VARIATIONS OF LUCAS’ THEOREM MODULO PRIME POWERS

ROMEO MESTROVIĆ

Abstract. Let $p$ be a prime, and let $k, n, m, n_0$ and $m_0$ be nonnegative integers such that $k \geq 1$, and $n_0$ and $m_0$ are both less than $p$. K. Davis and W. Webb established that for a prime $p \geq 5$ the following variation of Lucas’ Theorem modulo prime powers holds

$$\left( np^k + n_0 \atop mp^k + m_0 \right) \equiv \left( np^{(k-1)/3} \atop mp^{(k-1)/3} \right) \left( n_0 \atop m_0 \right) \pmod{p^k}.$$ 

In the proof the authors used their earlier result that present a generalized version of Lucas’ Theorem.

In this paper we present a a simple inductive proof of the above congruence. Our proof is based on a classical congruence due to Jacobsthal, and we additionally use only some well known identities for binomial coefficients. Moreover, we prove that the assertion is also true for $p = 2$ and $p = 3$ if in the above congruence one replace $\lfloor (k-1)/3 \rfloor$ by $\lfloor k/2 \rfloor$, and by $\lfloor (k-1)/2 \rfloor$, respectively.

As an application, in terms of Lucas’ type congruences, we obtain a new characterization of Wolstenholme primes.

1. INTRODUCTION AND MAIN RESULTS

In 1878, É. Lucas proved a remarkable result which provides a simple way to compute the binomial coefficient $\binom{a}{b}$ modulo a prime $p$ in terms of the binomial coefficients of the base-$p$ digits of nonnegative integers $a$ and $b$ with $b \leq a$. Namely, if $p$ is a prime, and $n, m, n_0$ and $m_0$ are nonnegative integers with $n_0, m_0 \leq p - 1$, then a beautiful theorem of Lucas ($\[\[\]$; also see $[6]$) states that for every prime $p$,

$$\left( np + n_0 \atop mp + m_0 \right) \equiv \left( n \atop m \right) \left( n_0 \atop m_0 \right) \pmod{p} \quad (1)$$

1991 Mathematics Subject Classification. 11A07, 11B65, 05A10.

Key words and phrases. Congruence modulo prime (prime power), Lucas’ Theorem, a generalization of Lucas’ Theorem to prime powers, result of Jacobsthal, Wolstenholme prime.
VARIATIONS OF LUCAS’ THEOREM MODULO PRIME POWERS

(with the usual convention that $\binom{0}{0} = 1$, and $\binom{l}{r} = 0$ if $l < r$). After more than 110 years D. F. Bailey established that under the above assumptions, $p$ can be replaced in (1) by $p^2$ [1, Theorem 3], and by $p^3$ if $p \geq 5$ [1, Theorem 5]. Moreover, it is noticed in [1, p. 209] that in the congruence (1) $p$ cannot be replaced by $p^4$. Using a Lucas’ theorem for prime powers [3, Theorem 2] (also cf. [4, Theorem 2]), in 1990 K. Davis and W. Webb [4, Theorem 3] generalized Bailey’s congruences for any modulus $p^k$ with $p \geq 5$ and $k \geq 1$. Their result is improved quite recently by the author of this paper in [12].

Moreover, in 2007 Z.-W. Sun and D. M. Davis [18] and in 2009 M. Chamberland and K. Dilcher [2] established analogues of Lucas’ theorem for certain classes of binomial sums. Quite recently, the author of this article [15] discussed various cases of the congruences from Theorem A with $n_0 = m_0 = 0$ in dependence of different values of exponents $k$ and $s$.

