد نامتناهی می‌باشد و هنوز این سؤال به‌صورت حل نشده می‌باشد.

تبصره ۹.۲. قرار می دهیم $S(m,k) = \sum_{i\in R_m} \frac{۱}{i^k}$. با الهام از اثبات دوم قضیه ولستن‌هولم، می‌توان نشان داد برای عدد طبیعی a به‌طوری‌که $(a,p) = ۱$ ، مجموعه $\{ai | i \in R_m\}$ تشکیل یک دستگاه مخفف مانده‌ها می‌دهد. بنابراین $S(m,k) \equiv \frac{۱}{a^k}S(m,k) \pmod{m}$. این نتیجه می‌دهد $(a^k-۱)S(m,k) \equiv ۰ \pmod{m}$. همچنین، به‌راحتی می‌توان نشان داد برای عدد فرد k همنهشتی $۲S(m,k) \equiv -mkS(m,k+۱) \pmod{m^۲}$ برقرار می‌باشد.

تبصره ۱۰.۲. با دانستن قضیه ولستن‌هولم، می‌توان همنهشتی $R_۲(p-۱) \equiv ۰ \pmod{p}$ را با روش زیر هم ثابت کرد:
توابع مقدماتی متقارن[۲۵] $e_i(x_۱,x_۲,\ldots,x_n)$ با مقدار اولیه $e_۰(x_۱,x_۲,\ldots,x_n) = ۱$ به‌صورت

$$e_i(x_۱,x_۲,\ldots,x_n) = \sum_{۱\le i_۱\le\cdots\le i_n} x_{i_۱}x_{i_۲}\cdots x_{i_n}$$

تعریف می‌شوند. به‌وسیله این توابع مقدماتی می‌توان نمایشی برای حاصل‌ضرب $x - x_i$ به‌صورت زیر به‌دست آورد:

$$\prod_{i=۱}^{n}(x-x_i) = e_۰(x_۱,x_۲,\ldots,x_n)x^n - e_۱(x_۱,x_۲,\ldots,x_n)x^{n-۱} + \cdots + (-۱)^n e_n(x_۱,x_۲,\ldots,x_n).$$

[24] Wolstenholme primes [25] elementary symmetric function

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

حال بسط زیر را در نظر بگیرید

$$\begin{aligned}\binom{x-۱}{n} =&\frac{۱}{n!}(x-۱)\cdots(x-n)=\prod_{i=۱}^{n}(\frac{x}{i}-۱)=(-۱)^n x^n\prod_{i=۱}^{n}(\frac{۱}{x}-\frac{۱}{i})\\ =&(-۱)^n x^n(x^{-x}-x^{-n+۱}e_۱(\frac{۱}{۱},\frac{۱}{۲},\ldots,\frac{۱}{n}+\cdots+((-۱)^n e_n(\frac{۱}{۱},\frac{۱}{۲},\ldots,\frac{۱}{n})\\ =&(-۱)^n(۱-xe_۱(\frac{۱}{۱},\frac{۱}{۲},\ldots,\frac{۱}{n})+\cdots+(-۱)^n x^n e_n(\frac{۱}{۱},\frac{۱}{۲},\ldots,\frac{۱}{n}).\end{aligned}$$

کافیست در رابطه فوق، قرار دهیم $x=p$ و $n=p-۱$ و آن‌را به پیمانه $p^۳$ محاسبه کنیم.

$$۱\equiv ۱-pe_۱(\frac{۱}{۱},\frac{۱}{۲},\ldots,\frac{۱}{p-۱})+p^۲e_۲(\frac{۱}{۱},\frac{۱}{۲},\ldots,\frac{۱}{p-۱})\pmod{p^۳}.$$

از طرفی با توجه به تعریف توابع مقدماتی متقارن داریم

$$e_۱(\frac{۱}{۱},\frac{۱}{۲},\ldots,\frac{۱}{p-۱})=H_{p-۱},$$

و

$$e_۲(\frac{۱}{۱},\frac{۱}{۲},\ldots,\frac{۱}{p-۱})=\sum_{۱\le i\le j\le p-۱}\frac{۱}{ij}=H_۲(p-۱).$$

با استفاده از اتحاد مربع تساوی

$$\begin{aligned}H_۲(p-۱) &= \sum_{۱\le i\le j\le p-۱}\frac{۱}{ij}=\frac{۱}{۲}(\sum_{i=۱}^{p-۱}\frac{۱}{i}\times\sum_{j=۱}^{p-۱}\frac{۱}{j}-\sum_{i=۱}^{p-۱}\frac{۱}{i^۲})\\ &= \frac{۱}{۲}\big(H_۱^۲(p-۱)-R_۲(p-۱)\big)\end{aligned}$$

برقرار می‌باشد. پس

$$pH_۱(p-۱)\equiv\frac{p^۲}{۲}H_۱^۲(p-۱)-\frac{p^۲}{۲}R_۲(p-۱)\pmod{p^۳}.$$

با توجه به قضیه ولستن‌هولم

$$\frac{p^۲}{۲}H_۱^۲(p-۱)\equiv pH_۱(p-۱)\equiv ۰\pmod{p^۳}.$$

قضیه ولستن‌هولم به‌صورت زیر نیز بیان می‌گردد که با استفاده از تابع تعریف شده $f(x)$ در قضیه ۷.۲ اثبات می‌شود.

