TESTING THE CONVERSE OF WOLSTENHOLME'S THEOREM

Vilmar Trevisan **Kenneth Weber**

Abstract

A classical result of Wolstenholme in 1862 shows that if $p \geq 5$ is a prime number then

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

Its converse, stating that a natural p satisfying this congruence is necessarily a prime number, is commonly believed to be true, although no proof has been given so far. In this note, we present an elementary proof of a partial result, namely, that the converse is true for even numbers and for powers of 3. Further, we prove that if $n = p^l$ is a prime power then

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

producing a relatively inexpensive converse test for powers of odd prime numbers.

Resumo

Um resultado clássico de Wolstenholme mostra que se p é um número primo, então

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

A recíproca desse teorema, indicando que um número natural p satisfazendo a congruência é necessariamente um número primo, embora acredita-se verdadeira, ainda não tem uma prova. Nesta nota, apresentamos uma prova elementar de um resultado parcial; especificamente, que a recíproca é verdadeira para números pares e para potências de 3. Além disso, provamos que se $n = p^l$ é uma potência de um primo, então

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

que é um teste eficiente para testar a recíproca de potência de primos ímpares.

AMS Classification Numbers: 11Y11, 11A51, 11-04

1 Introduction

A simple characterization of prime numbers is always an interesting goal, not only because this may be a hard problem but also because a simple characterization may lead to an efficient primality test, a task today sought with great interest by the scientific community, especially in the area of number theory.

A famous result for prime numbers, called the Theorem of Wolstenholme, is the following

Property 1 (Wolstenholme, 1862) *If $p \geq 5$ is a prime number then*

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

Apparently, it was James P. Jones [10, Problem B31,p. 84] who first conjectured that the converse of this theorem is true, namely that a natural number p satisfying the congruence of Property 1 is necessarily prime. The converse of Wolstenholme's Theorem is regarded as a very difficult problem.

In [9], Richard J. McIntosh obtains restrictive conditions on n for solutions of $\binom{2n-1}{n-1} \equiv 1 \pmod{n^r}$ and concludes that Wolstenholme's converse is probably true. For example, he shows that if p is a prime number and $n = p^2$ satisfies

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

(which would be a counterexample to the converse), then p satisfies

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^6},$$

which is unlikely. McIntosh also reports that the converse is known to be true for all composite numbers $n < 10^9$.

No proof, however, has been obtained for the converse of Wolstenholme's property. In section 3 we partially fill this gap, by proving that Property 1 does not hold for positive even numbers. This result is probably known to other authors who work on the subject, but we are unaware of a published proof. Moreover, the proof we present uses only elementary mathematics.

For a given composite number n, to show that $\binom{2n-1}{n-1} \not\equiv 1 \pmod{n^3}$, it suffices to show that $\binom{2n-1}{n-1} \not\equiv 1 \pmod{R}$, where $R > 1$ is any factor of n. Using this idea, we study the converse of Wolstenholme's theorem for powers of primes p, by determining the value of the binomial coefficient modulo p^3, p^4 and p^5. In section 4 we prove that if n is a power of 3, than it does not satisfy property 1, proving that the converse is true for $n = 3^l$. Additionally, we prove that if p is a prime number and $n = p^l,\ l \geq 2$, then

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

which reduces the size of the computational task for testing the converse.

Finally, we claim that the converse of Wolstenholme's theorem is true for all powers of primes $p < 2.5 \times 10^8$ (see section 5), by using the criteria given by equation (1).

2 Generalities

In this section, we review some well known results that will be used throughout this note.

First, we make use of a well known equation that is sometimes called *Vandermonde's convolution* $\binom{r+s}{i} = \sum_{j=0}^{i} \binom{r}{j}\binom{s}{i-j}$ [6, p. 169]. If we set $i = s = r = n$, where n is a positive integer, then we obtain

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

Also well known is the following equation, true for any positive integers r and s:

$$\binom{r}{s} = \frac{r}{s}\binom{r-1}{s-1}. \tag{3}$$

Applying this identity, it follows that for any positive integer n,

$$\binom{2n-1}{n-1} = \frac{1}{2}\sum_{j=0}^{n} \binom{n}{j}^2. \tag{4}$$

We see from this equation that

$$\binom{2p}{p} \equiv 2 \pmod{p^3},$$

true for primes $p \geq 5$ (see the paper by D. F. Bailey [4, lemma 1, p. 209]), is equivalent to the Wolstenholme's theorem.

Also widely used in this note is the following well known fact.

