F. T. Howard

Prime divisors of $q$-binomial coefficients

Rendiconti del Seminario Matematico della Università di Padova,
tome 48 (1972), p. 181-188

<http://www.numdam.org/item?id=RSMUP_1972__48__181_0>
Introduction.

1. The \( q \)-binomial coefficient is defined by

\[
\begin{bmatrix} n \\ k \end{bmatrix} = \prod_{i=1}^{k} \frac{q^{n-i+1}-1}{q^i-1}
\]

for \( q \) an indeterminate and \( n \) a non-negative integer. It is known that the \( q \)-binomial coefficient is a polynomial in \( q \) and that for \( q=1 \) it reduces to the ordinary binomial coefficient. For additional properties and references see [2].

In this paper we generalize some recently proved results for ordinary binomial coefficients to \( q \)-binomial coefficients. In section 2 we consider the problem of determining if there are \( q \)-binomial coefficients divisible by a specified factor, and we generalize a theorem of Simmons [5], who considered this problem for ordinary binomial coefficients. In section 3 we find formulas for the number of \( q \)-binomial coefficients divisible by a fixed power of a prime, thus generalizing results of Carlitz [1] and the author [3], [4].

In section 2 we assume the following, which we call conditions (1.1).
Let \( p_1, \ldots, p_k \) be prime numbers and let \( q \) be a rational number such that when \( q \) is reduced to its lowest terms, \( p_i \) does not divide the numerator or denominator for \( i = 1, \ldots, k \). Let \( e(i) \) be the smallest positive integer such that \( q^{e(i)} \equiv 1 \pmod{p_i} \) and let \( p_i^{h(i)} \) be the highest power of \( p_i \) dividing \( q^{e(i)} - 1 \). If \( p_i^{h(i)} = 2 \), let \( p_i^{t(i)} \) be the highest power of \( p_i \) dividing \( q + 1 \).

In section 3 we assume:

(1.2) Assume (1.1) holds, with \( k = 1 \). We use the notation \( p = p_1 \), \( e = e(1) \), \( h = h(1) \), \( t = t(1) \).

Throughout this paper we shall use the following rule, which is due to Fray [2], for determining the highest power of a prime \( p \) dividing a \( q \)-binomial coefficient. Suppose conditions (1.2) hold. Then any positive integer \( n \) can be written uniquely as

\[
(1.3) \quad n = a_0 + e(a_1 + a_2 p + \ldots + a_k p^{k-1})
\]

where \( 0 \leq a_0 < e, 0 \leq a_i < p \ (i = 1, \ldots, k) \).

Similarly

\[
(1.4) \quad r = b_0 + e(b_1 + b_2 p + \ldots + b_k p^{k-1})
\]

\[
(1.5) \quad n + r = c_0 + e(c_1 + c_2 p + \ldots + c_k p^{k-1}).
\]

We can write

\[
\begin{align*}
a_0 + b_0 &= e_0 e + c_0 \\
e_0 + a_1 + b_1 &= e_1 p + c_1 \\
&\quad \ldots \\
e_{k-2} + a_{k-1} + b_{k-1} &= e_{k-1} p + c_{k-1} \\
e_{k-1} + a_k + b_k &= c_k
\end{align*}
\]

where each \( e_i \) is either zero or one. If \( p^h > 2 \) then the highest power of \( p \) dividing \( \left\lfloor \frac{n + r}{r} \right\rfloor \) is \( p^t \) where
If $p^k = 2$ then the highest power of $p$ dividing $\binom{n + r}{r}$ is $p^s$ where

$$s = \varepsilon_0 h + \varepsilon_1 + \ldots + \varepsilon_{k-1}.$$  

2. Specified divisors of $q$-binomial coefficients. Simmons [5] has shown that if $r$ and $N$ are any positive integers then there are infinitely many $m \geq r$ such that

$$\left( \binom{m}{r}, N \right) = 1.$$  

This result can easily be generalized to $q$-binomial coefficients.