قضیه ۱۱.۲. فرض کنیم $p\ge ۵$ باشد. در این‌صورت

$$\binom{۲p-۱}{p-۱}\equiv ۱\pmod{p^۳}.$$

اثبات. فرض کنیم $p\ge ۵$ عددی اول و

$$f(x)=(x-۱)(x-۲)\cdots(x-p+۱)-(x^{p-۱}-۱)$$

چند جمله‌ای تعریف شده در قضیه ۷.۲ باشد. با قرار دادن $x = ۲p$ داریم

$$\begin{aligned} f(۲p) &= (۲p-۱)(۲p-۲)\cdots(۲p-(p-۱)) - (۲p)^{p-۱} - ۱) \\ &= a_{p-۲}(۲p)^{p-۲} + \cdots + a_۱(۲p) + a_۰. \end{aligned}$$

بنابراین $a_۰ = (p-۱)! + ۱$ و

$$\frac{(۲p-۱)!}{p!} - (۲p)^{p-۱} + ۱ = a_{p-۲}(۲p)^{p-۲} + \cdots + a_۱(۲p) + (p-۱)! + ۱.$$

که نتیجه می‌دهد

$$\frac{(۲p-۱)!}{p!} = (۲p)^{p-۱} + a_{p-۲}(۲p)^{p-۲} + \cdots + a_۱(۲p) + (p-۱)!.$$

با توجه به تعریف ضرایب دوجمله‌ای داریم

$$\binom{۲p-۱}{p-۱}(p-۱)! = (۲p)^{p-۱} + a_{p-۲}(۲p)^{p-۲} + \cdots + a_۱(۲p) + (p-۱)!.$$

در اثبات قضیه قبل، نشان دادیم $p|a_۲$ و $p^۲|a_۱$. لذا $p^۳|a_۱(۲p)$. از طرفی

$$p^۳|(۲p)^{p-۱} + a_{p-۲}(۲p)^{p-۲} + \cdots + a_۳(۲p)^۳$$

که این نتیجه می‌دهد

$$\binom{۲p-۱}{p-۱} \equiv (p-۱)! \pmod{p^۳}.$$

از طرفی $p \nmid (p-۱)!$. که این اثبات را کامل می‌کند. □

تبصره ۱۲.۲. قضیه ۱۱.۲ را می‌توان با توسیع دادن بسط دوجمله‌ای $\binom{۲p-۱}{p-۱}$ به‌صورت زیر اثبات کرد:
اعداد تعمیم یافته هارمونیک[۲۶] به‌صورت $H_n(p-۱) = \sum_{۱\le i_۱<i_۲\cdots<i_n\le p-۱} \frac{۱}{i_۱ i_۲\cdots i_n}$ تعریف می‌کنیم. پس می‌توان نوشت

$$\begin{aligned} \binom{۲p-۱}{p} &= \frac{(۲p-۱)(۲p-۲)\cdots(۲p-p)}{۱\times۲\times\cdots\times(p-۱)} \\ &= (\frac{۲p}{۱}-۱)(\frac{۲p}{۲}-۱)\cdots(\frac{۲p}{p-۱}-۱) \\ &= \sum_{i=۰}^{p-۱}(-۱)^i(۲p)^i H_i(p-۱) \\ &\equiv ۱ - ۲pH_۱(p-۱) + ۴p^۲H_۲(p-۱) \pmod{p^۳}. \end{aligned}$$

در قضیه ۷.۲ نشان دادیم $p^۲|H_۱(p-۱)$ و $p|H_۲(p-۱)$. بنابراین $\binom{۲p-۱}{p-۱} \equiv ۱ \pmod{p^۳}$.

تبصره ۱۳.۲. برای عدد اول p، با استفاده از قضیه لوکا ۵.۲ داریم $\binom{۲p}{p} \equiv ۲ \pmod{p}$. این همنهشتی برای حالت $p^۲$ در سال ۱۸۱۹ توسط باباج[۲۷] [۲] اثبات گردید. برای حالت $p^۳$ معادل با قضیه ولستن‌هولم می‌باشد. زیرا $\binom{۲p}{p} = ۲\binom{۲p-۱}{p-۱} \equiv ۲ \pmod{p^۳}$. بررسی مسئله لوکا برای توان‌های بیشتر عدد اول p، برای ریاضیدان‌ها از اهمیت بالایی برخوردار بوده است. همچنین،

[26] generalized harmonic [27] Babbage

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

عکس قضیه ولستن‌هولم که به حدس جونز[۲۸] معروف می‌باشد نیز برای آن‌ها جذاب بوده است. تعدادی زیادی از ریاضیدان‌ها به‌بررسی این حدس پرداخته‌اند و نشان دادند این حدس برای اعداد زوج و اعداد اول توانی کمتر از 10^9 برقرار می‌باشد [۲۲].

حدس ۱۴.۲ (حدس جونز). اگر برای عدد طبیعی n داشته باشیم $\binom{2n-1}{n-1} \equiv 1 \pmod{n^3}$، آنگاه n عددی اول می‌باشد.

عکس قضیه ولستن‌هولم در [۱۴] را در بخش ۴ مورد بررسی قرار داده‌ایم.

۳. بررسی قضیه ولستن‌هولم برای توان‌های بالاتر عدد اول p

در این بخش قضیه ولستن‌هولم را برای توان‌های بالاتر عدد اول p بررسی می‌کنیم. در سال ۱۹۰۰ گلایشر[۲۹] همنهشتی توسیع یافته ولستن‌هولم را برای $p \geq 5$ و عدد صحیح n به‌صورت

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

اثبات کرد [۷، ۸]. اعداد برنولی[۳۰] B_n که در ضرایب تابع نمایی

$$\sum_{n=0}^{\infty} B_n \frac{x^n}{n!} = \frac{x}{e^x - 1}$$

ظاهر می‌گردند، از اهمیت ویژه‌ای در نظریه اعداد تحلیلی برخوردار است. این اعداد در بسیاری از شاخه‌های ریاضی مخصوصاً در توان‌های بالاتر قضیه ولستن‌هولم ظاهر می‌گردد. یکی از مهمترین کاربردهای اعداد برنولی، ارتباط آن با مجموع توانی اعداد صحیح

$$S_m(n) = 1^m + 2^m + 3^m + \cdots + n^m,$$

می‌باشد. به راحتی می‌توان نشان داد

$$S_m(n) = \frac{1}{m+1} \sum_{k=0}^{m} \binom{m+1}{k} B_k n^{m-k+1}.$$

علاقمندان برای مطالعه بیشتر خواص و روابط این اعداد می‌توانند به [۱۱] مراجعه کنند. در سال ۲۰۰۰، هانگ سان[۳۱] قضیه زیر را با استفاده از قضیه کوچک فرما ۲.۲ و رابطه

$$S_m(p-1) = \frac{B_{m+1}(p) - B_{m+1}}{m+1},$$

اثبات کرد و نشان داد اعداد هارمونیک را می‌توان بر حسب ضرایبی از اعداد برنولی بیان کرد.