Another generalization of mentioned D. F. Bailey’s Lucas-like theorem to every prime powers $p^k$ with $p \geq 5$ and $k = 2, 3, \ldots$ was discovered in 1990 by K. S. Davis and W. A. Webb (3, Theorem 3), also see [10, p. 88, Theorem 5.1.2] and independently by A. Granville [7] (also see [8] and [6, Theorem 1]). Using mentioned result, in 1993 K. S. Davis and W. A. Webb [4] generalized Bailey’s congruences for any modulus $p^k$ with $p \geq 5$ and $k \geq 1$. Namely, they proved the following congruence.

**Theorem A** ([4, Theorem 3]). Let $p$ be any prime, and let $k, n, m, n_0$ and $m_0$ be positive integers such that $0 < n_0, m_0 < p^s$. Then

$$\binom{np^{k+s} + n_0}{mp^{k+s} + m_0} \equiv \binom{np^k}{mp^k} \binom{n_0}{m_0} \pmod{p^k+1}.$$ 

**Remark 1.** As noticed above, Theorem A is proved by the authors using their result in [3, Theorem 3] which is slightly more complicated (cf. remarks by A. Granville in [6, Introduction]). The aim of this note is to give a simple elementary approach to the proof of Theorem A. For this purpose, in this note, we establish a simple induction proof of Corollary of Theorem A ([4, Corollary 1]). We point out that, proceeding by induction on $s$, the congruence in this Corollary (our Theorem given below) allows us to establish a short and simple proof of Theorem A. This proof will be presented in the following version of this article.

**Theorem** ([4, Corollary 1]). Let $p$ be any prime, and let $k, n, m, n_0$ and $m_0$ be nonnegative integers such that $k \geq 1$, and $n_0$ and $m_0$ are both less
than $p$. If $p \geq 5$ then
\[
\left( \frac{np^k + n_0}{mp^k + m_0} \right) \equiv \left( \frac{np^{\lfloor (k-1)/3 \rfloor}}{mp^{\lfloor (k-1)/3 \rfloor}} \right) \left( \frac{n_0}{m_0} \right) \pmod{p^k},
\]
(2)
where $\lfloor a \rfloor$ is the greatest integer less than or equal to $a$.

Furthermore, for $p = 2$ the congruence (2) with $\lfloor k/2 \rfloor$ instead of $\lfloor (k - 1)/3 \rfloor$ is satisfied, and for $p = 3$ the congruence (2) with $\lfloor (k - 1)/2 \rfloor$ instead of $\lfloor (k - 1)/3 \rfloor$ is also satisfied.

As noticed above, the congruences (2) for $k = 2$ and $k = 3$ are given by Bailey in [1, Theorem 3 and Theorem 5, respectively] (our Corollaries 1 and 2, respectively). Recall that proof of Theorem 5 in [1] is derived by using the congruence $\left( \frac{np}{mp} \right) \equiv \left( \frac{n}{m} \right) \pmod{p^3}$ with $p \geq 5$ [1, Theorem 4] and a counting technique of M. Hausner from [9]. This theorem is refined modulo $p^5$ by a recent result of J. Zhao [19, Theorem 3.5].

Our proof of the above theorem is inductive, and it is based on some congruences of Jacobsthal (see, e.g., [6]) and Sun and Davis [18]. Namely, the following lemma provides a basis for induction proof of Theorem.

**Lemma.** Let $n, m$ and $k$ be nonnegative integers with $m \leq n$ and $k \geq 1$. If $p$ is a prime greater than 3, then
\[
\left( \frac{np^k}{mp^k} \right) \equiv \left( \frac{np^{\lfloor (k-1)/3 \rfloor}}{mp^{\lfloor (k-1)/3 \rfloor}} \right) \pmod{p^k}.
\]
(3)
Furthermore, for $p = 2$ and $p = 3$ we have
\[
\left( \frac{n \cdot 2^k}{m \cdot 2^k} \right) \equiv \left( \frac{n \cdot 2^{\lfloor k/2 \rfloor}}{m \cdot 2^{\lfloor k/2 \rfloor}} \right) \pmod{2^k},
\]
(4)
\[
\left( \frac{n \cdot 3^k}{m \cdot 3^k} \right) \equiv \left( \frac{n \cdot 3^{\lfloor (k-1)/2 \rfloor}}{m \cdot 3^{\lfloor (k-1)/2 \rfloor}} \right) \pmod{3^k}.
\]
(5)

