Czechoslovak Mathematical Journal

Romeo Meštrović

A note on the congruence $\binom{np^k}{mp^k} \equiv \binom{n}{m} \pmod{p^r}$

Czechoslovak Mathematical Journal, Vol. 62 (2012), No. 1, 59–65

Persistent URL: `http://dml.cz/dmlcz/142040`

Czechoslovak Mathematical Journal, 62 (137) (2012), 59–65

A NOTE ON THE CONGRUENCE $\binom{np^k}{mp^k} \equiv \binom{n}{m} \pmod{p^r}$

Romeo Meštrović, Kotor

(Received July 23, 2010)

Abstract. In the paper we discuss the following type congruences:

$$\binom{np^k}{mp^k} \equiv \binom{m}{n} \pmod{p^r},$$

where p is a prime, n, m, k and r are various positive integers with $n \geqslant m \geqslant 1$, $k \geqslant 1$ and $r \geqslant 1$. Given positive integers k and r, denote by $W(k,r)$ the set of all primes p such that the above congruence holds for every pair of integers $n \geqslant m \geqslant 1$. Using Ljunggren's and Jacobsthal's type congruences, we establish several characterizations of sets $W(k,r)$ and inclusion relations between them for various values k and r. In particular, we prove that $W(k+i,r) = W(k-1,r)$ for all $k \geqslant 2$, $i \geqslant 0$ and $3 \leqslant r \leqslant 3k$, and $W(k,r) = W(1,r)$ for all $3 \leqslant r \leqslant 6$ and $k \geqslant 2$. We also noticed that some of these properties may be used for computational purposes related to congruences given above.

Keywords: congruence, prime powers, Lucas' theorem, Wolstenholme prime, set $W(k,r)$

MSC 2010: 11B65, 11A07

1. Introduction and main result

Let p be a prime, and k and r positive integers. As noticed in ([8], Remarks, p. 76) we do not know which are the possible prime powers p^k and p^r such that the congruence

$$\binom{np^k}{mp^k} \equiv \binom{n}{m} \pmod{p^r} \tag{1.1}$$

is satisfied for every pair of integers $n \geqslant m \geqslant 1$.

The variations of the congruence (1.1) for the case $k = 1$ with $r = 1$, $r = 2$ or $r = 3$ have been investigated by many authors (see [1], [3], [5], [6], [8] and [9]). However,

the case $r \geqslant 4$ is more complicated for any given $k \geqslant 1$, and it is not still established (see [6], [7] and [10]).

It is well known that for $k = 1$ and $r = 3$ the congruence (1.1) is satisfied for any prime $p \geqslant 5$. The basic congruences for our purposes are given by the following three statements.

Proposition 1.1. *Let n and m be positive integers with $m \leqslant n$. Then for each prime p,*

$$\binom{np}{mp} \equiv \binom{n}{m} \pmod{p}. \tag{1.2}$$

If $n = n_0 + n_1 p + \ldots + n_s p^s$ and $m = m_0 + m_1 p + \ldots + m_s p^s$ are the *p-adic expansions* of n and m (so that $0 \leqslant m_i, n_i \leqslant p-1$ for each i), then by the famous *Lucas' theorem* ([5]; also see [3]),

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

Applying the above congruence to $\binom{np}{mp}$, we note that the corresponding product on the right hand side is the same as that of $\binom{n}{m}$. Hence, the congruence (1.2) holds for all n and m with $1 \leqslant m \leqslant n$.

In 1952 W. Ljunggren generalized the congruence (1.2) to the following form.

Proposition 1.2 ([1]; also see [3])**.** *Let $p \geqslant 5$ be a prime, and let n and m be positive integers with $m \leqslant n$. Then*

$$\binom{np}{mp} \equiv \binom{n}{m} \pmod{p^3}. \tag{1.3}$$

Further, the congruence (1.3) was refined by E. Jacobsthal as follows.

Proposition 1.3 ([1]; also see [4])**.** *Let $p \geqslant 5$ be a prime, and let n and m be positive integers with $m \leqslant n$. Then*

$$\binom{np}{mp} \equiv \binom{n}{m} \pmod{p^r}, \tag{1.4}$$

where r is a power of p dividing $p^3 nm(n-m)$ (this exponent r can only be increased if p divides B_{p-3}, the $(p-3)$rd Bernoulli number).