قضیه ۱.۳. فرض کنید p عدد اول بزرگتر از۳ باشد. در این‌صورت برای $k \in \{1, 2, \ldots, p-4\}$ داریم

$$R_k(p-1) = \sum_{x=1}^{p-1} \frac{1}{x^k} \equiv \begin{cases} \binom{k+1}{2} \frac{B_{p-2-k}}{p-2-k} p^2 \pmod{p^3} & \text{اگر } 2 \nmid k \\ k\left(\frac{B_{2p-2-k}}{2p-2-k} - 2\frac{B_{p-1-k}}{p-1-k} p\right) \pmod{p^3} & \text{اگر } 2 \mid k. \end{cases}$$

[28] Jones' conjecture [29] Glaisher [30] Bernoulli numbers [31] Zhi-Hong Sun

با قرار دادن $k = ۱, ۲$ در قضیه ۶ داریم

$$H_۱(p-۱) = ۱ + \frac{۱}{۲} + \frac{۱}{۳} + \cdots + \frac{۱}{p-۱} \equiv -\frac{۱}{۳}p^۲B_{p-۳} \pmod{p^۳};$$
$$R_۲(p-۱) = ۱ + \frac{۱}{۲^۳} + \frac{۱}{۳^۳} + \cdots + \frac{۱}{(p-۱)^۳} \equiv -\frac{۶}{۵}p^۲B_{p-۵} \pmod{p^۳}.$$

تبصره ۲.۳. با استفاده از قضیه ۶ می‌توان خیلی از روابط تقسیم‌پذیری برای $R_k(p-۱) = \sum_{k=۱}^{p-۱} \frac{۱}{x^k}$ را محاسبه کرد و این تابع را برحسب تابع هارمونیک $H_k(p-۱)$ بیان کرد. به‌عنوان مثال با قرار دادن $k \to p-k$ و استفاده از روابط مقدماتی همنهشتی در نظریه اعداد داریم

$$\begin{aligned} ۲H_۱(p-۱) &= \sum_{k=۱}^{p-۱} \frac{۱}{k} + \sum_{k=۱}^{p-۱} \frac{۱}{p-k} \\ &\equiv \sum_{k=۱}^{p-۱} \frac{p}{k(p-k)} \equiv \sum_{k=۱}^{p-۱} \frac{-p}{k^۲}\left(\frac{۱}{۱-\frac{p}{k}}\right) \\ &\equiv \sum_{k=۱}^{p-۱} \frac{-p}{k^۲} \equiv -pR_۲(p-۱) \pmod{p^۴}. \end{aligned}$$

بنابراین

$$۲H_۱(p-۱) \equiv -\frac{۲}{۳}p^۲B_{p-۳} \equiv -pR_۲(p-۱) \pmod{p^۴}.$$

به راحتی می‌توان نشان داد

$$۲H_۱(p-۱) \equiv -pR_۲(p-۱) \pmod{p^۳},$$

لذا

$$R_۲(p-۱) \equiv \frac{۱}{۳}pB_{p-۳} \pmod{p^۲}.$$

حالت $p^۴$ قضیه ولستن‌هولم برای نخستین‌بار توسط گلایشر مورد بررسی قرار گرفته است [۷]. البته اثباتی که ما ارائه می‌دهیم بسیار متفاوت با اثبات گلایشر می‌باشد.

قضیه ۳.۳. فرض کنید $p \geq ۵$ عددی اول باشد. در این‌صورت

$$\binom{۲p-۱}{p-۱} \equiv ۱ - ۲pH_۱(p-۱) \equiv ۱ - \frac{۲}{۳}p^۳B_{p-۳} \pmod{p^۴}.$$

در حالت کلی

$$\binom{np-۱}{p-۱} \equiv ۱ - \frac{۱}{۳}n(n-۱)p^۳B_{p-۳} \pmod{p^۴}.$$

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

اثبات. ضریب دوجمله‌ای فوق را به‌صورت زیر باز می‌کنیم:

$$\begin{aligned}\binom{np-1}{p} &= \frac{(np-1)(np-2)\cdots(np-p+1)}{1\times 2\times\cdots\times(p-1)}\\ &= (\frac{np}{1}-1)(\frac{np}{2}-1)\cdots(\frac{np}{p-1}-1)\\ &= \sum_{i=0}^{p-1}(-1)^i(np)^iH_i(p-1)\\ &\equiv 1-npH_1(p-1)+(np)^2H_2(p-1)-(np)^3H_3(p-1)\\ &\equiv 1-npH_1(p-1)+(np)^2H_2(p-1)\\ &\equiv 1-\frac{1}{3}np^3B_{p-3}+\frac{1}{3}n^2p^3B_{p-3}\equiv 1-\frac{1}{3}n(n-1)p^3B_{p-3} \pmod{p^4}.\end{aligned}$$