**Proof.** We first suppose that $p \geq 5$. Then we claim that the congruence
\[
\left( \frac{np^k}{mp^k} \right) \equiv \left( \frac{np^{k-i}}{mp^{k-i}} \right) \pmod{p^{3(k-i+1)}}
\]
holds for all nonnegative integers $n, m, k$ and $i$ such that $1 \leq i \leq k$. If we put $i = k - \lfloor (k - 1)/3 \rfloor$ in (6), then since $3(k - i + 1) = 3\lfloor (k - 1)/3 \rfloor + 3 \geq 3(k - 3)/3 + 3 = k$, we immediately obtain (3) from our Lemma.
To prove (6), we use induction on \( i \geq 1 \). By a result of Jacobsthal (see, e.g., [6]),
\[
\binom{np}{mp} \equiv \binom{n}{m} \pmod{p^e},
\]
for any integers \( n \geq m \geq 0 \) and prime \( p \geq 5 \), where \( e \) is the power of \( p \) dividing \( p^3 nm(n - m) \) (this exponent \( e \) can only be increased if \( p \) divides \( B_{p-3} \), the \((p - 3)\)rd Bernoulli number). Therefore, the congruence (7) with \( np^{k-1} \) and \( mp^{k-1} \) instead of \( n \) and \( m \), respectively, is satisfied for the exponent \( e = 3 + 3(k - 1) = 3k \). This is in fact the congruence (6) with \( i = 1 \).

Now suppose that (6) holds for some \( i \) such that \( 1 \leq i \leq k - 1 \). Then by a result of Jacobsthal mentioned above, the congruence (7) with \( np^{k-(i+1)} \) and \( mp^{k-(i+1)} \) instead of \( n \) and \( m \), respectively, is satisfied for the exponent \( e = 3 + 3(k - (i+1)) = 3(k-i) \). This, together with the induction hypothesis given by (6), yields
\[
\binom{np^k}{mp^k} \equiv \binom{np^{k-(i+1)}}{mp^{k-(i+1)}} \pmod{p^{3(k-i)}},
\]
as desired.

If \( p = 2 \) then by [18, Lemma 3.2, the congruence (3.3)], we have
\[
\binom{2n}{2m} \equiv (-1)^m \binom{n}{m} \pmod{2^{\text{ord}_2(n)+1}},
\]
where \( \text{ord}_2(n) \) is the largest power of 2 dividing \( n \).

Then by induction on \( k \geq 1 \), similarly as above, easily follows the congruence (4).

Finally, if \( p = 3 \) then by [18, Lemma 3.2, the congruence (3.2)], we have
\[
\binom{3n}{3m} \equiv \binom{n}{m} \pmod{3^{\text{ord}_3(n)+2}},
\]
where \( \text{ord}_3(n) \) is the largest power of 3 dividing \( n \).

Then by induction on \( k \geq 1 \) easily follows the congruence (5).

This completes the induction proof. \( \square \)

**Proof of Theorem.** First suppose that \( p \geq 5 \), and that \( k \) is any fixed positive integer. In order to prove the congruence (2), we proceed by induction on the sum \( s := n_0 + m_0 \geq 0 \), where \( 0 \leq n_0, m_0 \leq p - 1 \), and hence \( 0 \leq s \leq 2p - 2 \). If \( s = 0 \), that is \( n_0 = m_0 = 0 \), then the congruence (2) reduces to the congruence (3) of our Lemma.