As noticed previously, the situation is more complicated for the congruence (1.4) related to modulo prime powers p^r with $r \geqslant 4$. A prime p is said to be a *Wolstenholme prime* if it satisfies the congruence $\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}$. This is equivalent to

$$\binom{2p}{p} \equiv 2 \pmod{p^4}. \tag{1.5}$$

Two known such primes are 16843 and 2124679, and by a recent result of McIntosh and Roettger [7] these primes are the only two Wolstenholme primes less than 10^9. Furthermore, McIntosh [6] conjectured that there are infinitely many Wolstenholme primes and that no prime satisfies (1.5) with $\pmod{p^5}$ instead of $\pmod{p^4}$.

Let P denote the set of all primes. Given positive integers k and r, denote by $W(k,r)$ the set of all primes p such that the congruence (1.1) holds for every pair of integers $n \geqslant m \geqslant 1$. In this paper we prove the following result.

Theorem1.1. *The following statements about the sets $W(k,r)$ are valid.*

(i) $W(1,1) = W(1,2) = P$ *and* $W(1,3) = P \setminus \{2,3\}$.

(ii) $W(1,4)$ *is a set of all Wolstenholme primes.*

(iii) *For all $k \geqslant 2$, $i \geqslant 0$ and $r \leqslant 3k$, a prime $p \geqslant 5$ is in $W(k+i,r)$ if and only if it is in $W(k-1,r)$.*

(iv) (*reduction property*). *For all $k \geqslant 2$, $i \geqslant 0$ and $3 \leqslant r \leqslant 3k$, we have $W(k+i,r) = W(k-1,r)$.*

(v) *For any $3 \leqslant r \leqslant 6$ and $k \geqslant 2$, we have $W(k,r) = W(1,r)$.*

(vi) $W(k,r) \subseteq W(k,r-1)$ *and* $W(k-1,r) \subseteq W(k,\min\{r,3k\})$.

We believe that the assertions of Theorem 1.1 may be useful for further investigation of congruences of the type (1.1). In particular, this may be related to some applications of properties (iii)–(vi) in computational purposes concerned with the examinations of such congruences.

Proof of the above theorem is given in the next section, and it is based on the auxiliary results given by the previous propositions.

2. Proof of Theorem 1.1

In order to prove Theorem 1.1, besides Propositions 1.1–1.3, we need the following results.

Lemma 2.1. *If p is a prime and n, m and k are positive integers with $m \leqslant n$, then*

$$\binom{np^k}{mp^k} \equiv \binom{n}{m} \pmod{p}. \tag{2.1}$$

P r o o f. We proceed by induction on $k \geqslant 1$ (given any fixed n and m). For $k = 1$, the congruence (2.1) is given by (1.2) of Proposition 1.1.

Now if we suppose that $\binom{np^k}{mp^k} \equiv \binom{n}{m} \pmod{p}$ for some $k \geqslant 1$, then by Proposition 1.1 and this hypothesis, we have

$$\binom{np^{k+1}}{mp^{k+1}} \equiv \binom{np^k}{mp^k} \equiv \binom{n}{m} \pmod{p}.$$

Thus, (2.1) holds for each integer $k \geqslant 1$. □

Lemma 2.2. *Let $p \geqslant 5$ be a prime, and let n, m and k be positive integers with $m \leqslant n$. Then*

$$\binom{np^k}{mp^k} \equiv \binom{n}{m} \pmod{p^3}. \tag{2.2}$$

P r o o f. By Proposition 1.2, we see that the congruence (2.2) holds for $k = 1$ and each prime $p \geqslant 5$. Now, by induction on k, we immediately obtain (2.2) as in the induction proof of Lemma 2.1. □

Lemma 2.3. *A prime p is a Wolstenholme prime if and only if*

$$\binom{np}{mp} \equiv \binom{n}{m} \pmod{p^4} \tag{2.3}$$

for all integers $n \geqslant m \geqslant 1$.

P r o o f. If (2.3) is satisfied for every integers $n \geqslant m \geqslant 1$, then (2.3) in particular holds for $n = 2$ and $m = 1$. This shows that p is a Wolstenholme prime.

Conversely, suppose that p is a Wolstenholme prime. Then by Glaisher's congruence ([2], p. 21; also cf. [6], Corollary, p. 386) a prime p is a Wolstenholme prime if and only if p divides the numerator of the Bernoulli number B_{p-3}. In this case, by Proposition 1.3, the congruence (2.3) holds for all n and m with $n \geqslant m \geqslant 1$. □

We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1. (i) Observe first that by the congruence (1.3) of Proposition 1.2, every prime $p \geqslant 5$ is in $W(1,3)$. Since $\binom{4}{2} \not\equiv \binom{2}{1} \pmod{8}$ and $\binom{6}{3} \not\equiv \binom{2}{1} \pmod{27}$, it follows that $W(1,3) = P \setminus \{2,3\}$.

