Publ. Math. Debrecen
59 / 1-2 (2001), 51–56

A generalization of Lucas' congruence for q-binomial coefficients

By TIANXIN CAI (Hangzhou)

Abstract. In this paper, we generalize the Lucas' congruence for q-binomial coefficients.

1. Introduction

The famous Lucas' property for binomial coefficients is

$$\binom{n}{r} \equiv \prod_{i\geq 0} \binom{n_i}{r_i} \pmod{p}, \tag{1}$$

where and throughout this paper p is a prime, n, r are integers, their expansions in base p are given by $n = \sum_{i\geq 0} n_i p^i$ and $r = \sum_{i\geq 0} r_i p^i$, with $0 \leq n_i,\ r_i \leq p-1$ (only a finite number of the n_i's are non-zero). This relation has been generalized to many unidimensional or bidimensional sequences, such as Apéry numbers. Also, many authors have studied the values of these sequences modulo a prime power, see [1]–[8]. In this paper, we investigate whether identity (1) holds when replacing the binomial coefficient $\binom{n}{r}$ by the Gaussian binomial coefficient, i.e., the q-binomial

Mathematics Subject Classification: 11A07, 11B65, 05A10.
Key words and phrases: Lucas' property, Kummer's "carries", q-binomial coefficients.
Project supported by NNSFC and project supported by NSF of Zhejiang Province.
This work was done while the author was visiting at Department of Mathematics, the University of Georgia.

coefficient $\binom{n}{r}_q$ defined by the following formula,

$$\binom{n}{r}_q = \begin{cases} \dfrac{q^n-1}{q^r-1}\dfrac{q^{n-1}-1}{q^{r-1}-1}\cdots\dfrac{q^{n-r+1}-1}{q-1}, & \text{if } 0 < r \le n, \\ 1, & \text{if } r = 0, \\ 0, & \text{if } r < 0 \text{ or } r > n. \end{cases}$$

However, for $\binom{n}{r}_q$, (1) is not always true. For example, if $q \not\equiv 1 \pmod{p}$, $(q,p)=1$, taking $n = p\,\mathrm{ord}_p(q) - 1$, $r = 1$, it is easy to verify that

$$\binom{n}{1}_q \not\equiv \binom{\mathrm{ord}_p(q)-1}{0}_q \binom{p-1}{1}_q \pmod{p},$$

where $\mathrm{ord}_p(q)$ is the order of q modulo p, i.e., the smallest positive integer f such that

$$q^f \equiv 1 \pmod{p}.$$

Although (1) fails in general for q-binomial coefficients, Fray [2] proved an interesting result: let $d = \mathrm{ord}_p(q)$, $n = n_0 + d\sum_{i\ge1} a_i p^i$, $r = r_0 + d\sum_{i\ge1} b_i p^i$, with $0 \le n_0$, $r_0 < d$, $0 \le a_i$, $b_i \le p$, $i \ge 1$, then

$$\binom{n}{r}_q \equiv \binom{n_0}{r_0}_q \prod_{i\ge1}\binom{a_i}{b_i} \pmod{p}.$$

In this paper, we first obtain the following

Theorem 1. *If $q \ne 1$, $n = n_0 + n_1 p$, $r = r_0 + r_1 p$, $0 \le n_0$, $r_0 \le p-1$, $n_1, r_1 \ge 0$, then*

$$\binom{n}{r}_q \Big/ \binom{n_1}{r_1}_{q^p} \equiv \binom{n_0}{r_0}_q \left(\mathrm{mod}\,\frac{q^p-1}{q-1}\right). \tag{2}$$

In particular, let $q \to 1$, (2) become (1), i.e., Lucas' property (1) is a direct consequence of Theorem 1.

Proof. It is obvious that (2) is true if $n_1 < r_1$. Let $n_1 \ge r_1$, if $r_0 > n_0$, then

$$\binom{n_0}{r_0}_q = 0. \tag{3}$$

On the other hand, one has

$$\binom{n}{r}_q = \prod_{1\le i\le r} \frac{q^{n-i+1}-1}{q^i-1} \tag{4}$$

$$= \frac{\prod_{0\le j\le r_1}(q^{(n_1-j)p}-1)}{\prod_{1\le j\le r_1}(q^{jp}-1)} \frac{\prod_{n-i+1\not\equiv 0 \pmod p}(q^{n-i+1}-1)}{\prod_{i\not\equiv 0 \pmod p}(q^i-1)}.$$

The first fraction in (4) is equal to

$$\binom{n_1}{r_1}_{q^p}(q^{(n_1-r_1)p}-1) \equiv 0 \left(\mathrm{mod}\ \frac{q^p-1}{q-1}\right). \tag{5}$$

From the well-known property of the greatest common divisor: $(q^s-1, q^t-1) = q^{(s,t)}-1$, it follows that

$$\left(\prod_{\substack{1\le i\le r\\ i\not\equiv 0 \pmod p}}(q^i-1), \quad \frac{q^p-1}{q-1}\right) = 1.$$