Now suppose that the congruence (2) is satisfied for all \( n, m, n_0 \) and \( m_0 \) such that \( n_0 + m_0 = s \) for some \( s \) with \( 0 \leq s \leq 2p - 3 \). Next assume that \( n_0 \) and \( m_0 \) are any nonnegative integers such that \( n_0 + m_0 = s + 1 \). Then
consider the cases: \( n_0 < m_0, n_0 = m_0 \geq 1 \) and \( n_0 \geq m_0 + 1 \).

**Case 1.** \( n_0 < m_0 \). Then \( \left( \begin{array}{c} n_0 \\ m_0 \end{array} \right) = 0 \), and hence the right side of (2) is equal to 0. Using the identity \( \left( \begin{array}{c} r \end{array} \right) = \frac{i-r+1}{r} \left( \begin{array}{c} i \end{array} \right) \), we find that

\[
\left( \begin{array}{c} np^k + n_0 \\ mp^k + m_0 \end{array} \right) = \frac{p^k(n - m) - (m_0 - n_0 - 1)}{mp^k + m_0} \left( \begin{array}{c} np^k + n_0 \\ mp^k + (m_0 - 1) \end{array} \right).
\]

If \( n_0 = m_0 - 1 \) then since \( 1 \leq m_0 \leq p - 1 \), the first factor on the right hand side of the above equality is divisible by \( p^k \). If \( n_0 < m_0 - 1 \) then since \( n_0 + (m_0 - 1) = s \), by the induction hypothesis, we get

\[
\left( \begin{array}{c} np^k + n_0 \\ mp^k + (m_0 - 1) \end{array} \right) \equiv \left( \begin{array}{c} np^{l(k-1)/3} \\ mp^{l(k-1)/3} \end{array} \right) \left( \begin{array}{c} n_0 \\ m_0 \end{array} \right) = 0 \pmod{p^k}.
\]

Hence, in both cases we obtain

\[
\left( \begin{array}{c} np^k + n_0 \\ mp^k + m_0 \end{array} \right) \equiv 0 = \left( \begin{array}{c} np^{l(k-1)/3} \\ mp^{l(k-1)/3} \end{array} \right) \left( \begin{array}{c} n_0 \\ m_0 \end{array} \right) \pmod{p^k},
\]

as desired.

**Case 2.** \( n_0 = m_0 \geq 1 \). If \( n_0 = m_0 \geq 1 \), then by the identity \( \left( \begin{array}{c} r \end{array} \right) = \frac{i-r+1}{r} \left( \begin{array}{c} i \end{array} \right) \), in view of \( 1 \leq n_0 \leq p - 1 \) and \( n_0 + (m_0 - 1) = s \), the induction hypothesis gives

\[
\left( \begin{array}{c} np^k + n_0 \\ mp^k + n_0 \end{array} \right) = \frac{p^k(n - m) + 1}{mp^k + m_0} \left( \begin{array}{c} np^k + n_0 \\ mp^k + (n_0 - 1) \end{array} \right)
\equiv \frac{p^k(n - m) + 1}{mp^k + n_0} \left( \begin{array}{c} np^{l(k-1)/3} \\ mp^{l(k-1)/3} \end{array} \right) \left( \begin{array}{c} n_0 \\ m_0 \end{array} \right) \pmod{p^k}
\]

\[
= n_0 \cdot \frac{p^k(n - m) + 1}{mp^k + n_0} \left( \begin{array}{c} np^{l(k-1)/3} \\ mp^{l(k-1)/3} \end{array} \right) \pmod{p^k}.
\]

This congruence and the fact that \( 1 \leq n_0 \leq p - 1 \) imply

\[
\left( \begin{array}{c} np^k + n_0 \\ mp^k + m_0 \end{array} \right) - \left( \begin{array}{c} np^{l(k-1)/3} \\ mp^{l(k-1)/3} \end{array} \right) \left( \begin{array}{c} n_0 \\ m_0 \end{array} \right)
\equiv \left( n_0 \cdot \frac{p^k(n - m) + 1}{mp^k + n_0} - 1 \right) \left( \begin{array}{c} np^{l(k-1)/3} \\ mp^{l(k-1)/3} \end{array} \right) \pmod{p^k}
\]

\[
= p^k \cdot n_0(n - m) - m \left( \begin{array}{c} np^{l(k-1)/3} \\ mp^{l(k-1)/3} \end{array} \right) \equiv 0 \pmod{p^k},
\]

whence follows (2).

