Wolstenholme's theorem

In mathematics, **Wolstenholme's theorem** states that for a prime number $p \geq 5$, the congruence

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

holds, where the parentheses denote a binomial coefficient. For example, with $p = 7$, this says that 1716 is one more than a multiple of 343. The theorem was first proved by Joseph Wolstenholme in 1862. In 1819, Charles Babbage showed the same congruence modulo p^2, which holds for $p \geq 3$. An equivalent formulation is the congruence

$$\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^3}$$

for $p \geq 5$, which is due to Wilhelm Ljunggren[1] (and, in the special case $b = 1$, to J. W. L. Glaisher) and is inspired by Lucas's theorem.

No known composite numbers satisfy Wolstenholme's theorem and it is conjectured that there are none (see below). A prime that satisfies the congruence modulo p^4 is called a **Wolstenholme prime** (see below).

As Wolstenholme himself established, his theorem can also be expressed as a pair of congruences for (generalized) harmonic numbers:

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1} \equiv 0 \pmod{p^2}\text{, and}$$
$$1+\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{(p-1)^2} \equiv 0 \pmod{p}.$$

since

$$\binom{2p-1}{p-1} = \prod_{1\leq k\leq p-1} \frac{2p-k}{k} \equiv 1 - 2p \sum_{1\leq k\leq p-1} \frac{1}{k} \pmod{p^2}$$

(Congruences with fractions make sense, provided that the denominators are coprime to the modulus.) For example, with p=7, the first of these says that the numerator of 49/20 is a multiple of 49, while the second says the numerator of 5369/3600 is a multiple of 7.

Wolstenholme primes

A prime p is called a Wolstenholme prime iff the following condition holds:

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

If p is a Wolstenholme prime, then Glaisher's theorem holds modulo p^4. The only known Wolstenholme primes so far are 16843 and 2124679 (sequence A088164 in the OEIS); any other Wolstenholme prime must be greater than 10^{11}.[2] This result is consistent with the heuristic argument that the residue modulo p^4 is a pseudo-random multiple of p^3. This heuristic predicts that the number of Wolstenholme primes between K and N is roughly $\ln \ln N - \ln \ln K$. The Wolstenholme condition has been checked up to 10^{11}, and the heuristic says that there should be roughly one Wolstenholme prime between 10^{11} and 10^{24}. A similar heuristic predicts that there are no "doubly Wolstenholme" primes, for which the congruence would hold modulo p^5.

A proof of the theorem

There is more than one way to prove Wolstenholme's theorem. Here is a proof that directly establishes Glaisher's version using both combinatorics and algebra.

For the moment let p be any prime, and let a and b be any non-negative integers. Then a set A with ap elements can be divided into a rings of length p, and the rings can be rotated separately. Thus, the a-fold direct sum of the cyclic group of order p acts on the set A, and by extension it acts on the set of subsets of size bp. Every orbit of this group action has p^k elements, where k is the number of incomplete rings, i.e., if there are k rings that only partly intersect a subset B in the orbit. There are $\binom{a}{b}$ orbits of size 1 and there are no orbits of size p.[3] Thus we first obtain Babbage's theorem

$$\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^2}.$$

Examining the orbits of size p^2, we also obtain

$$\binom{ap}{bp} \equiv \binom{a}{b} + \binom{a}{2}\left(\binom{2p}{p} - 2\right)\binom{a-2}{b-1} \pmod{p^3}.$$

Among other consequences, this equation tells us that the case $a=2$ and $b=1$ implies the general case of the second form of Wolstenholme's theorem.

