Wolstenholme-Jacobstahl Congruence, Wolstenholme's Theorem

Siddharth Srinivasan

December 11, 2018

Abstract

Wolstenholme showed that the numerator of the sum

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}...+\frac{1}{p-1}$$

when reduced is divisible by p^2 and the numerator of

$$1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}...+\frac{1}{(p-1)^2}$$

when reduced is divisible by p. As Wolstenholme himself proved, this same set of congruences can be expressed otherwise as

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

Charles Babbage also showed that congruence for modulo p^2. In this article, we present an elementary proof of this theorem and a few generalizations, along with its applications and extensions.

1 Introduction

Understanding the prime numbers has been the holy grail in number theory for a long time, probably since the time of Fermat, and one way that we get to know more about them are through congruences. Let's review a few congruences that may seem very familiar:

Theorem 1 (Fermat's Little Theorem)**.** *Let p be a prime and a be any integer. Then Fermat's Little Theorem says that*

$$a^p - a \equiv 0 \pmod{p}$$

We also have Wilson's theorem as follows

Theorem 2 (Wilson)**.** *Let p be a prime. Then,*

$$(p-1)! \equiv -1 \pmod{p}$$

In 1819, Charles Babbage came up with the following congruence:

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

which Wolstenholme later extended to modulo p^3 in 1862. We can also write this congruence modulo p itself, through Lucas's theorem [1].

Theorem 3 (Lucas)**.**

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod{p}$$

where

$$m = m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0$$

and

$$n = n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0$$

This immediately implies

$$\binom{np}{mp} \equiv \binom{n}{m} \pmod{p}$$

Now, setting $n = 2, m = 1$ yields the congruence modulo p.

2 Wolsenholme's Theorem and its Generalizations and Extensions

Theorem 4. *For a prime $p > 3$, the following congruence*

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

holds. This can also be expressed as

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

.

Wolstenholme initially asserted that the numerator of the sum

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} ... + \frac{1}{p-1}$$

when reduced is divisible by p^2 and

$$1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} ... + \frac{1}{(p-1)^2}$$

when reduced is divisible by p. From here, it is easy to see that the binomial coefficient $\binom{2p-1}{p-1}$ satisfies the above congruence. Thus, we will prove Wolstenholme's Theorem as follows:

Proof. Here, we will use the alternate harmonic version above. We want to prove that for any prime $p > 4$ then when

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} ... + \frac{1}{p-1}$$

is reduced, the numerator is divisible by p^2.

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

, so it is sufficient to show that

$$\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i(p-i)} \equiv 0 \pmod{p}$$

We know that in $\pmod{p}$, $\frac{1}{i(p-i)} \equiv -\frac{1}{i^2} \pmod{p}$.Now, because of unique inverses, we have $\sum_{i=1}^{\frac{p-1}{2}} i^2 \equiv 0 \pmod{p}$, and so this is just sum of squares until p, which is $0 \pmod{p}$ □

There is also a beautiful proof by means of a combinatorial argument as follows [2]:

Proof. We would like to show that

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

. Let p be any prime, and and choose a, b as any nonnegative integers, with $a \geq b$. We can then construct a set X with ap elements. Consider the cyclic group of order p, which is isomorphic to $\mathbb{Z}_p$. We can model this as separating X into a subsets of p elements each, and the cyclic group is the act of rotating each of those subsets. Then we can describe it as a group action on the set A ,and any subset of size bp. Then we obtain the theorem by examining the orbit lengths.

□

2.1 Extensions to other powers

Glasier in 1900 [3] extended the p^3 case to p^4 with the following, of which Wolstenholme's Theorem is a special case:

Theorem 5 (Glasier)**.**

$$\binom{2p-1}{p-1} \equiv 1 - 2p\sum_{i=1}^{p-1}\frac{1}{i} \pmod{p^4}$$

Then, Macintosh established the following for the 5th power:

Theorem 6 (Macintosh)**.**

$$\binom{2p-1}{p-1} \equiv 1 - p^2\sum_{i=1}^{p-1}\frac{1}{i^2} \pmod{p^5}$$

3 Congruences in relation to the Bernoulli Numbers

The Bernoulli numbers defined based on the following generating function,

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

We can see that the first few terms of the Bernoulli numbers are. $B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_3 = -\frac{1}{30}, B_n = 0$ for odd $n > 2$. Glasier's congruence above may be written as:

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

for primes $p > 6$ Glasier generalized this as:

$$\binom{np-1}{p-1} \equiv 1 - \frac{1}{3}n(n-1)p^3 B_{p-3} \pmod{p^4}$$

Similarly, Macintosh's congruence can also be written as such:

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

for $p > 6$.

