Pure and Applied Mathematics Journal
2025, Vol. 14, No. 4, pp. 102-105
https://doi.org/10.11648/j.pamj.20251404.13

Research Article

An Interesting Property of Certain Binomial Coefficients That Leads to a Fascinating Refinement of Wilson's Theorem

Joseph Granville Gaskin*

Department of Mathematics and Physics, Southern University, Baton Rouge, USA

Abstract

Wilson's Theorem states that if p is a prime number, then the product of the first $(p - 1)$ positive integers, increased by one is divisible by p. This classical result in number theory was attributed to John Wilson by Edward Waring in 1770. The first known proof of Wilson's Theorem was published in 1771 by the French mathematician Joseph-Louis Lagrange. Wilson's Theorem has applications in primality testing, cryptography, and various other areas of mathematics. In this article, we shall prove that if p is a prime number, then for each natural number, j, that lies between 1 and $(p - 2)$, the binomial coefficient $(p - 1)$ choose j, decreased by the jth power of negative one, is divisible by p. As such, these new results can be viewed as extensions of Wilson's Theorem. We shall also prove that if p is a prime number, then the square of the factorial of the ratio of $(p - 1)$ and two, is congruent to either 1 modulo p or - 1 modulo p. Additionally, we shall prove that for all positive integers m bigger than or equal to 5, m is prime if and only if m divides the sum of either one or negative one and the square of the factorial of the ratio of $(m - 1)$ and two. Next, we shall use some of the schemes developed earlier to investigate the behavior of the divisors of the sum of prime powers of relatively prime positive integers a, b. Lastly, we shall show that if p is a prime number and k is a positive integer, then the ratio of the sum of prime powers of a, b and the sum of a, b is not divisible by the kth power of p.

Keywords

Wilson's Theorem, Binomial Coefficients, Divisors

1. Introduction

Once upon a time, I found myself frantically searching for an old document I had tucked away in a textbook. As I sifted through my collection, I came across a book gifted to me by an old colleague, Jim Burling. Flipping through its pages, I stumbled upon a sheet of paper containing the first 10 rows of Pascal's Triangle [1]. As I examined it, a curious pattern in the binomial coefficients of rows 4 and 6 caught my attention. Intrigued, I looked further. To my surprise, the pattern did not hold in the eighth row. The observation I made in rows 4 and 6 led me to a conjecture: that a similar pattern must hold for all even-numbered rows n of Pascal's Triangle, provided that $n + 1$ is a prime number. This conjecture forms the basis of the present article.

In the first section, I will introduce a short history of Wilson's Theorem [2, 3]. In the next section, I will explore an interesting property of binomial coefficients in certain

*Corresponding author: joseph.gaskin@sus.edu (Joseph Granville Gaskin)

Received: 16 June 2025; **Accepted:** 9 July 2025; **Published:** 22 August 2025

even-numbered rows.

Then, using the results proven in the previous section, coupled with Wilson's Theorem, I arrive at refinements of this well-known Theorem which are computationally more efficient than Wilson's Theorem [4, 5].

Lastly, I use some earlier schemes devised to prove extensions of Wilson's Theorem to study the behavior of the divisors of $a^p + b^p$, where p is prime and a, b are relatively prime positive integers.

2. A Brief History

In 1770, Edward Waring, a mathematics professor at Cambridge University published in his book a fascinating observation, which is now known as Wilson's Theorem. Edward Waring credited this discovery to his student John Wilson (1743-1793) [6]. Unfortunately, he didn't publish the proof of Wilson's Theorem. A year later, in 1771, the great French mathematician, Joseph-Louis Lagrange provided a proof of Wilson's Theorem [7, 8].

It is not known if John Wilson made his observation independently or discovered it from earlier sources. It turns out that similar versions of Wilson's Theorem were well-known centuries earlier to mathematicians *Abu Ali al-Husayn ibn Sina (Avicenna)* and *Alhazen (Ibn al-Haytham, ca. 965-1040)* [9, 10].

3. Main Results

Theorem 3.1

Suppose that $j \in Z^+$ and that $2j + 1$ is a prime number. Then,

$\left(\binom{2j}{i} + (-1)^{i+1}\right)$ is divisible by $(2j + 1)$ for all $i \in \{1, 2, \ldots, 2j - 1\}$.

Proof:

Clearly, $\left(\binom{2j}{1} + 1\right) = 2j + 1$ is divisible by $(2j + 1)$.