Switching from combinatorics to algebra, both sides of this congruence are polynomials in a for each fixed value of b. The congruence therefore holds when a is any integer, positive or negative, provided that b is a fixed positive integer. In particular, if $a=-1$ and $b=1$, the congruence becomes

$$\binom{-p}{p} \equiv \binom{-1}{1} + \binom{-1}{2}\left(\binom{2p}{p} - 2\right) \pmod{p^3}.$$

This congruence becomes an equation for $\binom{2p}{p}$ using the relation

$$\binom{-p}{p} = \frac{(-1)^p}{2}\binom{2p}{p}.$$

When p is odd, the relation is

$$3\binom{2p}{p} \equiv 6 \pmod{p^3}.$$

When $p \neq 3$, we can divide both sides by 3 to complete the argument.

A similar derivation modulo p^4 establishes that

$$\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^4}$$

for all positive a and b if and only if it holds when $a=2$ and $b=1$, i.e., if and only if p is a Wolstenholme prime.

The converse as a conjecture

It is conjectured that if

(1)

when $k=3$, then n is prime. The conjecture can be understood by considering $k = 1$ and 2 as well as 3. When $k = 1$, Babbage's theorem implies that it holds for $n = p^2$ for p an odd prime, while Wolstenholme's theorem implies that it holds for $n = p^3$ for $p > 3$, and it holds for $n = p^4$ if p is a Wolstenholme prime. When $k = 2$, it holds for $n = p^2$ if p is a Wolstenholme prime. These three numbers, $4 = 2^2$, $8 = 2^3$, and $27 = 3^3$ are not held for (1) with $k = 1$, but all other prime square and prime cube are held for (1) with $k = 1$. Only 5 other composite values (neither prime square nor prime cube) of n are known to hold for (1) with $k = 1$, they are called **Wolstenholme pseudoprimes**, they are

> 27173, 2001341, 16024189487, 80478114820849201, 20378551049298456998947681, ... (sequence A082180 in the OEIS)

The first three are not prime powers (sequence A228562 in the OEIS), the last two are 16843^4 and 2124679^4, 16843 and 2124679 are Wolstenholme primes (sequence A088164 in the OEIS). Besides, with an exception of 16843^2 and 2124679^2, no composites are known to hold for (1) with $k = 2$, much less $k = 3$. Thus the conjecture is considered likely because Wolstenholme's congruence seems over-constrained and artificial for composite numbers. Moreover, if the congruence does hold for any particular n other than a prime or prime power, and any particular k, it does not imply that

$$\binom{an}{bn} \equiv \binom{a}{b} \pmod{n^k}.$$

The number of Wolstenholme pseudoprimes up to x is $O(x^{1/2}\log(\log(x))^{499712})$, so the sum of reciprocals of those numbers converges. The constant 499712 follows from the existence of only three Wolstenholme pseudoprimes up to 10^{12}. The number of Wolstenholme pseudoprimes up to 10^{12} should be at least 7 if the sum of its reciprocals diverged, and since this is not satisfied because there are only 3 of them in this range, the counting function of these pseudoprimes is at most $O(x^{1/2}\log(\log(x))^{C})$ for some efficiently computable constant C; we can take C as 499712. The constant in the big O notation is also effectively computable in $O(x^{1/2}\log(\log(x))^{499712})$.

Generalizations

Leudesdorf has proved that for a positive integer *n* coprime to 6, the following congruence holds:[4]

$$\sum_{\substack{i=1 \\ (i,n)=1}}^{n-1} \frac{1}{i} \equiv 0 \pmod{n^2}.$$

In 1900, Glaisher[5] [6] showed further that: for prime p>3,

$$\binom{2p-1}{p-1} \equiv 1 - \frac{2p^3}{3} B_{p-3} \pmod{p^4}.$$

Where B_n is the Bernoulli number.