**Case 3.** \( n_0 \geq m_0 + 1 \). Then we proceed in a similar way as in Case
2. Using the identity \( \binom{l}{r} = \binom{l - 1}{r - 1} \), in view of \( 1 \leq n_0 - m_0 \leq p - 1 \) and 
\( (n_0 - 1) + m_0 = s \), the induction hypothesis yields
\[
\binom{np^k + n_0}{mp^k + m_0} = \frac{np^k + n_0}{p^k(n - m) + n_0 - m_0} \binom{np^k + (n_0 - 1)}{mp^k + m_0}
\]
\[
\equiv \frac{np^k + n_0}{p^k(n - m) + n_0 - m_0} \binom{np^{(k-1)/3}}{mp^{(k-1)/3}} \binom{n_0 - 1}{m_0} \pmod{p^k}
\]
\[
= \frac{np^k + n_0}{p^k(n - m) + n_0 - m_0} \binom{np^{(k-1)/3}}{mp^{(k-1)/3}} \binom{n_0}{m_0} \cdot \frac{n_0 - m_0}{n_0}.
\]

The above congruence and the facts that \( 1 \leq n_0 \leq p - 1 \) and \( 1 \leq n_0 - m_0 \leq p - 1 \), yield
\[
\binom{np^k + n_0}{mp^k + m_0} - \frac{np^{(k-1)/3}}{mp^{(k-1)/3}} \binom{n_0}{m_0} \equiv \binom{n_0}{m_0} \pmod{p^k}
\]
\[
= p^k \cdot \frac{mn_0 - nm_0}{n_0(p^k(n - m) + n_0 - m_0)} \binom{np^{(k-1)/3}}{mp^{(k-1)/3}} \binom{n_0}{m_0} \equiv 0 \pmod{p^k},
\]
and so, (2) is satisfied.

This concludes the assertion for any prime \( p \geq 5 \).

The assertions of Theorem for \( p = 2 \) and \( p = 3 \) can be obtained by using the same method as in the above induction proof for \( p \geq 5 \), and hence may be omitted. Recall that the bases of induction proofs related to \( p = 2 \) and \( p = 3 \) are the congruences (4) and (5) of Lemma, respectively.

This completes the induction proof of Theorem.

\[\square\]

We now obtain two immediate consequences of Theorem.

**Corollary 1 (II, Theorem 3).** If \( p \) is a prime, \( n, m, n_0 \) and \( m_0 \) are nonnegative integers, and \( n_0 \) and \( m_0 \) are both less than \( p \), then
\[
\binom{np^2 + n_0}{mp^2 + m_0} \equiv \binom{n}{m} \binom{n_0}{m_0} \pmod{p^2}.
\]

**Proof.** First observe that the above assertion for \( p \geq 5 \) is a particular case of Theorem for \( k = 2 \).

If \( p = 3 \) then taking \( k = 2 \) in (5) of Lemma, we obtain
\[
\binom{9n}{9m} \equiv \binom{n}{m} \pmod{9}.
\]
If we assume that the above congruence is a base of induction, then applying the same method as in the proof of Theorem for the case \( p \geq 5 \), we obtain
\[
\binom{9n + n_0}{9m + m_0} \equiv \binom{n}{m} \binom{n_0}{m_0} \pmod{9},
\]
for all \( n, m, n_0 \) and \( m_0 \) with \( 0 \leq n_0 \leq 2 \) and \( 0 \leq m_0 \leq 2 \).