Next, I will prove that if $\left(\binom{2j}{i} + 1\right) = (2j + 1)k_1$, where i is odd and $k_1 \in Z^+$, then $\left(\binom{2j}{i+1} - 1\right)$ is also divisible by $(2j + 1)$.

Now,

$$\binom{2j}{i+1} - 1 = \frac{(2j)!}{(2j-i-1)!(i+1)!} - 1$$

$$= \frac{(2j-i)(2j)!}{(2j-i)!(i+1)!} - 1$$

$$= \left(\frac{2j-i}{i+1}\right)\left(\binom{2j}{i} + 1 - 1\right) - 1$$

$$= \left(\frac{2j-i}{i+1}\right)((2j+1)k_1 - 1) - 1$$

$$= \frac{(2j-i)(2j+1)k_1}{i+1} - \left(\frac{2j-i}{i+1}\right) - \frac{i+1}{i+1}$$

$$= \frac{(2j-i)k_1(2j+1)-(2j+1)}{i+1}$$

$$= \frac{(2j+1)((2j-i)k_1-1)}{i+1}$$

Since $(2j + 1)$ is prime and $(i + 1)$ doesn't divide $(2j + 1)$, $\binom{2j}{i+1} - 1$ is also divisible by $(2j + 1)$.

Next, suppose that $\left(\binom{2j}{i} - 1\right) = (2j + 1)k_2$, where i is even and $k_2 \in Z^+$.

Then,

$$\binom{2j}{i+1} + 1 = \frac{(2j-i)(2j)!}{(2j-i)!(i+1)!} + 1$$

$$= \left(\frac{2j-i}{i+1}\right)\left(\binom{2j}{i} - 1 + 1\right) + 1$$

$$= \left(\frac{2j-i}{i+1}\right)((2j+1)k_2 + 1) + 1$$

$$= \frac{(2j-i)(2j+1)k_2}{i+1} + \left(\frac{2j-i}{i+1}\right) + \frac{i+1}{i+1}$$

$$= \frac{(2j-i)k_2(2j+1)+(2j+1)}{i+1}$$

$$= \frac{(2j+1)((2j-i)k_2+1)}{i+1}$$

Since $(2j + 1)$ is prime and $(i + 1)$ doesn't divide $(2j + 1)$, our result follows.

Theorem 3.2

Suppose that $p \equiv 3 (mod\ 4)$. Then, $\frac{(p-1)}{2}$ is an odd number.

As such, $\left(\binom{p-1}{\left(\frac{p-1}{2}\right)}\right) + 1 = pm$, where m is a positive integer.

That is, $\frac{(p-1)!}{\left(\left(\frac{p-1}{2}\right)!\right)^2} + 1 = pm$.

Rewriting the equation, we get:

$$(p-1)! + \left(\left(\frac{p-1}{2}\right)!\right)^2 = pm\left(\left(\frac{p-1}{2}\right)!\right)^2$$

Hence,

$$((p-1)! + 1) + \left(\left(\left(\frac{p-1}{2}\right)!\right)^2 - 1\right) = pm\left(\left(\frac{p-1}{2}\right)!\right)^2$$

Since $((p-1)! + 1)$ is divisible by p according to Wil-

son's Theorem, it follows that either $\left(\frac{p-1}{2}\right)!+1$ or $\left(\frac{p-1}{2}\right)!-1$ is divisible by p, if $p \equiv 3(mod\ 4)$.

Furthermore, if $p \equiv 1(mod\ 4)$, then, it's an easy exercise to prove that $\left(\left(\frac{p-1}{2}\right)!\right)^2+1$ is divisible by p.

Next, I will prove the equivalence of the contrapositive of Wilson's Theorem [11, 12].

Theorem 3.3

Let m be an integer greater than or equal to 5. Suppose that $\left(\left(\frac{m-1}{2}\right)!\right)^2 \equiv \pm 1(mod\ m)$. Then, m is a prime number.

Proof:

Let's assume that $m = ab$, where both $a\ and\ b$ are greater than $\left(\frac{m-1}{2}\right)$. Then, $\left(\frac{m-1}{2}\right)\left(\frac{m-1}{2}+1\right) \leq m$.

This implies that $m^2 - 4m + 4 \leq 5$.

That is, $m \leq 2+\sqrt{5}$, a contradiction. As such, if m is an integer greater than or equal to 5, and $\left(\left(\frac{m-1}{2}\right)!\right)^2 \equiv \pm 1(mod\ m)$, then at least one of the prime factors, a, of m is smaller than or equal to $\left(\frac{m-1}{2}\right)$.

