A LUCAS TYPE THEOREM MODULO PRIME POWERS

ROMEO MEŠTROVIĆ

Abstract. In this note we prove that

$$\binom{np^s}{mp^s+r} \equiv (-1)^{r-1}r^{-1}(m+1)\binom{n}{m+1}p^s \pmod{p^{s+1}}$$

where p is any prime, n, m, s and r are nonnegative integers such that $n \geq m$, $s \geq 1$, $1 \leq r \leq p^s - 1$ and r is not divisible by p. We derive a proof by induction using a multiple application of Lucas' Theorem and two basic binomial coefficient identities. As an application, we prove that a similar congruence for a prime $p \geq 5$ established in 1992 by D. F. Bailey holds for all primes p.

1. Introduction and Main Result

In 1878 É. Lucas [9] (also see [6]) proved a remarkable result which provides a simple way to compute the binomial coefficient $\binom{n}{m}$ modulo a prime p in terms of the binomial coefficients of the base-p digits of n and m: if $n = n_0 + n_1p + \cdots + n_sp^s$ and $m = m_0 + m_1p + \cdots + m_sp^s$ such that $0 \leq m_i, n_i \leq p-1$ for each i, then

$$\binom{n}{m} \equiv \prod_{i=0}^{s} \binom{n_i}{m_i} \pmod{p} \tag{1.1}$$

(with the usual convention that $\binom{0}{0} = 1$, and $\binom{l}{r} = 0$ if $l < r$). *Lucas' Theorem* is often formulated in the literature in the following equivalent form. If p is a prime, and a, b, c and d are nonnegative integers with $a, b \leq p-1$, then

$$\binom{cp+a}{dp+b} \equiv \binom{c}{d}\binom{a}{b} \pmod{p}. \tag{1.2}$$

In 1990 D. F. Bailey [1, Theorems 3 and 5] proved that under the same assumptions on a, b, c, d for each prime $p \geq 5$

$$\binom{cp^f+a}{dp^f+b} \equiv \binom{c}{d}\binom{a}{b} \pmod{p^f}$$

with $f \in \{2, 3\}$. A generalization of this Lucas-like theorem to every prime power p^f with $p \geq 5$ and $f = 2, 3, \ldots$ was discovered in 1990 by K. S. Davis and W. A. Webb [5] and independently by A. Granville [7]. In 2001 H. Hu and Z.-W. Sun [8] proved a similar congruence to (1.2) for generalized binomial coefficients defined in terms of second order recurrent sequences with initial values 0 and 1. In 2007 Z.-W. Sun and D. M. Davis [10] and in 2009 M. Chamberland and K. Dilcher [4] established analogues of Lucas' Theorem for certain classes of binomial sums.

Some Lucas type congruences were established also by Bailey. Namely, in 1991 Bailey [2, Theorem 4] proved by induction on $n \geq 0$ that

$$\binom{np}{mp+i} \equiv (m+1)\binom{n}{m+1}\binom{p}{i} \pmod{p^2} \tag{1.3}$$

where p is a prime, n, m and i are nonnegative integers with $m \leq n$ and $1 \leq i \leq p-1$.

Applying the congruence (1.3), in the same paper [2, Theorem 5] the author extended it to the congruence

$$\binom{np^2}{mp^2+kp+i} \equiv (m+1)\binom{n}{m+1}\binom{p^2}{kp+i} \pmod{p^3} \tag{1.4}$$

where $p \geq 5$ is a prime, n, m, k and i are nonnegative integers with $m \leq n$, $0 \leq k \leq p-1$ and $1 \leq i \leq p-1$.

The following year, proceeding by induction on $s \geq 1$, Bailey [3, Theorem 2.1] generalized the congruence (1.4) modulo higher powers of a prime $p \geq 5$. This congruence, extended here for all primes p (Corollary 1.2 given below), is obtained as a consequence of the following result.

Theorem 1.1. *Let p be any prime, and let n, m, s and r be nonnegative integers such that $m \leq n$, $s \geq 1$, $1 \leq r \leq p^s - 1$ and r is not divisible by p. Then*

$$\binom{np^s}{mp^s+r} \equiv (-1)^{r-1} r^{-1}(m+1)\binom{n}{m+1}p^s \pmod{p^{s+1}}. \tag{1.5}$$

(Here r^{-1} denotes the inverse of r in the field $\mathbf{Z}_p$).