□

با روش مشابه، قضیه ۳.۳ را می‌توان برای توان‌های بیشتر p نیز توسیع داد. حدود ۳۰ سال قبل، تقریباً در اواخر قرن بیستم میلادی، در سال ۱۹۹۵، مَک‌اِینتاش[۳۲] [۱۴] و در سال ۲۰۰۷، زاهو[۳۳][۲۰] نشان دادند برای $p\geq 7$ داریم

$$\binom{2p-1}{p-1}\equiv 1-p^2R_2(p-1)\equiv 1+2pH_1(p-1) \pmod{p^5}.$$

تاوراسو[۳۴] در سال ۲۰۱۰ [۱۶]، قضیه ولستن‌هولم را برای p^6 و مِستراویچ[۳۵] در سال ۲۰۱۵ آن‌را برای p^7 به‌صورت زیر توسیع دادند:

$$\binom{2p-1}{p-1}\equiv 1+2pH_1(p-1)+\frac{2}{3}p^3R_3(p-1)\equiv 1-2pH_1(p-1)-2p^2R_2(p-1) \pmod{p^6},$$

$$\binom{2p-1}{p-1}\equiv 1-2pH_1(p-1)+4p^2H_2(p-1) \pmod{p^7},$$

همنهشتی‌های مختلف قضیه ولستن‌هولم و رابطه آن با اعداد برنولی توسط بسیاری از ریاضیدان‌ها مورد بررسی قرار گرفته است. اخیراً مانجیل ساکیا[۳۶] چند حدس که مرتبط با قضیه ولستن‌هولم و ضرایب دوجمله‌ای می‌باشد را بیان کرده است [۱۵]. این حدس‌ها توسط نویسندگان این مقاله اثبات شده‌اند [۱۸]. حدس اول این مقاله که صورت خاصی از قضیه ولستن‌هولم می‌باشد، روش اثبات کاملاً متفاوتی با قضیه ولستن‌هولم دارد. این حدس به‌صورت زیر می‌باشد:

حدس ۴.۳. برای عدد اول $p\geq 3$ و عدد صحیح مثبت n رابطه زیر درست می‌باشد.

$$\binom{np-1}{p}\equiv\begin{cases} n-1 & \text{اگر } p\geq 5\\ (n-1)(1-np^2(n-1)) & \text{اگر } p=3.\end{cases}$$

[32]McIntosh [33]Zaho [34]Tauraso [35]Meštrović [36]Manjil P. Saikia

حل این حدس در حالتی‌که $(n,p)=1$، راحت می‌باشد. می‌توان با استفاده از قضیه لوکا ۵.۲ در حالت p^3 نوشت

$$\begin{aligned}\binom{np-1}{p} &= \frac{(np-1)!}{(p!)(np-1-p)!}=\frac{(np-p)}{np}\frac{(np)(np-1)!}{p!(np-p-1)!}\\ &= \frac{n-1}{n}\binom{np}{p}\equiv\frac{n-1}{n}\times n\equiv n-1 \pmod{p^3}.\end{aligned}$$

البته اثبات حدس فوق در حالتی‌که $(n-1,p)=1$ با استفاده از قضیه ولستن‌هولم به‌صورت زیر می‌باشد:

$$\begin{aligned}\binom{np-1}{p} &= \frac{(np-1)!}{(p!)(np-1-p)!}=\frac{(np-1)!(np-p)}{(p!)(np-1-p)!(np-p)}\\ &= \frac{(np-1)!(n-1)}{(p-1)!(np-p)!}=(n-1)\binom{np-1}{p-1}\equiv n-1 \pmod{p^3}.\end{aligned}$$

ولی برای حالت $(n,p)\neq 1$ روش اثبات کاملاً متفاوت و سخت می‌باشد.

۴. بررسی معکوس و حالت‌های خاص قضیه ولستن‌هولم

در این بخش به بررسی عکس قضیه ولستن‌هولم که بیان می‌کند اگر رابطه $\binom{2n-1}{n-1}\equiv 1 \pmod{n^k}$ برای $k=3$ برقرار باشد آنگاه nعددی اول می‌باشد می‌پردازیم. عکس قضیه ولستن‌هولم برای نخستین‌بار توسط جونز[37] [۱۲] مطرح گردید. این مسئله در حالت خاص $n=p^2$ در [۱۴] مورد بررسی قرار گرفته و درستی آن برای تمامی اعداد غیر اول $n<10^9$ نشان داده شده است. اتحاد $\binom{r+s}{i}=\sum_{j=0}^{i}\binom{r}{j}\binom{s}{i-j}$ که یکی از مهمترین اتحادهای ترکیبیاتی منتسب به واندرموند[38] می‌باشد در اثبات ادامه قضایا زیاد مورد استفاده قرار می‌گیرد. در حالت $i=s=r=n$ داریم

$$\binom{2n}{n}=\sum_{j=0}^{n}\binom{n}{j}^2.$$

با توجه به اتحاد واندرموند به راحتی می‌توان عکس قضیه ولستن‌هولم به‌صورت

$$\binom{2n-1}{n-1}=\frac{1}{2}\sum_{j=0}^{n}\binom{n}{j}^2,$$

بازنویسی کرد.

لم ۱.۴. فرض کنید p عددی اول باشد. اگر $n=p^r$ و $s\leq r$ بزرگترین توان p باشد که عدد s را عاد می‌کند، بنابراین بزرگترین توان p که $\binom{n}{m}$ را عاد می‌کند برابر با $r-s$ می‌باشد.

اثبات. فرض کنید $\nu_p(n)$ برابر با بزرگترین توان از عدد اول p باشد که n را عاد می‌کند. به سادگی می‌توان دید برای عدد طبیعی k

$$\nu_p(k!)=\lfloor\frac{k}{p}\rfloor+\lfloor\frac{k}{p^2}\rfloor+\cdots.$$

[37] James P. Jones [38] Vandermonde

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

بنابراین

$$\begin{aligned}\nu_p(\binom{n}{m}) &= \lfloor\frac{n}{p}\rfloor + \lfloor\frac{n}{p^2}\rfloor + \cdots - (\lfloor\frac{m}{p}\rfloor + \lfloor\frac{m}{p^2}\rfloor + \cdots) - (\lfloor\frac{n-m}{p}\rfloor + \lfloor\frac{n-m}{p^2}\rfloor + \cdots)\\ &= (-\lfloor\frac{-m}{p}\rfloor - \lfloor\frac{m}{p}\rfloor) + (-\lfloor\frac{-m}{p^2}\rfloor - \lfloor\frac{m}{p^2}\rfloor) + \cdots + (-\lfloor\frac{-m}{p^s}\rfloor - \lfloor\frac{m}{p^s}\rfloor).\end{aligned}$$