**Theorem 2.1.** Let $N$ and $r$ be positive integers and let $p_1, \ldots, p_k$ be the prime divisors of $N$. Assume conditions (1.1) hold. Then there are infinitely many $m \geq r$ such that

$$\left( \binom{m}{r}, N \right) = 1.$$  

**Proof.** For each $p_i$ we write

$$r = b_0 + e_i(b_1 + b_2 p_i + \ldots + b_{f(i)} p_i^{f(i)-1})$$

where

$$0 \leq b_0 < e_i, \ 0 \leq b_j < p_i \ (j = 1, \ldots, f(i)).$$

Let $d$ be any positive integer and let

$$m = r + d \prod_{i=1}^k e_i p_i^{f(i)}.$$  

By (1.5) and (1.6) it is clear that

$$\left( \binom{m}{r}, N \right) = 1.$$
Theorem 2.1 says that for arbitrary primes $p_1, \ldots, p_k$ there are an infinite number of positive integers $m$ such that $p_i^b$ is the highest power of $p_i$ dividing $\left\lfloor \frac{m}{r} \right\rfloor$ for $i = 1, \ldots, k$, provided (1.1) holds. It seems natural to ask the following question: If $p_1, \ldots, p_k$ are arbitrary primes and $g(1), \ldots, g(k)$ are arbitrary non-negative integers, are there an infinite number of positive integers $m$ such that $f_i^{g(i)}$ is the highest power of $p_i$ dividing $\left\lfloor \frac{m}{r} \right\rfloor$? We shall prove that the answer is always yes for ordinary binomial coefficients. It is clear that the answer is not always yes for $q$-binomial coefficients, however. For example, if $p_1 = 3$, $q = 8$, $g(1) = 1$ and $r = 1$, then $e(1) = 2$ and since

$$\left\lfloor \frac{m}{1} \right\rfloor = (8m - 1)/7$$

it is clear that $3^{e(1)}$ is not the highest power of 3 dividing $\left\lfloor \frac{m}{1} \right\rfloor$ for any $m$. In fact, by (1.5), if $p_1^{h(1)} > 2$, $r < e(1)$ and $0 < g(1) < h(1)$, then $p_1^{h(1)}$ will not be the highest power of $p_1$ dividing $\left\lfloor \frac{m}{r} \right\rfloor$ for any $m$. By (1.6), if $p_1^{h(1)} = 2$, $r = 1$, and $0 < g(1) < t(1)$ then $p_1^{e(1)}$ will not be the highest power of $p_1$ dividing $\left\lfloor \frac{m}{1} \right\rfloor$ for any $m$.

**THEOREM 2.2.** Let $r$ be a positive integer, $p_1, \ldots, p_k$ prime numbers and $g(1), \ldots, g(k)$ non-negative integers. Assume conditions (1.1) hold. If $p_i^{h(i)} > 2$, assume $r \geq e(i)$ and/or $g(i) \geq h(i)$. If $p_i^{h(i)} = 2$, assume $r > 1$ and/or $g(i) \geq t(i)$. Then if $(e(i), e(j)) = 1$ for $i \neq j$ there are infinitely many positive integers $m$ such that the highest power of $p_i$ dividing $\left\lfloor \frac{m}{r} \right\rfloor$ is $p_i^{f(i)}$ ($i = 1, \ldots, k$).