4 Other Wolstenholme Type Harmonic Congeunces

We shall continue with other Wolstenholme type congruences, this type more of the form of the harmonic sum formulation. Let's quickly restate Wolstenholme's assertion, that for any prime $p \geq 5$ the following two congruences hold:

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} ... + \frac{1}{p-1}$$

$$1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} ... + \frac{1}{(p-1)^2}$$

Alkan [4] came up with a similar fomulation(From which the congruences above can be deduced)

$$\sum_{k=1}^{p-1}\frac{1}{k} \equiv -\frac{1}{3}p^2 B_{p-3} \pmod{p^3}$$

Another generalization of Wolstenholme's assertion is the following due to Carlitz [5]:

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

5 Wolstenholme Primes

We define a prime to be a Wolstenholme Prime if it satisfies the Wolstenholme-Jacobstaal Congruence modulo p^4, namely if

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

From this, we can see that the Wolstenholme Quotient has to be divisible by p, or

$$W_p = -\frac{2}{3}B_{p-3}$$

, by a special case of Glasier's Bernoulli. Thus we get the statement that a prime is Wolstenholme iff it is divides the numerator of B_{p-3}, a beautiful result. This is also equivalent to the result that the numerator of $\sum_{k=1}^{p-1}\frac{1}{k}$ is divisible by p^3, and that the numerator $\sum_{k=1}^{p-1}\frac{1}{k^2}$ is divisible by p^2. Only two Wolstenholme primes have been discovered so far, and they are by no means trivial, they are 16843 and 2124679, however, Macintosh [6] established the bound that there is no other prime less than $5 * 10^8$.

6 q-analogues of similar congruences

Consider the generalized Harmonic number sequence, which is defined as the following:

$$H_a^b = \sum_{k=1}^{a}\frac{1}{k^b}$$

where we can see that $H_n^1 = H_n = \sum_{k=1}^{n}\frac{1}{k}$ Then we define the q-analog of H_n to be as follows:

$$H_n(q) := \sum_{k=1}^{n}\frac{1}{[k]_q}, |q| < 1$$

where

$$[k]_q = 1 + q + q^2...q^{k-1}$$

Using these definitions, Andrews [7]proved that

$$H_{p-1}(q) \equiv \frac{(p-1)(1-q)}{2} \pmod{[p]_q}$$

Andrews also showed another result that relies on more notation. Define

$$[n]_q! = [n]_q[n-1]_q...[1]_q$$

and

$$\binom{n}{k}_q = \frac{[n]_q!}{[k]_q![n-k]_q!}$$

Then Andrews showed that

$$\binom{np}{mp}_q \equiv \binom{n}{m}_{q^p} q^{(n-m)m\frac{p}{2}} \pmod{[p]_q^2}$$

Thus, we can obtain a q-analog for our original Wolstenholme Congruence by setting $n = 2, m = 1$:

$$\binom{2p}{p}_q \equiv [2]_{q^{p^2}} - \frac{p^2-1}{12}(q^p-1)^2 \pmod{[p]_q^2}$$

References

[1] E.Lucas, "Sur les congruences des nombres euleriens et les coefficients differentiels des fonctions trigonometriques, suivant un module premier,," *Bull.Soc.Math.France*, vol. 6, pp. 49–54, 1877-1878.

[2] J. Glaisher, "Congruences relating to the sums of products of the first n numbers and to other sums of products," *Q.J.Math*, 1900.

[3] Wikipedia, "Wolstenholme's theorem," *Wikipedia*, 2018.

[4] E. Alkan, "Variations on wolstenholme's theorem," *Amer. Math. Monthly*, vol. 101, 1994.

[5] L. Carlitz, "A note on wolstenholme's theorem," *Amer. Math. Monthly*, vol. 61, 1974.

[6] R. McIntosh, "h, on the converse of wolstenholme's theorem," *Acta Arith*, vol. 71, 1995.

[7] G. Andrews, "q-analogs of the binomial coefficient congruences of babbage," *Discrete Math*, vol. 204, 1999.

[8] R. Mestrovic, "Wolstenholme's theorem: Its generalizations and extensions in the last hundred and fifty years (1862–2012)," *arxiv*, 2011.