By (1.2) of Proposition 1.1, we see that $W(1,1) = P$.

Note that $P \setminus \{2,3\} = W(1,3) \subseteq W(1,2)$. By the congruence (3.2) of Lemma 3.2 in [9],

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

whence we see that (1.1) holds for $p = 3$, $k = 1$ and $r = 2$. Hence, $3 \in W(1,2)$.

By (3.3) of the same lemma,

$$\binom{2n}{2m} \equiv (-1)^m \binom{n}{m} \pmod{2^{2\mathrm{ord}_2(n)+1}},$$

where $\mathrm{ord}_2(n)$ is the exponent of 2 in the prime factorization of n. If n and m are even, then from the above we see that $\binom{2n}{2m} \equiv \binom{n}{m} \pmod 8$. If $n = 2n'$ is even and $m = 2m' - 1$ is odd, then the above congruence implies that $\binom{2n}{2m} \equiv -\binom{n}{m} \pmod 4$. Since for such values n and m the exact power of 2 dividing $\binom{n}{m}$ is greater than or equal to

$$\left\lfloor \frac{2n'}{2} \right\rfloor - \left\lfloor \frac{2m'-1}{2} \right\rfloor - \left\lfloor \frac{2(n'-m')+1}{2} \right\rfloor = n' - (m'-1) - (n'-m') = 1,$$

where $\lfloor x \rfloor$ is the greatest integer less than or equal to x, it follows that $\binom{n}{m}$ is even, and so $-\binom{n}{m} \equiv \binom{n}{m} \pmod 4$. This together with the previous congruence shows that $\binom{2n}{2m} \equiv \binom{n}{m} \pmod 4$.

It remains to consider the case when n is odd. By the last congruence in the proof of Lemma 3.2 in [9] we have

$$\binom{2n}{2m} \equiv (-1)^m \binom{n}{m} - (-1)^m 2n^2 \binom{n-1}{m-1} \left(1 + \frac{1+(-1)^m}{2}\right) \pmod{2^{2\mathrm{ord}_2(n)+2}}.$$

In particular, for odd $n = 2n' - 1$ and odd $m = 2m' - 1$, we obtain

$$\binom{2(2n'-1)}{2(2m'-1)} \equiv -1 \binom{2n'-1}{2m'-1} + 2\binom{2n'-2}{2m'-2} \pmod 4.$$

From the identity

$$\binom{2n'-1}{2m'-1} = \frac{2n'-1}{2m'-1} \binom{2n'-2}{2m'-2}$$

we see that $\binom{2n'-1}{2m'-1}$ and $\binom{2n'-2}{2m'-2}$ are both even or both odd, and therefore, $2\binom{2n'-1}{2m'-1} \equiv 2\binom{2n'-2}{2m'-2} \pmod 4$. From this and the above congruence we get $\binom{2(2n'-1)}{2(2m'-1)} \equiv \binom{2n'-1}{2m'-1} \pmod 4$. The case when $n = 2n' - 1$ is odd and $m = 2m'$ is even reduces to the previous case, in view of the fact that $\binom{2(2n'-1)}{4m'} = \binom{2(2n'-1)}{2(2(n'-m')-1)}$. This shows that $\binom{2n}{2m} \equiv \binom{n}{m} \pmod 4$ for all n and m; thus $2 \in W(1,2)$, and therefore, $W(1,2) = P$.

(ii) This is immediate from Lemma 2.3.

(iii) By a result of Jacobsthal given in Proposition 1.3, we get

$$\binom{np^k}{mp^k} \equiv \binom{np^{k-1}}{mp^{k-1}} \pmod{p^{3k}} \tag{2.4}$$

for any integers $k \geqslant 1$, $n \geqslant m \geqslant 1$ and prime $p \geqslant 5$. Then by induction on $i \geqslant 0$ (cf. proof of Lemma 2.1), it follows easily from the above congruence that

$$\binom{np^{k+i}}{mp^{k+i}} \equiv \binom{np^{k-1}}{mp^{k-1}} \pmod{p^{3k}}, \quad i = 0, 1, 2, \ldots.$$

This shows that for arbitrary fixed $k \geqslant 2$, $r \leqslant 3k$ and $i \geqslant 0$, a prime $p \geqslant 5$ is in $W(k+i, r)$ if and only if it is in $W(k-1, r)$.