**PROOF.** We again use expansions (2.1), assuming $b_{f(i)} \neq 0$. If $r = b_0$ we say that $f(i) = 0$. Let

$$S_i = r \text{ if } g(i) = 0$$

$$= b_0 + e_i(b_1 + \ldots + b_{f(i)-1}p_i^{f(i)-2} + p_i^{f(i)+g(i)-1})$$

if $f(i) \geq 2$, $g(i) > 0$,
By the Chinese Remainder Theorem, the system of congruences

\[ \begin{align*}
\equiv b_0 + e_ip_i^{e(i)} & \quad \text{if } f(i) = 1, \ g(i) > 0, \ p_i^{h(i)} > 2, \\
\equiv e_ip_i^{e(i)+g(i)+1} & \quad \text{if } f(i) = 1, \ g(i) \geq t(i), \ p_i^{h(i)} = 2.
\end{align*} \]

has an infinite number of positive simultaneous solutions. If \( m \) is such a solution, it is clear by (1.5) and (1.6) that \( p_i^{e(i)} \) is the highest power of \( p_i \) dividing \( \left\lfloor \frac{m}{r} \right\rfloor \).

Theorem 2.2 could be stated more generally by replacing the condition that \((e(i), e(j)) = 1\) for \( i \neq j \) by the condition that congruences (2.2) have a simultaneous solution.

**COROLLARY.** Let \( N = p_1^{e(1)} \cdots p_k^{e(k)} \) be any positive integer and let \( r \) be a positive integer. If the hypotheses of Theorem 2.2 are satisfied, then there are an infinite number of positive integers \( m \) such that

\[ \left\lfloor \frac{m}{r} \right\rfloor = NM, \ M \equiv 0 \pmod{p_i} \quad (i = 1, \ldots, k). \]

We note that the conclusions of Theorem 2.2 and its corollary always hold for ordinary binomial coefficients.

3. The number of \( q \)-binomial coefficients divisible by a fixed power of a prime. L. Carlitz [1] has defined \( \theta_j(n) \) as the number of binomial coefficients

\[ \binom{n}{s} \quad (s = 0, 1, \ldots, n) \]

divisible by exactly \( p' \), where \( p \) is a prime number, and he has found formulas for \( \theta_j(n) \) for certain values of \( j \) and \( n \). The writer [3], [4] has also considered this problem. In particular, if we write
then we have the formulas

\begin{align}
\theta_0(n) &= (c_0 + 1)(c_1 + 1) \ldots (c_r + 1) \\
\theta_1(n) &= \sum_{i=0}^{r-1} (c_0 + 1) \ldots (c_{i-1} + 1)(p - c_i - 1)c_{i+1}(c_{i+2} + 1) \ldots (c_r + 1).
\end{align}

Assume that we have conditions (1.2) and let denote the number of $q$-binomial coefficients

\[
\begin{bmatrix}
  n \\
  s
\end{bmatrix} \quad (s = 0, 1, \ldots, n)
\]

divisible by exactly $p'$. Fray [2] has proved that if $n$ has expansion (1.3) then

\[
\alpha_0(n) = (a_0 + 1)(a_1 + 1) \ldots (a_k + 1)
\]

which is a special case of our next theorem.

We note that if $p > 2$ and $j > h + k + 1$, or if $p = 2$ and $j > y + k - 2$, where $y$ is $t$ if $p = 2$ and $y = 1$ if $p = 2$, $h > 1$, then

\[
\alpha_j(n) = 0.
\]

In the next theorem we assume $j \leq h + k - 1$ if $p > 2$ and $j \leq y + k - 2$ if $p = 2$.

**Theorem 3.1.** Assume (1.2) holds and $n$ is a positive integer having expansion (1.3). For $m = 1, \ldots, k$ define

\[
n_m = a_m + a_{m+1}p + \ldots + a_kp^{k-m}.
\]

If $p > 2$ then

\[
\alpha_j(n) = (a_0 + 1)\theta_j(n_1) + (e - a_0 - 1)a_1\theta_{j-h}(n_2) + \\
\quad + (e - a_0 - 1)\sum_{m=1}^{j-h} (p - a_1) \ldots (p - a_m)a_{m+1}\theta_{j-h-m}(n_{m+2}).
\]

If $p = 2$, $h > 1$, then

\[
\alpha_j(n) = \theta_j(n).
\]
If \( p^h = 2 \), then

\[
\alpha_j(n) = (a_1 + 1)\theta_j(n_2) + (1 - a_1)a_2\theta_{j-1}(n_3) + \\
+ \sum_{m=2}^{j-1} (1 - a_1)(2 - a_2) \ldots (2 - a_m)a_{m+1}\theta_{j-t-m+1}(n_{m+2}).
\]

**Proof.** If \( p > 2 \) we use (1.5). Let \( r \) have expansion (1.4). If \( \begin{pmatrix} n \\ r \end{pmatrix} \)
is to be divisible by exactly \( p^i \) then we consider the possibilities for \( \varepsilon_i \).