See also

- Fermat's little theorem
- Wilson's theorem
- Wieferich prime
- Wilson prime
- Wall–Sun–Sun prime
- List of special classes of prime numbers
- Table of congruences

Notes

1. Granville, Andrew (1997), "Binomial coefficients modulo prime powers" (https://web.archive.org/web/20170202003812/http://www.dms.umontreal.ca/~andrew/PDF/BinCoeff.pdf) (PDF), *Canadian Mathematical Society Conference Proceedings*, **20**: 253–275, MR 1483922

(https://mathscinet.ams.org/mathscinet-getitem?mr=1483922) , archived from the original (http://www.dms.umontreal.ca/%7Eandrew/PDF/BinCoeff.pdf) (PDF) on 2017-02-02

2. Booker, Andrew R.; Hathi, Shehzad; Mossinghoff, Michael J.; Trudgian, Timothy S. (2022-07-01). "Wolstenholme and Vandiver primes" (https://link.springer.com/article/10.1007/s11139-021-00438-3) . *The Ramanujan Journal*. **58** (3): 913–941. doi:10.1007/s11139-021-00438-3 (https://doi.org/10.1007%2Fs11139-021-00438-3) . ISSN 1572-9303 (https://search.worldcat.org/issn/1572-9303) .
3. See "Explanation of the Wolstenholme theorem proof" (https://math.stackexchange.com/questions/3031711/explanation-of-the-wolstenholme-theorem-proof) . for an explanation.
4. Leudesdorf, C. (1888). "Some results in the elementary theory of numbers" (https://zenodo.org/record/1447726) . *Proc. London Math. Soc*. **20**: 199–212. doi:10.1112/plms/s1-20.1.199 (https://doi.org/10.1112%2Fplms%2Fs1-20.1.199) .
5. 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.
6. 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.

References

- Babbage, C. (1819), "Demonstration of a theorem relating to prime numbers" (https://books.google.com/books?id=KrA-AAAAYAAJ&pg=PA46) , *The Edinburgh Philosophical Journal*, **1**: 46–49.
- Glaisher, J.W.L. (1900), "Congruences relating to the sums of products of the first n numbers and to other sums of products" (https://books.google.com/books?id=23KWAAAAMAAJ&pg=PA1) , *The Quarterly Journal of Pure and Applied Mathematics*, **31**: 1–35.
- Glaisher, J.W.L. (1900), "Residues of binomial-theorem coefficients with respect to p^3", *The Quarterly Journal of Pure and Applied Mathematics*, **31**: 110–124.
- Glaisher, J.W.L. (1900), "On the residues of the sums of products of the first p−1 numbers, and their powers, to modulus p^2 or p^3", *The Quarterly Journal of Pure and Applied Mathematics*, **31**: 321–353.
- Granville, Andrew (1997), "Binomial coefficients modulo prime powers" (https://web.archive.org/web/20170202003812/http://www.dms.umontreal.ca/~andrew/PDF/BinCoeff.pdf) (PDF), *Canadian Mathematical Society Conference Proceedings*, **20**: 253–275, MR 1483922 (https://mathscinet.ams.org/mathscinet-getitem?mr=1483922) , archived from the original (http://www.dms.umontreal.ca/%7Eandrew/PDF/BinCoeff.pdf) (PDF) on 2017-02-02.

- McIntosh, R. J. (1995), "On the converse of Wolstenholme's theorem" (http://matwbn.icm.edu.pl/ksiazki/aa/aa71/aa7144.pdf) (PDF), *Acta Arithmetica*, **71** (4): 381–389, doi:10.4064/aa-71-4-381-389 (https://doi.org/10.4064%2Faa-71-4-381-389) .
- R. Mestrovic, Wolstenholme's theorem: Its Generalizations and Extensions in the last hundred and fifty years (1862—2012) (https://arxiv.org/abs/1111.3057) .
- Wolstenholme, Joseph (1862), "On certain properties of prime numbers" (https://books.google.com/books?id=vL0KAAAAIAAJ&pg=PA35) , *The Quarterly Journal of Pure and Applied Mathematics*, **5**: 35–39.

External links

- The Prime Glossary: Wolstenholme prime (http://primes.utm.edu/glossary/page.php?sort=Wolstenholme)
- Status of the search for Wolstenholme primes (http://www.loria.fr/~zimmerma/records/Wieferich.status)