Corollary 1.2. ([3, Theorem 2.1]). *Let $p \geq 5$ be a prime and let n, m and s be nonnegative integers such that $m \leq n$ and $s \geq 1$. Let $r = \sum_{j=0}^{s-1} a_j p^j$ with nonnegative integers a_j such that $1 \leq a_0 \leq p-1$ and $0 \leq a_j \leq p-1$ for all $j = 1, \ldots, s-1$. Then*

$$\binom{np^s}{mp^s+r} \equiv (m+1)\binom{n}{m+1}\binom{p^s}{r} \pmod{p^{s+1}}. \tag{1.6}$$

Remark. In the proof of Corollary 1.2, using Vandermonde's Identity, Bailey proceeds by induction on s assuming for the base of induction the cases $s = 1$ and $s = 2$, that is, the congruences (1.3) and (1.4), respectively. Recall that his inductive proof of the congruence (1.4) [1, Theorem 5] is based on Vandermonde's Identity and *Ljunggren's Congruence* (see e.g., [1, Theorem 4] or [6]) which asserts that $\binom{np}{mp} \equiv \binom{n}{m} \pmod{p^3}$ for all primes $p \geq 5$ and nonnegative integers n and m with $n \geq m$. Bailey applied the same arguments (with $\binom{np}{mp} \equiv \binom{n}{m} \pmod{p^2}$ instead of Ljunggren's Congruence) in the proof of the congruence (1.3) [1, Theorem 4].

In the next section, using only Lucas' Theorem and two basic binomial coefficient identities, we give an inductive proof of Theorem 1.1.

2. Proof of Theorem 1.1 and Corollary 1.2

Proof of Theorem 1.1. First observe that if $n = m$ then since $r \geq 1$, (1.5) reduces to the identity $0 = 0$. Thus, we can assume that p, n, m and s are arbitrary fixed integers satisfying the assumptions of Theorem 1.1 and $n \geq m+1 \geq 1$. Since by the assumptions, $1 \leq r \leq p^s - 1$ and r is not divisible by p, if $s \geq 2$ we can write $r = kp + i$ with $0 \leq k \leq p^{s-1} - 1$ and $1 \leq i \leq p-1$, and if $s = 1$, then $k = 0$ and $r = i$ with $1 \leq i \leq p-1$.

We will prove (1.5) by induction on i $(= r(\bmod p))$ in the range $1 \le i \le p-1$. For $i = 1$, using the identities $\binom{a}{b+1} = \frac{a-b}{b+1}\binom{a}{b}$ and $\binom{a}{b+1} = \frac{a}{b+1}\binom{a-1}{b}$ with $0 \le b \le a-1$, we find that

$$\begin{aligned}\binom{np^s}{mp^s+kp+1} &= \frac{(n-m)p^s-kp}{mp^s+kp+1}\binom{np^s}{mp^s+kp}\\ &= p\cdot\frac{(n-m)p^{s-1}-k}{mp^s+kp+1}\binom{np^s}{(mp^{s-1}+k)p}\\ &= p\cdot\frac{(n-m)p^{s-1}-k}{mp^s+kp+1}\cdot\frac{np^s}{(mp^{s-1}+k)p}\binom{np^s-1}{(mp^{s-1}+k)p-1}\\ &= p^s\cdot\frac{((n-m)p^{s-1}-k)n}{(mp^s+kp+1)(mp^{s-1}+k)}\binom{np^s-1}{(mp^{s-1}+k)p-1}.\end{aligned}\tag{2.1}$$

Now we consider two cases.

Case 1: $k = 0$. Then $r = 1$ and for $m = 0$ (1.5) reduces to the identity $np^s = np^s$. If $m \ge 1$, then the right hand side of (2.1) with $k = 0$ is equal to

$$p^s\cdot\frac{(n-m)n}{(mp^s+1)m}\binom{np^s-1}{mp^s-1} = p^s\cdot\frac{(n-m)n}{(mp^s+1)m}\binom{(np^{s-1}-1)p+(p-1)}{(mp^{s-1}-1)p+(p-1)},$$

which by iterating Lucas' Theorem in the form (1.2) s times and using the identity $\frac{(n-m)n}{m}\binom{n-1}{m-1} = (m+1)\binom{n}{m+1}$, gives