Combining (4) and (5),

$$\binom{n}{r}_q \Big/ \binom{n_1}{r_1}_{q^p} \equiv 0 \left(\mathrm{mod}\ \frac{q^p-1}{q-1}\right). \tag{6}$$

Here we used the following property of divisibility for integers: if $c \mid a$, $(c,P)=1$, $a \equiv 0 \pmod P$, then $\frac{a}{c} \equiv 0 \pmod P$. Comparing (3) with (6), we deduce (2). If $r_0 \le n_0$, then

$$\binom{n}{r}_q \Big/ \binom{n_1}{r_1}_{q^p} = \prod_{\substack{1\le i\le r\\ n-i+1\not\equiv 0 \pmod p}}(q^{n-i+1}-1) \Big/ \prod_{\substack{1\le i\le r\\ i\not\equiv 0 \pmod p}}(q^i-1) \tag{7}$$

$$\equiv \prod_{i=1}^{r_0}\frac{q^{n_0-i+1}-1}{q^i-1}\prod_{i=1}^{p-1}\frac{(q^i-1)^{r_1}}{(q^i-1)^{r_1}} = \binom{n_0}{r_0}_q \left(\mathrm{mod}\,\frac{q^p-1}{q-1}\right).$$

Here in (7) we used the following property of divisiblity for integers: if $b \mid a$, $d \mid c$, $a \equiv c \pmod P$, $b \equiv d \pmod P$, $(b,P)=1$, then $\frac{a}{b} \equiv \frac{c}{d} \pmod P$. Therefore (2) is true. □

Next, we want to generalize (2) to modulo $(q^{p^b}-1)/(q-1)$ for any integer $b \geq 1$, in order to do this, we recall the following remarkable observation of Kummer in 1885: for any prime p and positive integers $n \geq r \geq 0$, the exact power of p that divides the binomial coefficient $\binom{n}{r}$ is given by the number of "carries" when adding r and $n-r$ in base p. Therefore, if n and r are expanded in base p as the beginning of this paper, then $p \nmid \binom{n}{r}$ means $n_i \geq r_i$ for each $i \geq 0$.

Theorem 2. *Define n'_j to be the least non-negative residue of $n \pmod{p^j}$, $j \geq 1$, if p does not divide $\binom{n}{r}$, then for any positive integer b,*

$$\binom{n}{r}_q \equiv \binom{n'_b}{r'_b}_q \binom{[n/p]}{[r/p]}_{q^p} \Big/ \binom{[n'_b/p]}{[r'_b/p]}_{q^p} \left(\bmod\ \frac{q^{p^b}-1}{q-1}\right) \tag{8}$$

in particular, if $b=1$, (8) becomes (2).

Proof. Let $n = n'_b + n''_b p^b$, $r = r'_b + r''_b p^b$, and $n''_b, r''_b \geq 0$, then

$$\binom{n}{r}_q = \prod_{1\leq i\leq r} \frac{q^{n-i+1}-1}{q^i-1} = \prod_{\substack{1\leq i\leq p^b\\ 0\leq j\leq r''_b-1}} \frac{q^{(n''_b-j-1)p^b+i}-1}{q^{jp^b+i}-1} \tag{9}$$

$$\times \frac{\prod_{1\leq i\leq n'_b}(q^{n''_b p^b+i}-1)}{\prod_{1\leq i\leq r'_b}(q^{r''_b p^b+i}-1)\prod_{1\leq i\leq n'_b-r'_b}(q^{(n''_b-r''_b)p^b+i}-1)}, \tag{10}$$

if $r''_b=0$, the right product in (9) is 1; if $r''_b>0$, the product could be split into two parts, i.e., over $i \equiv 0 \pmod p$ and $i \not\equiv 0 \pmod p$, respectively, the second part is congruent to 1 modulo $(q^{p^b}-1)/(q-1)$, here again we use the property of divisiblity for integers, hence the product is congruent to

$$\binom{n''_b p^{b-1}}{r''_b p^{b-1}}_{q^p} \left(\bmod\ \frac{q^{p^b}-1}{q-1}\right). \tag{11}$$

Noting that (11) is also true for $r''_b=0$; the fraction in (10) could be denoted by $\prod = \prod_1 / \prod_2 \prod_3$, and

$$\prod\nolimits_1 = \prod_{1\leq i\leq n'_b} \frac{q^{n''_b p^b+i}-1}{q^i-1} \prod_{1\leq i\leq n'_b}(q^i-1), \tag{12}$$

the first product on the right of (12) could be split into two parts, over $i \equiv 0 \pmod p$ and $i \not\equiv 0 \pmod p$, respectively. The first part is equal to $\binom{[n/p]}{[n'_b/p]}_{q^p}$, as for the second part, since the numerator is congruent to the denominator modulo $(q^{p^b}-1)/(q-1)$, hence

$$\prod\nolimits_1 \Big/ \binom{[n/p]}{[n'_b/p]}_{q^p} \equiv \prod_{1\le i\le n'_b}(q^i-1) \left(\mathrm{mod}\ \frac{q^{p^b}-1}{q-1}\right). \tag{13}$$