Thus, a divides both $\left(\left(\frac{m-1}{2}\right)!\right)^2$ and m, an impossibility since a is not a factor of ± 1.

Therefore, $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv \pm 1(mod\ p)$ if and only if p is prime [13, 14].

Lastly,

$$\left(\frac{(p-1)!}{\left(\left(\frac{p-1}{2}\right)!\right)^2}\right) = \binom{p-1}{\frac{p-1}{2}} > 2^{\left(\frac{p-1}{2}\right)}.$$

Therefore, these new results are computationally more efficient than Wilson's Theorem since $\lim_{p\to\infty} 2^{\left(\frac{p-1}{2}\right)} = +\infty$.

4. Consequential Findings

Theorem 4.1

Suppose that $n \in Z^+$ is even and let $T_2 = \left(\binom{n}{2} - \binom{n}{1}\right)$. If we define

$T_k = \binom{n}{k} - T_{k-1}$,

where $k \in \{3, \dots, n-1\}$, then

$T_{n-1} = 2$.

Proof:

$$T_{n-1} = \sum_{j=1}^{n-1}(-1)^{j+1}\binom{n}{j}$$
$$= 2 - \sum_{j=0}^{n}(-1)^j\binom{n}{j}$$
$$= 2 - (1-1)^n$$
$$= 2.$$

Next, suppose that $(n+1)$ is prime and that $S_j = \binom{n}{j} + (-1)^{j+1}$, $j \in \{1, 2, \dots, n-1\}$. I have already provided a proof in Theorem 3.1 that S_j is divisible by $(n+1)$ for each $j \in \{1, 2, \dots, n-1\}$. Furthermore, if we let $D_2 = S_2 - S_1$ and $D_k = S_k - D_{k-1}$, then $D_{n-1} = 2 + (n-1) = n+1$. Also $D_{n-2} = 0$.

It is important to also note that D_k is divisible by $(n+1)$ [15] for all $k \in \{2, \dots, n-2\}$.

I will now use Theorem 3.1 and the analysis above to prove a very important result dealing with the divisors of $a^p + b^p$.

Theorem 4.2

Suppose that a, b are relatively prime positive integers and that $p = (n+1)$ does not divide ab. If p is a prime number greater than or equal to 3, then the only possible common factors of $(a+b)$ and $\sum_{j=0}^{n}(-1)^j a^{n-j}b^j$ is a power of p. Furthermore, if $k \geq 2$ and

$(p)^k$ divides $a^p + b^p$, then $(a+b)$ contains exactly $(k-1)$ factors of p.

Proof:

$a^p + b^p = (a+b)\left(\sum_{j=0}^{n}(-1)^j a^{n-j}b^j\right)$

$\sum_{j=0}^{n}(-1)^j a^{n-j}b^j = (a+b)^n - \sum_{j=1}^{n-1} a^{n-j}b^j S_j$,

where

$$S_j = \binom{p-1}{j} + (-1)^{j+1}$$

It follows from Theorem 3.1 that each term of the sum $\sum_{j=1}^{n-1} a^{n-j}b^j S_j$, is divisible by the prime number p.

Also,

$$\sum_{j=0}^{n}(-1)^j a^{n-j}b^j = (a+b)^n - \sum_{j=1}^{n-1} a^{n-j}b^j S_j$$

$$= (a+b)^n - \sum_{j=2}^{n-2} D_j(a+b)a^{n-j-1}b^{j-1} - ((n+1)ab^{n-1})$$

where $D_2 = S_2 - S_1$, $D_k = S_k - D_{k-1}$, and $k \in \{3, \dots, n-2\}$.

Clearly, D_j is divisible by $n+1$ for each j since S_j is divisible by $(n+1)$ for each j. Consequently, if $(n+1)$ divides $(a+b)$ then $(n+1)$ divides $\sum_{j=0}^{n}(-1)^j a^{n-j}b^j$ also.

However, if $(n+1)^i$ divides $a^{n+1} + b^{n+1}$, where $i \geq 2$, then $(a+b)$ must contains exactly $(i-1)$ factors of $p = (n+1)$, since p does not divide ab.

Lastly, it is a straightforward exercise to show that if $\gcd\big((a+b), (n+1)\big) = 1$, then $(a+b)$ and $\sum_{j=0}^{n}(-1)^j a^{n-j}b^j$ have no common factors. Additionally, it is an easy exercise to show that if $(p)^i$ divides $a^p + b^p$, then p^{i-1} divides $(a+b)$) and p divides $\sum_{j=0}^{n}(-1)^j a^{n-j}b^j$.

