Revista Colombiana de Matemáticas
Volumen 35 (2001), páginas 61–65

Two Wolstenholme's type theorems on q-binomial coefficients

TIANXIN CAI
GILBERTO GARCÍA-PULGARÍN
Universidad de Antioquia, Medellín, COLOMBIA

ABSTRACT. In this note we prove two 'Wolstenholme-type' Theorems on q-binomial coefficients, with the help of a result on partition of integers modulo prime.

Keywords and phrases. Wolstenholme's Theorem, q-binomial coefficients, modulo prime powers.

2000 Mathematics Subject Classification. Primary: 11A07. Secondary: 11B65, 05A10.

The famous Wilson's Theorem (which actually first appeared in Leibnitz's work) states that

$$(p-1)! \equiv -1 \pmod p,$$

for all primes p. Babbage noticed in 1819 that

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

for all primes $p \geq 3$, and Wolstenholme proved in 1862 that

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

for all primes $p \geq 5$. In 1952, Ljunggren generalized this to

$$\binom{np}{rp} \equiv \binom{n}{r} \pmod{p^3};$$

Project supported by Universidad de Antioquia.

and Jacobsthal to

$$\binom{np}{rp} \Big/ \binom{n}{r} \equiv 1 \pmod{p^a},$$

for any integers $n > r > 0$ and primes $p \geq 5$, where a is the power of p dividing $p^3nr(n-r)$. This exponent could only be increased in case $p \mid B_{p-3}$, the $(p-3)$rd Bernoulli number. Recently, Granville [1] developed several congruences which could lead to the generalization of both Wolstenholm's and Ljunggren's Theorems, as well as many other interesing congruences. For example, he showed that

$$\binom{3p}{2p} \Big/ \binom{2p}{p}^3 \equiv \binom{3}{2} \Big/ \binom{2}{1}^3 \pmod{p^5}$$

for all primes $p \geq 7$. In this paper, we study whether 'Wolstenholme-type' Theorems hold for q-binomial coefficients $\binom{n}{r}_q$, which as usual, it is defined by the following formula:

$$\binom{n}{r}_q = \begin{cases} \frac{q^n-1}{q-1}\frac{q^{n-1}-1}{q^2-1}\cdots\frac{q^{n-r+1}-1}{q^r-1}, & \text{if } 0 < r \leq n, \\ 1, & \text{if } r = 0, \\ 0, & \text{if } r < 0 \text{ or } r > n. \end{cases}$$

The first result we obtain is the following theorem:

Theorem 1. *Let $p \geq 5$ be a prime, then for any integer $q \neq 1$,*

$$\binom{2p-1}{p-1}_{q^{p^2}} \equiv 1 + K\,p^2\,\frac{q^{p^3}-1}{q^{p^2}-1} \pmod{q^{p^3}-1}, \tag{2}$$

where K is an integer only depending on p. In particular, when $q \to 1$, one derives (1) immediately from (2).

In order to prove Theorem 1, we need the following lemma.

Lemma 1. *Let $p \geq 3$ be a prime, $0 \leq k < p$. Define $f(k)$ as the number of solutions of the congruence,*

$$k \equiv i_1 + i_2 + \cdots + i_{p-1} \pmod{p},$$

with $1 \leq i_1 < i_2 < \cdots < i_{p-1} \leq 2p-1$. Then

$$f(0) - 1 = f(1) = f(2) = \cdots = f(p-1).$$

Proof. For $1 \leq m \leq 2p-1$, define $f_m(k)$ as the number of solutions of the congruence

$$k \equiv i_1 + i_2 + \cdots + i_m \pmod{p},\ 1 \leq i_1 < i_2 < \cdots < i_m \leq 2p-1. \tag{3}$$

Hence $f_{p-1}(k) = f(k)$.

Let X_k be the set of all solutions of (3) for fixed k and m. When $1 \leq k_1,\ k_2 \leq p-1$, we define a function ϕ between X_{k_1} and X_{k_2} by

$$\{i_1, i_2, \ldots, i_m\} \to \{k_2\bar{k_1}i_1, k_2\bar{k_1}i_2, \ldots, k_2\bar{k_1}i_m\},$$

where $\bar{k}$ is an associate of k, i.e., $\bar{k}k \equiv 1 \pmod{p}$.