واضح است

$$-\lfloor\frac{-m}{p^t}\rfloor - \lfloor\frac{m}{p^t}\rfloor = \begin{cases} 0 & \text{اگر } p^t \mid m \\ 1 & \text{اگر } p \nmid m. \end{cases}$$

□

قضیه ۲.۴. فرض کنید n عدد طبیعی زوجی باشد. در این‌صورت

$$\binom{2n-1}{n-1} \not\equiv 1 \pmod{n^3}.$$

اثبات. فرض کنید $n-1$ و $2n-1$ نمایشی بر مبنای ۲ به‌صورت $n-1 = a_0 + a_1 2 + a_2 2^2 + \cdots + a_k 2^k$ و $2n-1 = 2(n-1)+1 = 1 + a_0 2 + a_1 2^2 + \cdots + a_k 2^{k+1}$ داشته باشند. با توجه به قضیه لوکا ۵.۲ داریم:

$$\binom{2n-1}{n-1} = \binom{a_k}{0}\binom{a_{k-1}}{a_k}\cdots\binom{a_0}{a_1}\binom{1}{a_0} \pmod 2. \tag{۱۱}$$

$\binom{2n-1}{n-1}$ فرد می‌باشد اگر و فقط اگر دارای ضریبی به‌صورت $\binom{1}{0}$ نباشد. یعنی $(a_i, a_{i-1}) \neq (1,0)$ برای $i \in \{1,2,\ldots,k\}$. چون $a_k = 1$ لذا $a_k = a_{k-1} = \cdots = a_1 = a_0 = 1$ و $n-1 = 2^k + \cdots + 2 + 1 = 2^{k+1} - 1$. □

تبصره ۳.۴. قضیه فوق را می‌توان به‌عنوان نتیجه مستقیمی از نتیجه کومر[39] دانست که بیان می‌کند $\nu_p(\binom{a+b}{a})$ که برابر با بزرگترین توان عدد اول p می‌باشد برابر با تعداد انتقال‌ها یا همان قرض گرفتن‌های a و b در مبنای p می‌باشد. قرار می‌دهیم $\binom{2n-1}{n-1} = \frac{1}{2}\binom{n+n}{n}$. بنابراین نمایش بر پایه ۲ $\binom{2n-1}{n-1}$ فرد می‌باشد اگر n توانی از عدد ۲ باشد.

قضیه ۴.۴. اگر $n = 2^\ell$ و $\ell \geq 1$،

$$\binom{2n-1}{n-1} \equiv 3 \pmod{2^4}. \tag{۱۲}$$

اثبات. با استفاده از اتحاد واندرموند داریم

$$\begin{aligned}\binom{2n-1}{n-1} &= \frac{1}{2}\sum_{j=0}^{n}\binom{n}{j}^2\\ &= \frac{1}{2}\left(\binom{2^\ell}{0}^2 + \binom{2^\ell}{1}^2 + \cdots + \binom{2^\ell}{2^\ell-1} + \binom{2^\ell}{2^\ell}^2\right)\\ &= \frac{1}{2}\left(1^2 + \binom{2^\ell}{1}^2 + \cdots + \binom{2^\ell}{2^\ell-1} + 1^2\right)\\ &= 1 + \frac{1}{2}\left(\binom{2^\ell}{0}^2 + \binom{2^\ell}{1}^2 + \cdots + \binom{2^\ell}{2^\ell-1}\right).\end{aligned}$$

[39] Kummer

با استفاده از خاصیت تقارنی ضرایب دوجمله‌ای، یعنی $\binom{n}{m}=\binom{n}{n-m}$ داریم

$$\begin{aligned}\binom{2n-1}{n-1}&=1+\frac{1}{2}\left(2\left(\binom{2^\ell}{1}^2+\binom{2^\ell}{2}^2+\cdots+\binom{2^\ell}{2^{\ell-1}-1}^2\right)+\binom{2^\ell}{2^{\ell-1}}^2\right)\\&=1+\sum_{j=1}^{2^{\ell-1}-1}\binom{2^\ell}{j}^2+\frac{1}{2}\binom{2^\ell}{2^{\ell-1}}^2.\end{aligned}$$

کافی است نشان دهیم

$$A=\sum_{j=1}^{2^{\ell-1}-1}\binom{2^\ell}{j}^2+\frac{1}{2}\binom{2^\ell}{2^{\ell-1}}^2\equiv 2 \pmod{2^4}.$$

با توجه به لم ۱.۴، $\binom{2^\ell}{j}\equiv 0 \pmod 4$. بنابراین $\binom{2^\ell}{j}^2\equiv 0 \pmod{2^4}$ برای هر $j\in\{1,\dots,2^{\ell-1}-1\}$. لم ۱.۴ همچنین نتیجه می‌دهد $\binom{2^\ell}{2^{\ell-1}}=2X$ که X عددی فرد می‌باشد. لذا $\frac{1}{2}\binom{2^\ell}{2^{\ell-1}}^2=2X^2$ چون $X\equiv 1 \pmod 2$ بنابراین $X\equiv\pm 1 \pmod{2^3}$ یا $X\equiv\pm 3 \pmod{2^3}$. در هر صورت $X^2\equiv 1 \pmod{2^3}$. بنابراین $2X^2\equiv 2 \pmod{2^4}$. بنابراین $A\equiv 2 \pmod{2^4}$. □

در ادامه درستی عکس قضیه ولستن‌هولم را برای اعداد فرد مورد بررسی قرار می‌دهیم.

قضیه ۵.۴. فرض کنید ℓ عدد طبیعی باشد. برای $n=3^\ell$، عکس قضیه ولستن‌هولم درست می‌باشد.