Similarly we could deal with $\prod_2$ and $\prod_3$, i.e.,

$$\prod\nolimits_2 \Big/ \binom{[r/p]}{[r'_b/p]}_{q^p} \equiv \prod_{1\le i\le r'_b}(q^i-1) \left(\mathrm{mod}\ \frac{q^{p^b}-1}{q-1}\right), \tag{14}$$

$$\prod\nolimits_3 \Big/ \binom{[(n-r)/p]}{[(n'_b-r'_b)/p]}_{q^p} \equiv \prod_{1\le i\le n'_b-r'_b}(q^i-1) \left(\mathrm{mod}\ \frac{q^{p^b}-1}{q-1}\right). \tag{15}$$

Combining (13), (14) and (15), we have

$$\begin{aligned}\prod &\equiv \frac{\binom{[n/p]}{[n'_b]}_{q^p}}{\binom{[r/p]}{[r'_b]}_{q^p}\binom{[(n-r)/p]}{[(n'_b-r'_b)/p]}_{q^p}}\ \frac{\prod_{1\le i\le n'_b}(q^i-1)}{\prod_{1\le i\le r'_b}(q^i-1)\prod_{1\le i\le n'_b-r'_b}(q^i-1)} \\ &= \binom{[n/p]}{[r/p]}_{q^p}\binom{n'_b}{r'_b}_q \Big/ \binom{[n'_b/p]}{[r'_b/p]}_{q^p}\binom{[(n-n'_b)/p]}{[(r-r'_b)/p]}_{q^p} \quad \left(\mathrm{mod}\ \frac{q^{p^b}-1}{q-1}\right),\end{aligned} \tag{16}$$

from (11) and (16), we deduce (8). □

We have three immediate consequences:

Corollary 1. *If p does not divide $\binom{n}{r}$, then for any integer $b \ge 1$.*

$$\binom{n}{r} = \binom{n'_b}{r'_b}\binom{[n/p]}{[r/p]} \Big/ \binom{[n'_b/p]}{[r'_b/p]} \pmod{p^b}.$$

This is a result of Andrew Granville [4, Proposition 2].

Corollary 2. *If p does not divide $\binom{n}{r}$ and $n \equiv r \pmod{p^b}$, then*

$$\binom{n}{r}_q \equiv \binom{[n/p]}{[r/p]}_{q^p} \left(\mathrm{mod}\ \frac{q^{p^b}-1}{q-1}\right).$$

Corollary 3. *If p does not divide $\binom{n}{r}$ and $n \equiv r \pmod{p^k}$ where $k \geq b-1$, then*

$$\binom{n}{r}_q \equiv \binom{[n/p^{k+1-b}]}{[r/p^{k+1-b}]}_{q^p} \left(\bmod \frac{q^{p^b}-1}{q-1}\right).$$

Acknowledgement. The author is grateful to Prof. ANDREW GRANVILLE for his constructive comments and valuable suggestions.

References

[1] L. CARLITZ, The coefficients of the reciprocal of $J_0(x)$, *Arch. Mat.* **6** (1955), 121–127.

[2] R. D. FRAY, Congruence properties of ordinary and q-binomial coefficients, *Duke Math. J.* **34** (1967), 467–480.

[3] I. GESSEL, Some congruences for Apéry number, *J. Number Theory* **14** (1982), 362–368.

[4] A. GRANVILLE, Zaphod Beeblebrox's brain and the fifty-ninth row of Pascal's triangle, *Amer. Math. Monthly* **99** (1992), 318–331.

[5] A. GRANVILLE, Arithmetic properties of binomial coefficients I: binomial coefficients modulo prime powers, *Canadaian Mathematical Society Conference Proceedings* **20** (1997), 253–276.

[6] D. E. KNUTH and H. S. WILF, The power of a prime that divides a generalized binomial coefficients, *J. für die reine u. angew. Math.* **319** (1989), 212–219.

[7] R. J. MCINTOSH, A generalization of a congruential property of Lucas, *Amer. Math. Monthly* **99** (1992), 231–238.

[8] D. SINGMASTER, Notes on binomial coefficients – a generalization of Lucas' congruence, *J. London Math. Soc.* **8** (1974), 545–548.

TIANXIN CAI
DEPARTMENT OF MATHEMATICS
ZHEJIANG UNIVERSITY
HANGZHOU, 310028
P.R. CHINA

E-mail: txcai@mail.hz.zj.cn

(Received March 27, 2000, revised August 28, 2000;
galley proof received June 11, 2001)