Analogously, using the same argument, if we prove that
\[
\binom{4n}{4m} \equiv \binom{n}{m} \pmod{4},
\]
then it follows that
\[
\binom{4n + n_0}{4m + m_0} \equiv \binom{n}{m} \binom{n_0}{m_0} \pmod{4},
\]
for all \( n, m, n_0 \) and \( m_0 \) such that \( 0 \leq n_0 \leq 1 \) and \( 0 \leq m_0 \leq 1 \).

To prove (8), note that by (4) of Lemma, we have \( \binom{4n}{4m} \equiv \binom{2n}{2m} \pmod{4} \), and thus (8) is equivalent to the congruence
\[
\binom{2n}{2m} \equiv \binom{n}{m} \pmod{4} \tag{9}
\]
By the last congruence in the Proof of Lemma 3.2 in [18], we have
\[
\binom{2n}{2m} \equiv (-1)^m \binom{n}{m} - (-1)^m 2^n \binom{n - 1}{m - 1} \left( \frac{3 + (-1)^m}{2} \right) \pmod{2^{\text{ord}_2(n+2)}}. \tag{10}
\]
If \( m \) is even, then the above congruence immediately yields (9) for all \( n \).
If \( m \) is odd and \( n \) is even, then by Lucas’ Theorem, \( \binom{n}{m} \equiv 0 \pmod{2} \), and thus (10) implies that
\[
\binom{2n}{2m} \equiv -\binom{n}{m} + 2^n \binom{n - 1}{m - 1} \equiv -\binom{n}{m} \equiv \binom{n}{m} \pmod{4}.
\]
Finally, if \( n \) and \( m \) are both odd, then from the identity \( m \binom{n}{m} = m \binom{n - 1}{m - 1} \) we see that the integers \( \binom{n}{m} \) and \( \binom{n - 1}{m - 1} \) have the same parity. This fact implies that \( 2 \binom{n}{m} \equiv 2 \binom{n - 1}{m - 1} \pmod{4} \), which together with the fact that \( n^2 \equiv 1 \pmod{4} \), by (10) yields
\[
\binom{2n}{2m} \equiv -\binom{n}{m} + 2 \binom{n - 1}{m - 1} \equiv \binom{n}{m} \pmod{4}.
\]
This completes the proof. □

**Corollary 2 (Theorem 5).** Let $p$ be a prime greater than 3. If $n, m, n_0$ and $m_0$ are nonnegative integers with $n_0$ and $m_0$ less than $p$, then

$${np^3 + n_0 \over mp^3 + m_0} \equiv {n \choose m} {n_0 \choose m_0} \pmod{p^3}.$$ 

*Proof.* Clearly, the above assertion is a particular case of Theorem for $k = 3$ with a prime $p \geq 5$. □

2. **A CHARACTERIZATION OF WOLSTENHOLME PRIMES**

A prime $p$ is said to be *Wolstenholme prime* if it satisfies the congruence

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

or equivalently,

$${2p \choose p} \equiv 2 \pmod{p^4}. \quad (11)$$

The two known such primes are 16843 and 2124679, and McIntosh and Roettger reported in [17] that these primes are only two Wolstenholme primes less than $10^9$. However, McIntosh in [16] conjectured that there are infinitely many Wolstenholme primes (also see [13] and [14, Section 7]).

As an application of Theorem of Section 1, in terms of Lucas’ type congruences, we obtain the following characterization of Wolstenholme primes.