Lemma 1 *Let p be a prime number. If $n = p^r$ and $s \leq r$ is the highest power of p dividing m, then, the highest power of p dividing $\binom{n}{m}$ is $r - s$.*

3 Even Numbers

In this section we show the following

Theorem 1 *If $n > 0$ is even, then*

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

That is, the converse of Wolstenholme's Theorem is true for even positive integers.

We begin by noting

Fact 1 *The binomial coefficient*

$$\binom{2n-1}{n-1}$$

is odd if and only if n is a power of 2.

This is a trivial consequence of a classical result of E. Kummer [7], which states that the power r to which a prime p divides $\binom{a+b}{a}$ is equal to the number of carries in the addition of a and b in base p arithmetic. Writing $\binom{2n-1}{n-1} = \frac{1}{2}\binom{n+n}{n}$, it is easy to see from the binary representation of n that $\binom{2n-1}{n-1}$ is odd only when n is a power of 2.

Fact 1 also follows from Lucas' Theorem [8], which states that

$$\binom{a}{b} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1}\cdots\binom{a_k}{b_k} \pmod{p},$$

where $a = a_0 + a_1 p + \cdots + a_k p^k, b = b_0 + b_1 p + \cdots + b_k p^k, 0 \leq a_i, b_i \leq p-1$ are the base p representations of a and b. Employing the usual convention that $\binom{a}{b} = 0$ when $a < b$, it can be seen from the binary representation of $2n-1$ and $n-1$ that $\binom{2n-1}{n-1}$ is odd only when n is a power of 2. It is also possible to show fact 1 using only elementary manipulations with binomial coefficients.

Given n a natural number, there are unique integers, q and r such that

$$\binom{2n-1}{n-1} = qn^3 + r, \tag{5}$$

where either $r = 0$ or $0 < r < n^3$. The number r is, by definition, the modulo sought, that is $r \equiv \binom{2n-1}{n-1} \pmod{n^3}$.

For n even, not a power of two, fact 1 shows that the LHS of equation (5) is even, so that r must also be even and the converse of the Wolstenholme's property is true.

To complete the proof of theorem 1 it remains to show

Lemma 2 *If $n = 2^l,\ l \geq 1$, then*

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

Proof. For $l \geq 2$, using equation (4), we write

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

It remains to show that $B = \sum_{j=1}^{2^{l-1}-1} \binom{2^l}{j}^2 + \frac{1}{2}\binom{2^l}{2^{l-1}}^2 \equiv 2 \pmod{2^4}$. By lemma 1, 4 divides $\binom{2^l}{j}$ for any $j = 1, \ldots, 2^{l-1}-1$, implying that $B \equiv \frac{1}{2}\binom{2^l}{2^{l-1}}^2 \pmod{2^4}$. Lemma 1 also says that $\binom{2^l}{2^{l-1}} = 2X$, with X odd. Hence

$$\frac{1}{2}\binom{2^l}{2^{l-1}}^2 = 2X^2, \text{ odd } X.$$

As $X \equiv 1 \pmod{2}$, it follows that $X \equiv \pm 1 \pmod{8}$ or $X \equiv \pm 3 \pmod{8}$. In any case we have $X^2 \equiv 1 \pmod{8}$ and therefore $2X^2 \equiv 2 \pmod{16}$. Thus

$$B \equiv 2 \pmod{2^4}.$$

□

4 Odd Prime Powers

In this section we study the binomial congruence $\binom{2n-1}{n-1} \equiv 1 \pmod{n^3}$ for n a power of an odd prime number. We begin by showing

Theorem 2 *If $n = 3^l,\ l \geq 1$, then the converse of Wolstenholme's Theorem is true.*

Proof. We show that if $n = 3^l,\ l \geq 1$, then

$$\binom{2n-1}{n-1} \equiv 10 \pmod{3^5}.$$

For $l \geq 2$, we may write

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

Applying lemma 1, we see that $\binom{n}{j}$ is divisible by 9 for all j, but for $j = 3^{l-1}$, so that

$$C = \sum_{j=1}^{(n-1)/2} \binom{n}{j}^2 \equiv \binom{3^l}{3^{l-1}}^2 \pmod{3^4}.$$

We also know that $\binom{3^l}{3^{l-1}} = 3Y$, with Y and 3 relatively prime. That means $Y \equiv \pm 1 \pmod{3}$, implying that $Y^2 \equiv 1 \pmod{3}$. It follows that

$$C \equiv \binom{3^l}{3^{l-1}}^2 \equiv (3Y)^2 \equiv 9 \pmod{3^3},$$

and the theorem is proved.