اثبات. نشان می‌دهیم $\binom{2n-1}{n-1}\equiv 1 \pmod{3^5}$. به روش مشابه اثبات قضیه قبل داریم

$$\binom{2n-1}{n-1}=1+\sum_{j=1}^{\frac{n-1}{2}}\binom{n}{j}^2.$$

با توجه به لم ۱.۴، ضریب دوجمله‌ای $\binom{n}{j}\equiv 0 \pmod{3^2}$ برای تمام jـها به‌جز $j=3^{\ell-1}$. بنابراین

$$\sum_{j=1}^{\frac{n-1}{2}}\binom{n}{j}^2\equiv\binom{3^\ell}{3^{\ell-1}}^2 \pmod{3^4}.$$

از طرفی $\binom{3^\ell}{3^{\ell-1}}=3Y$ به‌طوری‌که $(3,Y)=1$. این نتیجه می‌دهد $Y\equiv\pm 1 \pmod 3$. لذا $Y^2\equiv 1 \pmod 3$. داریم

$$\binom{3^\ell}{3^{\ell-1}}^2=(3Y)^2\equiv 9 \pmod{3^3}.$$

□

قضیه ۶.۴. فرض کنید n عدد طبیعی و $p\geq 5$ عددی اول باشد. در این‌صورت

$$\binom{np}{p}\equiv n \pmod{p^3}.$$

اثبات. با توجه به نتیجه گلاشیر، به راحتی می‌توان دید $n\equiv n\binom{np-1}{p-1}=\binom{np}{p} \pmod{p^3}$. □

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

تبصره ۷.۴. قضیه ۶.۴ را می‌توان حالت توسیع‌یافته قضیه لوکا ۵.۲ در نظر گرفت. نتایج زیادی درباره حالت توسیع یافته قضیه لوکا به‌دست آمده است. به‌عنوان مثال حالت $\binom{np}{mp} \equiv \binom{a}{b} \pmod{p^3}$ اثبات شده است (از این ویژگی در اثبات حدس ۴.۳ برای حالت $(n,p)=1$ استفاده کرده‌ایم) [۴]. قضیه ۶.۴ را می‌توان با استقرا و کمک اتحاد واندرموند نیز اثبات کرد که به‌علت طولانی بودن از بیان آن خودداری می‌کنیم.

لم ۸.۴. فرض کنید $p \geq 5$ عددی اول و a, b اعداد صحیح نامنفی باشند. برای عدد طبیعی k داریم

$$\binom{p^k a}{p^k b} \equiv \binom{p^{k-1} a}{p^{k-1} b} \pmod{p^{3k}}.$$

اثبات. قرار می‌دهیم $c = b - a$. بنابراین

$$\binom{p^k a}{p^k b} = \frac{(p^k c+1)(p^k c+2)\cdots(p^k c+p^k b)}{1\cdot 2\cdots p^k b}, \tag{۱۳}$$

$$\begin{aligned}\binom{p^{k-1} a}{p^{k-1} b} &= \frac{(p^{k-1} c+1)(p^{k-1} c+2)\cdots(p^{k-1} c+p^{k-1} b)}{1\cdot 2\cdots p^{k-1} b} \\ &= \frac{(p^k c+p)(p^k c+2p)\cdots(p^k c+p^k b)}{p\cdot 2p\cdots p^k b}.\end{aligned}$$

قرار دهید R مجموعه تمام اعداد طبیعی کوچکتر از $p^k b$ باشد که بر p تقسیم‌پذیر نمی‌باشد. با توجه به رابطه بالا می‌توان نوشت

$$\begin{aligned}\binom{p^k a}{p^k b} &= \binom{p^{k-1} a}{p^{k-1} b} \prod_{i\in R}\left(1+\frac{p^k c}{i}\right) \\ &\equiv \binom{p^{k-1} a}{p^{k-1} b}\left(1+\sum_{i\in R}\frac{p^k c}{i}+\sum_{\substack{i,j\in R\\ i<j}}\frac{p^{2k} c^2}{ij}\right) \pmod{p^{3k}}.\end{aligned}$$

با توجه به تبصره ۹.۲ داریم $\sum_{i\in R}\frac{1}{i} \equiv 0 \pmod{p^k}$ و $\sum_{\substack{i,j\in R\\ i<j}}\frac{1}{ij} \equiv 0 \pmod{p^{2k}}$. این اثبات قضیه را کامل می‌کند. □

قضیه ۹.۴. فرض کنیم $p \geq 5$ عددی اول و $n = p^\ell$ باشد. دراین‌صورت

$$\binom{2n-1}{n-1} \equiv 1 \pmod{p^3}.$$

اثبات. با توجه به ۶.۴ داریم

$$\binom{2n}{n} \equiv \binom{2p^\ell}{p^\ell} \equiv \cdots \equiv \binom{2p}{p} \pmod{p^3}.$$

بنابراین $\binom{2n-1}{n-1} = \frac{1}{2}\binom{2n}{n} \equiv \frac{1}{2}\cdot 2 \equiv 1 \pmod{p^3}$. □

قضیه ولستن‌هولم برای p^4 مورد بررسی قرارگرفت. قضیه زیر حالت $n = p^\ell$ را مورد بررسی قرار می‌دهد.