**Proposition.** The following statements about a prime $p \geq 5$ are equivalent.

(i) $p$ is a Wolstenholme prime;
(ii) for all nonnegative integers $n$ and $m$,

$${np \choose mp} \equiv {n \choose m} \pmod{p^4}; \quad (12)$$

(iii) for all nonnegative integers $n, m, n_0$ and $m_0$ such that $n_0$ and $m_0$ are less than $p$,

$${np^4 + n_0 \over mp^4 + m_0} \equiv {n \choose m} {n_0 \choose m_0} \pmod{p^4}. \quad (13)$$
Proof. (i) ⇒ (ii). By a special case of Glaisher’s congruence ([3, p. 21]; also cf. [16, Theorem 2]), for each prime \( p \geq 5 \),

\[
\binom{2p - 1}{p - 1} \equiv 1 - \frac{2}{3}p^3B_{p-3} \pmod{p^4},
\]

where \( B_{p-3} \) is the \((p - 3)\)rd Bernoulli number. This shows that a prime \( p \) is a Wolstenholme prime if and only if \( p \) divides the numerator of \( B_{p-3} \). On the other hand, by a result of Jacobsthal mentioned in the proof of Lemma (after the congruence (9)), the congruence (12) is satisfied for any integers \( n \geq m \geq 0 \) and prime \( p \geq 5 \) only if \( p \) divides \( B_{p-3} \).

(ii) ⇒ (iii). Note that for any prime \( p \geq 5 \) and \( k = 4 \) the congruence (2) of Theorem becomes

\[
\binom{np^4 + n_0}{mp^4 + m_0} \equiv \binom{np}{mp} \binom{n_0}{m_0} \pmod{p^4}.
\]

If we suppose that (12) is satisfied for all nonnegative integers \( n \) and \( m \), then (12) and the above congruence immediately yield (13), as desired.

(iii) ⇒ (i). If we suppose that (13) holds, then taking \( n = 2, m = 1, n_0 = m_0 = 0 \) in (13), we obtain the congruence \( \binom{2p^4}{p^4} \equiv 2 \pmod{p^4} \). On the other hand, taking \( n = 2, m = 1, k = 4 \) and \( i = 3 \) in (6), we have \( \binom{2p^4}{p^4} \equiv \binom{2p}{p} \pmod{p^6} \). These two congruences immediately imply (11), and thus \( p \) is a Wolstenholme prime.

This completes the proof. \( \Box \)

Remark 2. Note that for any prime \( p \geq 5 \) and for every \( k \in \{4, 5, 6\} \) the congruence (2) of Theorem becomes

\[
\binom{np^k + n_0}{mp^k + m_0} \equiv \binom{np}{mp} \binom{n_0}{m_0} \pmod{p^k}.
\]

If \( n \) and \( m \).

By Wolstenholme’s theorem (see, e.g., [19, Theorem 1]), if \( p \) is a prime
greater than 3, then the numerator of the fraction
\[ H(p - 1) := 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p - 1} \]
is divisible by \( p^2 \). Now we define \( w_p < p^2 \) to be the unique nonnegative integer such that \( w_p \equiv H(p - 1)/p^2 \pmod{p^2} \). It is well known (see e.g., [5]) that
\[ w_p \equiv -\frac{1}{3} B_{p-3} \pmod{p}. \]
Furthermore, by a recent result of J. Zhao [19, the congruence (10) of Theorem 3.2], for given prime \( p \geq 7 \) the congruence (15) is satisfied for all \( n \) and \( m \) if and only if \( w_p = 0 \). However, using the argument based on the prime number theorem, McIntosh [16, p. 387] conjectured that no prime satisfies the congruence \( \binom{2p-1}{p-1} \equiv 1 \pmod{p^5} \). Since the previous congruence is a particular case of (15) for \( n = 2 \) and \( m = 1 \), McIntosh’s Conjecture suggests the following.

**Conjecture.** The exponent \( \lfloor (k-1)/3 \rfloor \) in the congruence (2) of Theorem can only be decreased for \( k = 4 \) when \( p \) is a Wolstenholme prime.