□

We notice that the result of lemma 2 implies that $\binom{2n-1}{n-1} \not\equiv 1 \pmod{4}$, for $n = 2^l$ and the result of theorem 2 implies that $\binom{2n-1}{n-1} \not\equiv 1 \pmod{3^3}$, for $n = 3^l$. We conclude that the converse of Wolstenholme's theorem is true for powers of 2 and 3.

If $n = p^l$, where p is a prime number greater than 3, we need to compute the value of the binomial coefficient modulo a power of p higher than 3 because of the following

Theorem 3 *If $p \geq 5$ is prime and $n = p^l$ $l \geq 1$, then*

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

Proof. Theorem 4 of [4] states that for any nonnegative integers k and r, $\binom{kp}{rp} \equiv \binom{k}{r} \pmod{p^3}$. Applying this result l times, we have

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

As $\binom{2n-1}{n-1} = \frac{1}{2}\binom{2n}{n}$ and p is odd, the result follows.

□

By considering the binomial coefficient modulo p^4, we obtain the following reduction theorem.

Theorem 4 *If $p \geq 5$ is a prime number, $l \geq 1$ is an integer and $n = p^l$, then*

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

Proof. Since p is odd, it suffices to show that $\binom{2n}{n} \equiv \binom{2p}{p} \pmod{p^4}$. We write

$$\binom{2n}{n} = 2 + \sum_{j=1}^{n-1} \binom{n}{j}^2 = 2 + \sum_{j=1}^{p^l-1} \binom{p^l}{j}^2,$$

and notice that if p^{l-1} does not divide j then, applying lemma 1, we see that

p^2 divides $\binom{p^l}{j}$ or that $\binom{p^l}{j}^2 \equiv 0 \pmod{p^4}$ and

$$\binom{2n}{n} = 2 + \sum_{j=1}^{p-1} \binom{p^l}{jp^{l-1}}^2 \pmod{p^4}.$$

We quote lemma A of [5]which states that

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

Assuming that $l \geq 3$ and setting $k = 2$, we apply the result and write

$$\binom{p^l}{jp^{l-1}} \equiv \binom{p^k p^{l-2}}{p^k jp^l - 3} \equiv \binom{pp^{l-2}}{jp^{l-3}} \pmod{p^6}.$$

We repeat the argument $l - 3$ more times, following that

$$\binom{p^l}{jp^{l-1}} \equiv \binom{p^2}{jp} \pmod{p^6},$$

for all $0 < j < p$ and $l \geq 2$. So we can write

$$\binom{2n}{n} \equiv 2 + \sum_{j=1}^{p-1} \binom{p^2}{jp}^2 \pmod{p^4}.$$

We invoke now theorem 2.2 of [5] to claim that $\binom{p^2}{jp} \equiv \binom{p}{j} \pmod{p^4}$ and so it follows that

$$\binom{2n}{n} \equiv 2 + \sum_{j=1}^{p-1} \binom{p}{j}^2 \equiv \binom{2p}{p} \pmod{p^4},$$

completing the proof.

□

This reduction is computational useful since one may compute $\binom{2p-1}{p-1} \pmod{p^4}$. If this value is not 1, then the converse of Wolstenholme's Theorem is true for all powers of the prime p.

Studying criteria for solutions of $\binom{2n-1}{n-1} \equiv 1 \pmod{n^r}$, R. J. McIntosh considers primes p satisfying

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^4} \tag{6}$$

and calls them *Wolstenholme primes* [9].

Theorem 4 shows that if p is not a Wolstenholme prime, then the converse of Wolstenholme's theorem is true for all powers of p.

5 Computer Experiments

We performed the computation of $\binom{2p-1}{p-1} \pmod{p^4}$ for all primes $p < 2.5 \times 10^8$ which is, according to the reduction criterion of theorem 4, sufficient to show that the converse of Wolstenholme's Theorem is true for all powers of p, when p is not a Wolstenholme prime.

It is important to notice that computing the binomial coefficient $\binom{2p-1}{p-1} \pmod{p^4}$ is not a trivial task, since the arithmetic involves large numbers.

The same computation of $\binom{2p-1}{p-1} \pmod{p^4}$ was considered by McIntosh in the search for Wolstenholme primes and several statements equivalent to equation (6) are proven in [9]. The following is the most appealing for computational purposes (because it reduces to calculations modulo p):

Theorem 5 *For all primes $p \geq 11, p$ is a Wolstenholme prime if and only if*

$$\sum_{j=\lfloor p/6\rfloor+1}^{\lfloor p/4\rfloor} \frac{1}{j^3} \equiv 0 \pmod{p}.$$

Using this criterion, we performed the computation for primes $p < 2.5 \times 10^8$. This extends the search of [9], reporting that there are only two Wolstenholme primes $p < 2 \times 10^8$, namely, $p_1 = 16,843$ and $p_2 = 2,124,679$.