$$\begin{aligned}&\equiv p^s\cdot\frac{(n-m)n}{m}\binom{np^{s-1}-1}{mp^{s-1}-1} \pmod{p^{s+1}}\\ &= p^s\cdot\frac{(n-m)n}{m}\binom{(np^{s-2}-1)p+(p-1)}{(mp^{s-2}-1)p+(p-1)} \pmod{p^{s+1}}\\ &\equiv p^s\cdot\frac{(n-m)n}{m}\binom{np^{s-2}-1}{mp^{s-2}-1} \pmod{p^{s+1}} \equiv \cdots\\ &\equiv p^s\cdot\frac{(n-m)n}{m}\binom{n-1}{m-1} = (m+1)\binom{n}{m+1}p^s \pmod{p^{s+1}}.\end{aligned}$$

Comparing this with (2.1) for $k = 0$, we find that

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

This proves (1.5) with $r = 1$ (that is, with $i = 1$ and $k = 0$).

Case 2: $1 \le k \le p^{s-1}-1$. Then from $r = kp+1 \le p^s - 1$ we see that we must have $s \ge 2$. First notice that by Lucas' Theorem it follows immediately that

$$\binom{ap^f+c}{bp^f+d} \equiv \binom{a}{b}\binom{c}{d} \pmod{p},\tag{2.2}$$

where p is a prime, f, a, b, c and d are nonnegative integers such that $f \ge 1$, $c \le p^e - 1$, $d \le p^e - 1$, and $b \le a$. Similarly, by (1.1) with the usual conventions, we have

$$\binom{ap^e}{bp^e} \equiv \binom{a}{b} \pmod{p}.\tag{2.3}$$

Also notice that for each prime p and any integer j such that $0 \le j \le p-1$ we have

$$\binom{p-1}{j} = \frac{(p-1)(p-2)\cdots(p-j)}{j!} \equiv \frac{(-1)^j j!}{j!} = (-1)^j \pmod p. \tag{2.4}$$

Take $k = up^l$ where $l \ge 0$ and $u \ge 1$ are nonnegative integers such that u is not divisible by p. Then since $r = kp+1 = up^{l+1}+1 \le p^s - 1$, we see that we must have $s \ge 3$, $l \le s-2$ and $u < p^{s-1-l}$. Taking $k = up^l$ for $u = \sum_{j=0}^{s-l-2} u_j p^j$ with $0 \le u_j \le p-1$ for each $j = 0, 1, \dots, s-l-2$ and $u_0 \ge 1$ into (2.1), using Lucas' Theorem, (2.2), (2.3) and (2.4) we find that

$$\begin{aligned}
&\binom{np^s}{mp^s + up^{l+1} + 1} \\
&= p^s \cdot \frac{((n-m)p^{s-1-l} - u)n}{(mp^s + up^{l+1} + 1)(mp^{s-l-1} + u)} \binom{np^s - 1}{(mp^{s-l-1} + u)p^{l+1} - 1} \\
&\equiv p^s \cdot \frac{-un}{u} \binom{(np^{s-l-1} - 1)p^{l+1} + (p^{l+1} - 1)}{(mp^{s-l-1} + u - 1)p^{l+1} + (p^{l+1} - 1)} \pmod{p^{s+1}} \\
&\equiv -np^s \binom{np^{s-l-1} - 1}{mp^{s-l-1} + u - 1} \pmod{p^{s+1}} \\
&= -np^s \binom{(n-1)p^{s-l-1} + p^{s-l-1} - 1}{mp^{s-l-1} - 1 + \sum_{j=0}^{s-l-2} u_j p^j} \\
&= -np^s \binom{(n-1)p^{s-l-1} + \sum_{j=0}^{s-l-2} (p-1)p^j}{mp^{s-l-1} + (u_0 - 1) + \sum_{j=1}^{s-l-2} u_j p^j} \\
&\equiv -np^s \binom{(n-1)p^{s-l-1}}{mp^{s-l-1}} \binom{p-1}{u_0 - 1} \prod_{j=1}^{s-l-2} \binom{p-1}{u_j} \pmod{p^{s+1}} \\
&\equiv -np^s \binom{n-1}{m} (-1)^{-1 + \sum_{j=0}^{s-l-2} u_j} \pmod{p^{s+1}} \\
&\equiv n \binom{n-1}{m} (-1)^u p^s \pmod{p^{s+1}} \\
&\equiv (m+1) \binom{n}{m+1} (-1)^{r-1} p^s \pmod{p^{s+1}}
\end{aligned} \tag{2.5}$$