**Remark 3.** Given any prime \( p \) and \( k \geq 2 \), setting \( n = m = n_0 = 1 \) and \( m_0 = 0 \) in (2) of Theorem, we obtain
\[ \binom{p^k + 1}{p^k} = p^k + 1 \equiv 1 \pmod{p^k}. \]
This, together with the trivial fact that \( p^k + 1 \not\equiv 1 \pmod{p^{k+1}} \), shows that the exponent \( k \) of the modulus \( \pmod{p^k} \) in the congruence (2) of Theorem cannot be increased for none \( k \) and \( p \).

**References**

[1] D. F. BAILEY, Two \( p^3 \) variations of Lucas’ theorem, *J. Number Theory* 35 (1990), 208–215.
[2] M. CHAMBERLAND and K. DILCHER, A binomial sum related to Wolstenholme’s theorem, *J. Number Theory* 129 (2009), 2659–2672.
[3] K. S. DAVIS and W. A. WEBB, Lucas’ theorem for prime powers, *European J. Combin.* 11 (1990), 229–233.
[4] K. S. DAVIS and W. A. WEBB, A binomial coefficient congruence modulo prime powers, *J. Number Theory.* 43 (1993), 20–23.
[5] J. W. L. GLAISHER, Congruences relating to the sums of products of the first \( n \) numbers and to the other sums of products, *Quart. J. Math.* 31 (1900), 1–35.
[6] A. GRANVILLE, Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers, in *Organic mathematics* (Burnaby, BC, 1995), 253–276, CMS Conf. Proc., 20, Amer. Math. Soc., Providence, RI, 1997.
[7] A. GRANVILLE, Zaphod Beeblebrox’s brain and the fifty-ninth row of Pascal’s triangle Amer. Math. Monthly, 99 (1992), 318–331.
[8] A. GRANVILLE, Correction to “Zaphod Beeblebrox’s brain and the fifty-ninth row of Pascal’s triangle, Amer. Math. Monthly 104 (1997), 848–851.
[9] M. HAUSNER, Applications of a simple of counting technique, Amer. Math. Monthly 90 (1983), 127–129.
[10] A. D. LOVELESS, Extensions in the Theory of Lucas and Lehmer Pseudoprimes, Ph.D. thesis, Washington State University, Department of Mathematics, 2005, available at http://research.wsulibs.wsu.edu/xmlui/handle/2376/368.
[11] É. LUCAS, Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier, Bull. Soc. Math. France 6 (1877–1878), 49–54.
[12] R. MEŠTROVIĆ, Lucas’ theorem modulo prime powers, 5 pages, submitted, to be posted at arXiv, January 2013.
[13] R. MEŠTROVIĆ, Congruences for Wolstenholme primes, 16 pages, submitted; available at arXiv:1108.4178v1 [mathNT], 2011.
[14] R. MEŠTROVIĆ, Wolstenholme’s theorem: its generalizations and extensions in the last hundred and fifty years (1862–2012), 31 pages, arXiv:1111.3057v2 [mathNT], 2011.
[15] R. MEŠTROVIĆ, A note on the congruence $\binom{n^p}{mp^k} \equiv \binom{n}{m} \pmod{p^r}$, Czechoslovak Math. J. 62, No. 1 (2012), 59–65.
[16] R. J. MCINTOSH, On the converse of Wolstenholme’s Theorem, Acta Arith. 71 (1995), 381–389.
[17] R. J. MCINTOSH and E. L. ROETTGER, A search for Fibonacci-Wieferich and Wolstenholme primes, Math. Comp. 76 (2007), 2087–2094.
[18] Z.-W. SUN and D. M. DAVIS, Combinatorial congruences modulo prime powers, Trans. Amer. Math. Soc. 359 (2007), 5525–5553.
[19] J. ZHAO, Bernoulli Numbers, Wolstenholme’s Theorem, and $p^5$ Variations of Lucas’ Theorem, J. Number Theory 123 (2007) 18–26.

Maritime Faculty, University of Montenegro, Dobrota 36, 85330 Kotor, Montenegro
E-mail address: romeo@ac.me