We confirmed this computation and found no other Wolstenholme prime up to 2.5×10^8. This implies that for all prime powers p^l, $l > 1$, with $p < 2.5 \times 10^8$, and $p \neq p_1, p_2$, the converse of Wolstenholme's Theorem is true.

For powers of Wolstenholme primes p, we need to work some more in order to find out whether the converse of Wolstenholme's Theorem is true. It is possible to prove that theorem 4 also holds modulo p^5. Hence, if $\binom{2p-1}{p-1} \not\equiv 1 \pmod{p^5}$, then the converse of Wolstenholme's Theorem is true. We then executed the computation $\binom{2p-1}{p-1} \pmod{p^5}$. As $\binom{2p-1}{p-1} = 1 + \sum_{j=1}^{(p-1)/2} \binom{p}{j}^2$ and p divides $\binom{p}{j}$, it follows that

$$\binom{2p-1}{p-1} = 1 + p^2 \sum_{j=1}^{(p-1)/2} (\binom{p}{j}/p)^2 \pmod{p^5}, \tag{7}$$

and so this computation can be done modulo p^3. Defining $L_1 = 1$, we see that $L_j = \binom{p}{j}/p$ satisfies

$$L_{j+1} = L_j \frac{p-j}{j+1},$$

for $1 \leq j < (p-1)/2$. Thus the computation induced by equation 7 is accomplished with $O(p)$ arithmetic operations with integer of size $O(p^3)$.

Using this method, we performed the computations for p_1 and p_2, obtaining for $l \geq 1$

$$\binom{2p_1^l - 1}{p_1^l - 1} \equiv 26742877554968189492 \pmod{p_1^5}$$

$$\binom{2p_2^l - 1}{p_2^l - 1} \equiv 331023884821531317892086403766 95 \pmod{p_2^5}$$

implying that the converse of Wolstenholme's theorem is also true for powers of p_1 and p_2.

Table 1 summarizes what is known to the authors about the converse of Wolstenholme's theorem at the time this paper was written.

Acknowledgments: This work was performed while the first author was visiting Kent State University. Financial support for the visit was provided

Integer Type	Status
Even	True
Prime powers $p^l,\ l \geq 2$	True if $p < 2.5 \times 10^8$ Unknown if $p > 2.5 \times 10^8$
Other n positive composite numbers	True if $n < 10^9$ Unknown if $n \geq 10^9$

Table 1: Status of the converse of Wolstenholme's theorem

by CAPES and UFRGS, Brazil. The computation was done with the generous support of LICC (Scientific Computation Laboratory) at the Institute of Mathematics—UFRGS. We would like to acknowledge the hospitality of the Department of Mathematics and Computer Science of KSU. We are particularly grateful to Prof. Hassan Peyravi of Kent State University, who was very kind to allow the use of his computer to perform part of the computation.

References

[1] Alkan, E., *Variations on Wolstenholme's theorem*, American Mathematical Monthly 101 (10), (1994), 1001-1004.

[2] Brinkmann, H. W., *Problem E435*, American Mathematical Monthly 48, (1941), 269-271.

[3] Bauer, F. L., *For all primes greater than 3,* $\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$ holds", Math. Intelligencer 10 (3), (1988), 42.

[4] Bailey, D. F., *Two p^3 variations of Lucas' theorem*, Journal of Number Theory 35 (2), (1990), 208-215.

[5] Gessel, I. M., *Some congruences for generalized Euler numbers*, Canadian Journal of Mathematics 35 (4), (1983), 687-709.

[6] Graham, R. L.; Knuth, D. E.; Patashnik, O., *Concrete Mathematics – A Foundation for Computer Science*, Addison-Wesley, Reading, (1989).

[7] Kummer, E. E., *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, J. Reine Angew. Math. 44, (1852), 93-146.

[8] Lucas, E., *Sur les congruences des nombres eulériens et de coefficients différentiels des fonctions trigonométriques, suivant un module premier*, Bull. Soc. Math. France 6, (1878), 49-54.

[9] McIntosh, R. J., *On the converse of Wolstenholme's Theorem*, Acta Arithmetica 71 (4), (1995), 381-389.

[10] Guy, R. K., *Unsolved Problems in Number Theory*, vol. 1, Springer-Verlag, (1994).

UFRGS-Instituto de Matemática
91509–900, Porto Alegre, RS
Brasil
email: trevisan@mat.ufrgs.br

Depart. of Computer and Information
Science - Mount Union College
Alliance, OH 44601
email: weberk@muc.edu