(iv) We will prove that $2 \notin W(k, r)$ and $3 \notin W(k, r)$ for all $k \geqslant 1$ and $r \geqslant 3$. If this is true, then (iii) immediately yields (iv).

By (3.3) of Lemma 3.2 from [9], for $p = 2$ we have

$$\binom{2n}{2m} \equiv (-1)^m \binom{n}{m} \pmod{2^{2\mathrm{ord}_2(n)+1}},$$

whence it easily follows by induction on $k \geqslant 1$ that

$$\binom{2^{k+1}}{2^k} \equiv \binom{4}{2} = 6 \pmod{8} \quad \text{for all } k \geqslant 1.$$

Thus, $\binom{2^k \cdot 2}{2^k \cdot 1} \not\equiv \binom{2}{1} \pmod{8}$, and hence $2 \notin W(k, r)$ for all $k \geqslant 1$ and $r \geqslant 3$.

Similarly, if $p = 3$, then by (3.2) of Lemma 3.2 from [9],

$$\binom{3n}{3m} \equiv \binom{n}{m} \pmod{3^{2\mathrm{ord}_2(n)+2}},$$

whence it easily follows by induction on $k \geqslant 2$ that

$$\binom{3^k \cdot 2}{3^k} \equiv \binom{6}{3} = 20 \pmod{3^4} \quad \text{for all } k \geqslant 1.$$

Thus, $\binom{3^k \cdot 2}{3^k \cdot 1} \not\equiv \binom{2}{1} \pmod{27}$ and hence, $3 \notin W(k, r)$ for all $k \geqslant 1$ and $r \geqslant 3$.

(v) The assertion (iv) with $k = 2$ yields $W(2+i, r) = W(1, r)$ for all $3 \leqslant r \leqslant 6$ and $i \geqslant 0$, as desired.

(vi) The inclusion $W(k, r) \subseteq W(k, r-1)$ is obvious, while the inclusion $W(k-1, r) \subseteq W(k, \min\{r, 3k\})$ follows directly from the congruence (2.4).

This completes the proof. □

References

[1] *V. Brun, J. O. Stubban, J. E. Fjelstad, R. Tambs Lyche, K. E. Aubert, W. Ljunggren, E. Jacobsthal*: On the divisibility of the difference between two binomial coefficients. 11. Skand. Mat.-Kongr., Trondheim *1949* (1952), 42–54.

[2] *J. W. L. Glaisher*: On the residues of the sums of the inverse powers of numbers in arithmetical progression. Quart. J. *32* (1900), 271–288.

[3] *A. Granville*: Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers. Organic mathematics. Proceedings of the workshop, Simon Fraser University, Burnaby, Canada, December 12-14, 1995. Providence, RI: American Mathematical Society. CMS Conf. Proc. *20* (1997), 253–276 (J. Borwein et al., ed.).

[4] *G. S. Kazandzidis*: Congruences on the binomial coefficients. Bull. Soc. Math. Grèce, N. Ser. *9* (1968), 1–12.

[5] *E. Lucas*: Sur les congruences des nombres eulériens et les coefficients différentiels des functions trigonométriques suivant un module premier. Bull. S. M. F. *6* (1878), 49–54. (In French.)

[6] *R. J. McIntosh*: On the converse of Wolstenholme's Theorem. Acta Arith. *71* (1995), 381–389.

[7] *R. J. McIntosh, E. L. Roettger*: A search for Fibonacci-Wieferich and Wolstenholme primes. Math. Comput. *76* (2007), 2087–2094.

[8] *R. Meštrović*: A note on the congruence $\binom{nd}{md} \equiv \binom{n}{m} \pmod{q}$. Am. Math. Mon. *116* (2009), 75–77.

[9] *Z.-W. Sun, D. M. Davis*: Combinatorial congruences modulo prime powers. Trans. Am. Math. Soc. *359* (2007), 5525–5553.

[10] *J. Zhao*: Bernoulli numbers, Wolstenholme's theorem, and p^5 variations of Lucas' theorem. J. Number Theory *123* (2007), 18–26.

Author's address: Romeo Meštrović, Department of Mathematics, Maritime Faculty, University of Montenegro, Dobrota 36, 85330 Kotor, Montenegro, e-mail: `romeo@ac.me`.