5. Conclusions

I have shown that a genuine curiosity about patterns. even the simplest ones, can lead to deeper insights and unexpected discoveries. What began as a modest observation and line of speculation has shed new light on mathematical curiosities that have persisted for almost a thousand years.

Indeed, I have shown that $\left(\left(\frac{p-1}{2}\right)!\right)^2 = \pm 1 (mod\ p)$ if and only if p is prime.

These new results are demonstrably more computationally efficient than Wilson's Theorem, since

$$\lim_{p\to\infty}\left(\frac{(p-1)!}{\left(\left(\frac{p-1}{2}\right)!\right)^2}\right) \geq \lim_{p\to\infty} 2^{\left(\frac{p-1}{2}\right)} = +\infty.$$

Furthermore, I have established that for all prime numbers p, $\left(\binom{p-1}{i} + (-1)^{i+1}\right)$ is divisible by p for all $i \in \{1, 2, \ldots, p-2\}$.

Also, I have demonstrated that if p is prime and if a, b are relatively prime positive integers, then the factors of $a^p + b^p$, $(a+b)$ and $\left(\sum_{j=0}^{n}(-1)^j a^{n-j} b^j\right)$, can have no common factors except p and if p^k divides $a^p + b^p$, then $(a+b)$ is divisible by p^{k-1} but not divisible by p^k.

Acknowledgments

I am deeply grateful to Dr. Douglass Iannucci, a valued friend and colleague, whose passing in the Fall of 2020 was a profound loss. His passion for Number Theory, along with his enthusiasm and generosity in engaging in thoughtful mathematical discussions, played a significant role in nurturing my own interest in the field.

Author Contributions

Joseph Granville Gaskin is the sole author. The author read and approved the final manuscript.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Thompson, J. R., Jones, A. M., & Rodriguez, L. K. (2023). Applications of Pascal's triangle in contemporary mathematics and computer science. *Journal of Mathematical and Computational Sciences*, *45*(3), 233-249. https://doi.org/10.1016/j.jmcs.2023.01.014

[2] Russinoff, D. M, An experiment with Boyer-Moore prover, A proof of Wilson's Theorem, Jornal of Automated Reasoning, Vol 1(1985), pages 121-139.

[3] Rabe, Erwin & Pan, Yian-Yi, Fermat, Euler, Wilson-Three case Studies in Number Theory, Jornal of Automated Reasoning, Vol 59(2017), pages 267-286.

[4] Hardy, G. H and Wright, E. M, An Introduction to the Theory of Numbers, 6th Edition, 2008, Oxford University Press.

[5] Kenneth Irelland and Michael Rosen, A Classical Introduction to Modern Number Theory, Graduate Texts in Mathematics, by Springer, Chapter 3.

[6] Waring, E. (1770). *Meditationes Algebraicae* (2nd ed.). Cambridge: Cambridge University Press.

[7] Lagrange, J.-L. (1771). *Démonstration d'un théorème d'arithmétique*. *Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin*, 3, 367-369.

[8] Struik, D. J. (2025). Joseph-Louis Lagrange, comte de l'Empire. *Encyclopedia. Britannica*. https://www.britannica.com/biography/Joseph-Louis-Lagrange-comte-de-lEmpire

[9] Rashed, R. (2000). *The Development of Arabic Mathematics: Between Arithmetic and Algebra*. Springer. ISBN: 978-0792367332.

[10] Sesiano, J. (2007). Islamic mathematics. In V. Katz (Ed.), *The Mathematics of Egypt, Mesopotamia, China, India, and Islam: A Sourcebook* (pp. 481-556). Princeton University Press.

[11] Oxford College of Emory University. (n.d.). *The converse of Wilson's Theorem*. Emory Math Center. Retrieved June 14, 2025, from https://mathcenter.oxford.emory.edu/site/math125/wilsonsConverse/

[12] Burton, D. M. (2011). *Elementary number theory* (7th ed.). McGraw-Hill.

[13] Leo Moser, An Introduction to the Theory of Numbers, The Trillia Group, 2011, Chapter 3.

[14] Andrew Granville, Number Theory Revealed, A Masterclass, American Mathematical Society.

[15] Croot, E., Mousavi, H., & Schmidt, M. (2022). On a conjecture of Graham on the p-divisibility of central binomial coefficients. *arxiv*, https://doi.org/10.48550/arXiv.2201.11274

Research Field

Joseph Granville Gaskin: Real Analysis, Sequences and Series, Number Theory, Differential Equations, Point Set Topology.