قضیه ۱۰.۴. فرض کنیم $p \geq 5$ عددی اول و $n = p^\ell$ عددی طبیعی باشد. در این‌صورت

$$\binom{2n-1}{n-1} \equiv \binom{2p-1}{p-1} \pmod{p^4}.$$

اثبات. چون p عدد اول فردی می‌باشد کافی است نشان دهیم $\binom{۲n}{n} \equiv \binom{۲p}{p} \pmod{p^۴}$. با استفاده از قضیه واندرموند داریم:

$$\binom{۲n}{n} = \sum_{j=۰}^{n} \binom{n}{j}^۲ = ۲ + \sum_{j=۱}^{p^{\ell}-۱} \binom{p^{\ell}}{j}^۲.$$

اگر $p^{\ell-۱} \nmid j$، بنابر لم ۱.۴، $p^۲ \mid \binom{p^{\ell}}{j}$، بنابراین $p^۴ \mid \binom{p^{\ell}}{j}^۲$. لذا

$$\binom{۲n}{n} \equiv ۲ + \sum_{j=۱}^{p-۱} \binom{p^{\ell}}{jp^{\ell-۱}}^۲ \pmod{p^۴}.$$

برای $\ell \geq ۳$ و $k = ۲$ با توجه به لم ۸.۴،

$$\binom{p^{\ell}}{jp^{\ell-۱}} \equiv \binom{p^k p^{\ell-۲}}{p^{k-۱} jp^{\ell-۳}} \equiv \binom{p^{\ell-۱}}{jp^{\ell-۲}} \pmod{p^۶}.$$

با استفاده مجدد لم ۸.۴ برای $\ell - ۳$ داریم:

$$\binom{p^{\ell}}{jp^{\ell-۱}} \equiv \binom{p^۲}{jp} \pmod{p^۶}.$$

بنابراین

$$\binom{۲n}{n} \equiv ۲ + \sum_{j=۱}^{p-۱} \binom{p^۲}{jp}^۲ \pmod{p^۴}.$$

از طرفی

$$\begin{aligned}
\binom{p^۲}{jp} &= \binom{p}{j} \prod_{\substack{۱ \leq i \leq jp \\ p \mid i}} \frac{p^۲ - i}{i} \\
&= \binom{p}{j} (-۱)^{jp-j} \prod_{\substack{۱ \leq i \leq jp \\ p \mid i}} (۱ - \frac{p^۲}{i}) \\
&\equiv \binom{p}{j} (-۱)^{j(p-۱)} (۱ - p^۲ \sum_{\substack{۱ \leq i \leq jp \\ p \mid i}} \frac{۱}{i}) \\
&\equiv \binom{p}{j} \pmod{p^۴}.
\end{aligned}$$

با استفاده از تبصره ۹.۲ و قرار دادن $m = jp$ و $k = ۱$ نتیجه به‌دست می‌آید. □

قضیه فوق برای محاسبه مقادیر $\binom{۲p-۱}{p-۱} \equiv ۱ \pmod{p}$ مهم می‌باشد. اعدادی که در رابطه فوق صدق کند را اعداد اول ولستن‌هولم[۴۰] گویند. تاکنون تنها دو عدد اول ولستن‌هولم ۱۶۸۴۳ در سال ۱۹۶۴ و ۲۱۲۴۶۷۹ در سال ۱۹۹۳ به‌دست آمده است. بنابراین قضیه قبل بیان می‌کند که اگر عدد اول p ولستن‌هولم نباشد آنگاه عکس قضیه ولستن‌هولم برای p برقرار می‌باشد. در [۲۲] نویسندگان مقدار $\binom{۲p-۱}{p-۱} \equiv ۱ \pmod{p^۴}$ را برای همه اعداد اول $p < ۲/۵ \times ۱۰^۸$ مورد بررسی قرار داده‌اند و در قضیه ۱۰.۴

[40] Wolstenholms prime

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

نشان دادند که عکس قضیه ولستن‌هولم به‌جز دو عدد اول ذکر شده برای تمامی توان‌های p درست می‌باشد. در هر صورت، نشان دادن اینکه قضیه ۱۰.۴ برای p^5 نیز درست می‌باشد سخت نیست.

۵. کارهای بیشتر

در [۱۵]، نویسنده حدس‌های زیر را مطرح کرده که صورت صحیح آن‌ها توسط نویسندگان این مقاله اثبات شده است [۱۸].

حدس ۱.۵ ([۱۵، حدس ۱]). فرض کنیم $p \geq ۳$ عددی اول باشد. در این‌صورت برای عدد طبیعی $n \geq ۱$ داریم

$$\binom{pn-۱}{p} \equiv n-۱ \pmod{p^۳}.$$

حدس ۲.۵ ([۱۵، حدس ۲]). برای عدد طبیعی n, ℓ و $k \equiv ۰, ۱ \pmod{۳}$ داریم

$$\binom{۳^\ell n-k}{۳} \equiv \lfloor \frac{۳^\ell n-k}{۳} \rfloor \pmod{۳^۲}.$$

حدس دوم را می‌توان به راحتی به‌صورت زیر توسیع داد:

حدس ۳.۵ ([۱۵، حدس ۳]). برای اعداد طبیعی n, ℓ، به‌طوری‌که $k \equiv ۰, ۱ \pmod{p}$ داریم

$$\binom{p^\ell n-k}{p} \equiv \lfloor \frac{p^\ell n-k}{p} \rfloor \pmod{p^۳}.$$

حدس‌های دوم و سوم حالت توسیع یافته نتیجه

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

می‌باشد. این نتیجه به راحتی با استفاده از قضیه لوکا ۵.۲ اثبات می‌شود. البته نتیجه فوق را می‌توان به‌صورت ابتکاری اثبات کرد. فرض کنیم $n = pq + r$ که $۰ \leq r \leq p$. بنابراین $q = \lfloor \frac{n}{p} \rfloor$. لذا

$$\begin{aligned}
\binom{n}{p} &= \frac{(pq+r)!}{p!(pq+r-p)!} \\
&= \frac{۱}{p!} \prod_{t=۰}^{p-۱} (pq+r-i) \\
&= \frac{pq}{p!} \prod_{\substack{۰ \leq t \leq p \\ t \neq r}} (pq+r-i) \\
&= \frac{q}{(p-۱)!} \prod_{\substack{۰ \leq t \leq p \\ t \neq r}} (pq+r-i).
\end{aligned}$$

مجموعه $\{pq+r-i \mid ۰ \leq i < p; i \neq r\}$ تشکیل یک دستگاه مخفّف مانده‌ها به پیمانه p می‌دهد. بنابراین $\prod_{\substack{۰ \leq t \leq p \\ t \neq r}} (pq+r-i) \equiv (p-۱)! \pmod{p}$. با استفاده از قضیه ویلسون ۳.۲، $\binom{n}{p} \equiv q(-۱)(-۱) = q \pmod{p}$.