It is easy to verify that ϕ is a bijection, since the restriction

$$1 \le i_1 < \cdots < i_m \le 2p-1$$

in (3) could be replaced by

$$1 \le i_1 \le i_2 \le \cdots \le i_m \le p$$

with at most two consecutive i's being equal and at most one i equal to p. Therefore, for any $1 \le k_1, k_2 \le p-1$, $f_m(k_1) = f_m(k_2)$; in particular,

$$f(1) = f(2) = \cdots = f(p-1). \tag{4}$$

Now we want to prove $f(0) = f(1)+1$. Define $F_m(k)$ as the number of solutions of the congruence

$$k \equiv i_1 + i_2 + \cdots + i_m \pmod{p}, \quad 1 \le i_1 < i_2 < \cdots < i_m \le 2p. \tag{5}$$

It is easy to verify that for all $1 \le m \le p-1$, $F_m(0) = F_m(1) = \cdots = F_m(p-1)$, since we could establish a bijection between Y_{k_1} and Y_{k_2} by

$$\{i_1, i_2, \ldots, i_m\} \to \{i_1 + (k_2-k_1)\bar{m},\ i_2 + (k_2-k_1)\bar{m}, \ldots, i_m + (k_2-k_1)\bar{m}\},$$

where $Y_k = \{y_k\}$ is the set of all solutions of (5). By taking $i_m = 2p$, we get that $F_m(k) - f_m(k)$ is equal to $f_{m-1}(k)$, therefore

$$\begin{aligned} f(0) - f(1) &= f_{p-1}(0) - f_{p-1} \\ &= F_{p-1}(0) - f_{p-2}(0) - (F_{p-1}(1) - f_{p-2}(1)) \\ &= -(f_{p-2}(0) - f_{p-2}(1)) = f_{p-3}(0) - f_{p-3}(1) \\ &= \cdots = -(f_1(0) - f_1(1)) = -(1-2) = 1 \end{aligned} \tag{6}$$

since p is an odd prime. Combining (4) with (6), the lemma is proved. ☑

Proof of Theorem 1. It is well known [2, Th. 348] that

$$\prod_{i=1}^{n} (1 + q_1^i x) = \sum_{k=0}^{n} \binom{n}{k}_{q_1} q_1^{\frac{k(k+1)}{2}} x^k. \tag{7}$$

Taking $n = 2p-1$, $q_1 = q^{p^2}$ and comparing the coefficients of x^{p-1} on both sides of (7), one has

$$f(0) + f(1)q_1 + \cdots + f(p-1)q_1^{p-1} \equiv \binom{2p-1}{p-1}_{q^{p^2}} \pmod{q^{p^3}-1} \tag{8}$$

(here $f(k)$ is defined as in the lemma), since $q_1^{j+p} \equiv q_1^j \pmod{q^{p^3}-1}$.

Let $q \to 1$ ($q_1 \to 1$). We derive from the lemma that

$$1 + f(1)p \equiv \binom{2p-1}{p-1} \pmod{p^3}; \tag{9}$$

by Wolstenholme's result (1) we get

$$f(1) \equiv 0 \pmod{p^2}.$$

Let $f(1) = Kp^2$. Combining (8) and (9), we deduce (2) from the lemma. ☑

The following result is a consequence of the proof of Theorem 1.

Corollary 1. *Let $p \geq 3$ be a prime and b a positive integer. If*

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

then for any integer $q \neq 1$,

$$\binom{2p-1}{p-1}_{q^{p^{b-1}}} \equiv 1 + K\,p^{b-1}\,\frac{q^{p^b}-1}{q^{p^{b-1}}-1} \pmod{q^{p^b}-1}.$$

Next, we prove a generalization of (1) modulo p^b for an arbitrary positive integer b.