If \( \varepsilon_0 = 0 \) there are \( a_0 + 1 \) choices for \( b_0 \), namely

\[
b_0 = 0, 1, \ldots, a_0,
\]

and clearly, by (1.5), there are

\[
(a_0 + 1)\theta_j(n_1)
\]

ways of writing \( r \). If \( \varepsilon_0 = \ldots = \varepsilon_m = 1, \varepsilon_{m+1} \neq 1 \), then there are \( e - a_0 - 1 \) choices for \( b_0 \),

\[
b_0 = a_0 + 1, a_0 + 2, \ldots, e - 1,
\]

there are \( p - a_i \) choices for \( b_i, i = 1, \ldots, m \),

\[
b_i = a_i, a_i + 1, \ldots, p - 1,
\]

and there are \( a_{m+1} \) choices for \( b_{m+1} \),

\[
b_{m+1} = 0, \ldots, a_{m+1} - 1.
\]

By (1.5) it is clear that the number of choices for \( r \) is

\[(e - a_0 - 1)(p - a_1) \ldots (p - a_m)a_{m+1}\theta_{j-h-n}(n_{m+2}).\]

Note that we let \( \theta_{j-h-n}(n_{k+1}) = 1 \) if \( j - h - k + 1 \geq 0 \). The proof is similar for the case \( p = 2 \). Note that for this case \( e = 1, n = n_1 \).

For example, if \( p > 2 \) and either \( h > j \) or \( a_1 = \ldots = a_{j-h+1} = 0 \) then

\[
\alpha_j(n) = (a_0 + 1)\theta_j(n_1).
\]

Thus if \( p > 2 \) and \( s > j \)
Also

\[
\alpha_i(ep^r) = \theta_i(p^r) = p^{i-1}(p-1),
\]

\[
\alpha_i(eap^r) = \theta_i(ap^r) = ap^{i-1}(p-1) \quad (0 \leq a < p).
\]

Thus by (3.1) and (3.2) we have for

\[
\alpha_1(n) = (a_0 + 1)\theta_1(n_1) \text{ if } h > 1, \ p > 2,
\]

\[
= (a_0 + 1)\theta_1(n_1) + (e - a_0 - 1)a_1\theta_0(n_2) \text{ if } h = 1, \ p > 2,
\]

\[
= (a_1 + 1)\theta_1(n_2) \text{ if } p^h = 2,
\]

\[
= \theta_1(n) \text{ if } p = 2, \ h > 1.
\]

Thus by (3.1) and (3.2) we have for

\[
0 \leq a_0 < e, \ 0 \leq a_i < p \ (i = 1, 2),
\]

\[
\alpha_1(a_0 + e(a_1 + a_2p))
\]

\[
= (a_0 + 1)(p-a_1-1)a_2 \text{ if } p > 2, \ h > 1,
\]

\[
= (a_0 + 1)(p-a_1-1)a_2 + (e - a_0 - 1)a_1(a_2 + 1) \text{ if } p > 2, \ h = 1,
\]

\[
= 0 \text{ if } p^h = 2,
\]

\[
= (1 - a_1)a_2 \text{ if } p = 2, \ h > 1.
\]

By using Theorem 3.1 and the formulas for \(\theta_f(n)\) found in [1], [3] and [4], we could write out many more formulas for \(\alpha_i(n)\).

REFERENCES


Manoscritto pervenuto in redazione il 6 maggio 1972.