حدس دوم ۲.۵ به راحتی و با یک محاسبه ساده به‌صورت زیر قابل حل می‌باشد.

$$\begin{aligned}\binom{n\mathbb{3}^{\ell}-k}{\mathbb{3}} &= \frac{(n\mathbb{3}^{\ell}-k)(n\mathbb{3}^{\ell}-k-\mathbb{1})\cdots(n\mathbb{3}^{\ell}-k-(\mathbb{3}-\mathbb{1})}{\mathbb{1}\times\mathbb{2}\times\cdots\times\mathbb{3}}\\ &= (\frac{n\mathbb{3}^{\ell}-k}{\mathbb{3}})(\frac{n\mathbb{3}^{\ell}-k}{\mathbb{1}}-\mathbb{1})(\frac{n\mathbb{3}^{\ell}-k}{\mathbb{2}}-\mathbb{1})\cdots(\frac{n\mathbb{3}^{\ell}-k}{\mathbb{3}-\mathbb{1}}-\mathbb{1})\\ &= (\frac{n\mathbb{3}^{\ell}-k}{\mathbb{3}})\sum_{i=\mathbb{0}}^{\mathbb{3}-\mathbb{1}}(-\mathbb{1})^{i}(n\mathbb{3}^{\ell}-k)^{i}H_{i}(\mathbb{3}-\mathbb{1})\\ &\equiv \lfloor\frac{\mathbb{3}^{\ell}n-k}{\mathbb{3}}\rfloor \pmod{\mathbb{3}^{\mathbb{2}}}.\end{aligned} \tag{۱۴}$$

در [۱۸]، نویسندگان حدس ۳.۵ را برای حالت $p^{\mathbb{4}}$ با نرم افزار متمتیکا مورد بررسی قرار داده‌اند، اما هنوز نتوانسته‌اند صورت کلی آن‌را حدس بزنند. به‌عنوان مثال برای حالت $p=\mathbb{7},\ell=\mathbb{3}$ و $k=\mathbb{14}$ داریم

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

ظاهراً مقدار عبارت فوق به تجزیه عدد n به اعداد اول وابسته می‌باشد. این سؤال را می‌توان برای توان‌های بیشتر p نیز مطرح کرد.

اعداد استرلینگ نوع دوم[41] $\left\{{n\atop k}\right\}$ برابر با تعداد افرازهای یک مجموعه n عضوی به k زیر مجموعه غیرتهی می‌باشد. محاسبه حدس ۳.۵ برای این اعداد و اعداد استرلینگ نوع اول نیز مسئله پژوهشی جذابی می‌باشد. یعنی

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

صورت کلی قضیه ولستن‌هولم را می‌توان به‌صورت زیر نیز بیان کرد:

حدس ۴.۵. به ازای چه مقادیری از m,n، معادله همنهشتی

$$\binom{np-\mathbb{1}}{mp-\mathbb{1}}\equiv\mathbb{1}\pmod{p^{\mathbb{3}}} \tag{۱۵}$$

برقرار می‌باشد.

حل کلی این سؤال ساده نیست، اما بررسی حالت‌های خاص n,m نباید سخت باشد.

حدس ۵.۵. فرض کنید n عدد طبیعی و p عددی اول باشد. در این‌صورت

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

برای هر $\mathbb{1}\le i\le p^{\ell+\mathbb{2}}$ داریم

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

[41] Stirling numbers of the second kind

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

مراجع

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

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

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

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

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

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

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

[22] 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.

[۲۳] م. میرزاوزیری، شمردنی‌ها را بشمارید، انتشارات سخن‌گستر، ۱۳۸۶.

دانیال یعقوبی
گروه کامپیوتر، مجتمع آموزش عالی تربت‌جام ، تربت‌جام، ایران
yaqubi@tjamcaas.ac.ir

دانیال یعقوبی متولد بهمن ماه ۱۳۶۵ در شهر تربت‌جام یکی از شهرستان‌های خراسان رضوی می‌باشد. وی در سال ۱۳۸۳ وارد مقطع کارشناسی رشته ریاضی محض دانشگاه فردوسی مشهد گردید و در سال ۱۳۸۷ از رساله ارشد خود دفاع کرد. وی دکتری خود را نیز در دانشگاه فردوسی سال ۱۳۹۱ در گرایش گراف و ترکیبیات جبری تحت سرپرستی دکتر مجید میرزاوزیری آغاز کرد و در سال ۱۳۹۶ از رساله دکتری خود تحت عنوان افرازهای ضربی دفاع کرد. وی هم‌اکنون عضو هیئت علمی دانشگاه تربت جام می‌باشد و زمینه‌های تحقیقاتی ایشان ترکیبیات شمارشی و نظریه مقدماتی اعداد است.

مجید میرزاوزیری
گروه ریاضی و کامپیوتر، دانشکده ریاضی، دانشگاه فردوسی، مشهد، ایران
mirzavaziri@um.ac.ir

مجید میرزاوزیری زاده ۹ اسفند ۱۳۵۰ در تهران می‌باشد. وی استاد تمام گروه ریاضی محض و گروه مهندسی کامپیوتر دانشگاه فردوسی مشهد و همچنین بنیانگذار شهر ریاضی است. وی مدرک دکتری خودش در ریاضیات محض را از دانشگاه فردوسی مشهد دریافت کرده است. دکتر مجید میرزاوزیری از سال ۱۳۹۸ تا ۱۴۰۲ رئیس گروه آموزش‌های آزاد (کالج دانشگاه فردوسی) نیز بوده است.

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