Theorem 2. *Let $p \geq 3$ be a prime, $(q,p) = 1$, $q \not\equiv 1 \pmod p$. Then for any positive integer b,*

$$\binom{2p}{p}_{q^{p^{b-1}}} \Big/ \binom{2}{1}_{q^{p^b}} \equiv \binom{\frac{2(p-1)}{d}}{\frac{p-1}{d}} \pmod{p^b}, \tag{10}$$

where d is the order of q modulo p, i.e., the smallest positive integer f such that

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

Proof. Let $q_1 = q^{p^{b-1}}$. Then

$$\begin{aligned}\binom{2p}{p}_{q_1} \Big/ \binom{2}{1}_{q_1^p} &= \prod_{1\leq j\leq p-1} \frac{q_1^{p+j}-1}{q_1^j-1} \\ &= \frac{q_1^{2p-1}-1}{q_1-1} \prod_{2\leq j\leq p-1} \frac{q_1^{p-1+j}-1}{q_1^j-1}.\end{aligned} \tag{11}$$

Since $q \not\equiv 1 \pmod p$, d must be no less than 2. Moreover, d is also the order of q_1 modulo p^b; hence

$$\prod_{2\leq j\leq p-1} \frac{q_1^{p-1+j}-1}{q_1^j-1} = \prod_{1\leq j\leq \frac{p-1}{d}} \frac{q_1^{(\frac{p-1}{d}+j)d}-1}{q_1^{jd}-1} \prod_{\substack{2\leq j\leq p-1 \\ j\not\equiv 0 \pmod d}} \frac{{q_1}^{p-1+j}-1}{{q_1}^j-1}. \tag{12}$$

The first product on the rightside of (12) is equal to

$$\binom{\frac{2(p-1)}{d}}{\frac{p-1}{d}}_{q_1^d} \equiv \binom{\frac{2(p-1)}{d}}{\frac{p-1}{d}} \pmod{p^b}. \tag{13}$$

Noting that $q_1^{p-1} \equiv 1 \pmod{p^b}$ and that $q_1^j \not\equiv 1 \pmod p$ for any positive integer $j \not\equiv 0 \pmod d$, and using the property of divisibility for integers, one has

$$\frac{q_1^{2p-1}-1}{q_1-1} \equiv 1 \pmod{p^b}, \tag{14}$$

$$\prod_{\substack{2\le j\le p-1 \\ j\not\equiv 0 \pmod d}} \frac{q_1^{p-1+j}-1}{q_1^j-1} \equiv 1 \pmod{p^b}. \tag{15}$$

Combining (11) and (15), we deduce (10). ☑

As an example, 2 is a primitive root of 5 and 4 belongs to the order 2 modulo 5 and it is easy to verify that $2^{3^{b-1}} \equiv -1 \pmod{5^3}, 2^{5^{b-1}} \equiv -1 \pmod{p^b}$, then for an arbitrary positive integer b,

$$\binom{10}{5}_{57}\Big/\binom{2}{1}_{57} \equiv 2 \pmod{5^3}, \quad \binom{10}{5}_{182}\Big/\binom{2}{1}_{182} \equiv 2 \pmod{5^4},$$

$$\binom{6}{3}_{3^b-1}\Big/\binom{2}{1}_{3^b-1} \equiv 2 \pmod{3^b}, \quad \binom{10}{5}_{5^b-1}\Big/\binom{2}{1}_{5^b-1} \equiv 6 \pmod{5^b}.$$

Remark. Similarly we could study the generalization of 'Ljunggren-type' Theorems, however, it seems to be much more complicated.

Acknowledgement. The first author is grateful to Prof. Andrew Granville for his constructive comments and valuable suggestion.

References

[1] A. Granville, *Arithmetic properties of binomial coefficients I: binomial coefficients modulo prime powers*, Canadian Mathematical Society Conference Proceeding, **20** (1997), 253–276.

[2] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Clarendom Press, Oxford, Fourth Edition, 1965.

(Recibido en febrero de 2001)

Departamento de Matemáticas
Universidad de Antioquia
Medellín, COLOMBIA
e-mail: `tcai@matematicas.udea.edu.co`
e-mail: `gigarcia@e-math.ams.org`