(the last two congruences are clearly satisfied since for odd prime p, $\sum_{j=0}^{s-l-2} u_j \equiv u (\bmod 2)$, and hence, $r - 1 = up^{l+1} \equiv u (\bmod 2)$, while for $p = 2$ we have $(-1)^t \equiv 1 (\bmod 2)$ for each integer t). The congruence (2.5) coincides with (1.5) for $r = up^{l+1} + 1$. This concludes the proof of the induction beginning ($i = 1$).

Now suppose that the congruence (1.5) holds for each $r = kp + i$ with $0 \le k \le p^{s-1} - 1$ and some fixed i with $1 \le i \le p - 2$; that is,

$$\binom{np^s}{mp^s + kp + i} \equiv (-1)^{kp+i-1} (kp+i)^{-1} (m+1) \binom{n}{m+1} p^s \pmod{p^{s+1}}. \tag{2.6}$$

Then using the identity $\binom{a}{b+1} = \frac{a-b}{b+1}\binom{a}{b}$ with $0 \le b \le a$ and (2.6), we find that

$$\begin{aligned}\binom{np^s}{mp^s+kp+i+1} &= \frac{(n-m)p^s-kp-i}{mp^s+kp+i+1}\binom{np^s}{mp^s+kp+i}\\ &\equiv \frac{(n-m)p^s-kp-i}{mp^s+kp+i+1}(-1)^{kp+i-1}(kp+i)^{-1}(m+1)\binom{n}{m+1}p^s \pmod{p^{s+1}}\\ &\equiv \frac{-i}{kp+i+1}(-1)^{kp+i-1}i^{-1}(m+1)\binom{n}{m+1}p^s \pmod{p^{s+1}}\\ &= (-1)^{kp+i}(kp+i+1)^{-1}(m+1)\binom{n}{m+1}p^s \pmod{p^{s+1}}.\end{aligned}$$

This proves (1.5) with r satisfying $r \equiv i+1 (\bmod\, p)$, which completes the proof of Theorem 1.1. □

Proof of Corollary 1.2. Taking $n = 1$ and $m = 0$ in the congruence (1.5) of Theorem 1.1, for all r such that $1 \le r \le p^s - 1$ and r not divisible by p, we get

$$\binom{p^s}{r} \equiv (-1)^{r-1}r^{-1}p^s \pmod{p^{s+1}}.$$

Comparing this with (1.5), we immediately obtain (1.6). □

3. Acknowledgement.

The author gratefully acknowledges the valuable comments and suggestions from the anonymous referee.

References

[1] D. F. Bailey, *Two p^3 variations of Lucas' theorem*, J. Number Theory, **35** (1990), 208–215.
[2] D. F. Bailey, *Some binomial coefficient congruences*, Appl. Math. Lett., **4** (1991), 1–5.
[3] D. F. Bailey, *More binomial coefficent congruences*, The Fibonacci Quarterly, **30.2** (1992), 121–125.
[4] M. Chamberland and K. Dilcher, *A binomial sum related to Wolstenholme's theorem*, J. Number Theory, **129** (2009), 2659–2672.
[5] K. S. Davis and W. A. Webb, *Lucas' theorem for prime powers*, European J. Combin., **11** (1990), 229–233.
[6] A. Granville, *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers*, Organic Mathematics (Burnaby, BC, 1995), CMS Conf. Proc., 20, American Mathematical Society, Providence, RI, 1997, 253–276.
[7] A. Granville, *Zaphod Beeblebrox's brain and the fifty-ninth row of Pascal's triangle*, Amer. Math. Monthly, **99** (1992), 318–331.
[8] H. Hu and Z.-W. Sun, *An extension of Lucas' theorem*, Proc. Amer. Math. Soc., **129** (2001), 3471–3478.
[9] 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.
[10] Z.-W. Sun and D. M. Davis, *Combinatorial congruences modulo prime powers*, Trans. Amer. Math. Soc., **359** (2007), 5525–5553.

MSC2010: 11B75, 11B65, 11A07, 05A10

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