RESEARCH NOTES

q-ANALOGUE OF A BINOMIAL COEFFICIENT CONGRUENCE

W. EDWIN CLARK

Department of Mathematics,
University of South Florida,
Tampa, FL 33620-5700, USA
eclark@math.usf.edu
(Received November 25, 1992)

ABSTRACT. We establish a q-analogue of the congruence

\[ \binom{pa}{pb} \equiv \binom{a}{b} \pmod{p^2} \]

where p is a prime and a and b are positive integers.

KEY WORDS AND PHRASES. Binomial coefficient, partition, congruence, cyclotomic polynomial, q-analogue.

1992 AMS SUBJECT CLASSIFICATION CODES. 05A10, 05A17, 11P83

1. INTRODUCTION.

R. P. Stanley [1, Ex. 1.6 c] gives the congruence:

\[ \binom{pa}{pb} \equiv \binom{a}{b} \pmod{p^2} \]

for a prime p and positive integers a and b. In this note we establish the following q-analogue of (1): If a, b, n are positive integers with a ≥ 2

\[ \binom{na}{nb}(q) = \binom{a}{b}(q^n)^2 \pmod{\Phi_n(q)^2} \]

where \( \binom{n}{k}(q) \) is the q-binomial coefficient and \( \Phi_n(q) \) is the n-th cyclotomic polynomial in the variable q.

For typographical reasons we write \( \binom{n}{k}(q) \) instead of the more usual \( \binom{n}{k}_q \).

2. PROOF OF (2).

Taking the limit in (2) as \( q \to 1 \) one obtains

\[ \binom{na}{nb} \equiv \binom{a}{b} \pmod{\Phi_n(1)^2} \]

If n is a power of the prime p, \( \Phi_n(1) = p \), so if we take \( n = p \) in (3) we obtain Stanley's congruence (1). Unfortunately \( \Phi_n(1) = 1 \) if n has two or more distinct prime factors (see,
e.g., Lidl and Niederreiter [2], Ex. 2.57, p. 82), so (3) is trivial if \( n \) is not a prime power.

Our proof of (2) is based on the following two lemmas.

As usual we write \( \binom{n}{k} \) in place of \( \binom{n}{k}(q) \) when \( q \) is fixed.

**LEMMA 1.** For positive integers \( a, b \) and \( n \) with \( a \geq 2 \):

\[
\binom{na}{nb} = \sum_{c_1 + c_2 + \ldots + c_a = nb} \binom{n}{c_1} \binom{n}{c_2} \ldots \binom{n}{c_a} q^{f(c_1, \ldots, c_a; n)}
\]

where \( f(c_1, \ldots, c_a; n) = n(c_2 + 2c_3 + 3c_4 + \ldots + (a-1)c_a) - \sum_{1 \leq i < j \leq a} c_i c_j \)

and the \( c_i \) are non-negative integers.

**PROOF.** By the \( q \)-Chu-Vandermonde identity (Andrews [3], Th. 3.4, p. 37) for all positive integers \( x \):

\[
\binom{na}{x} = \sum_{c_1 + c_2 + \ldots + c_a = x} \binom{n}{c_1} \binom{n}{c_2} \ldots \binom{n}{c_a} q^{f(c_1, c_2; n)}
\]

From (5) it is easy to establish by induction on \( k \) that for \( 1 \leq k \leq a \), and all positive integers \( x \):

\[
\binom{na}{x} = \sum_{c_1 + c_2 + \ldots + c_k = x} \binom{n}{c_1} \binom{n}{c_2} \ldots \binom{n}{c_k} q^{f(c_1, \ldots, c_k; n)}
\]

The lemma follows if we take \( x = nb \) and \( k = a \).

**LEMMA 2.** If \( 1 \leq k \leq n-1 \), then

\[
\binom{n}{k}(q) = \Phi_n(q) \Phi_{d_1}(q) \Phi_{d_2}(q) \ldots \Phi_{d_s}(q)
\]

where \( n > d_1 > \ldots > d_s \) for some positive integer \( s \geq 0 \). In particular \( \Phi_n(q) \) is a factor of the polynomial \( \binom{n}{k}(q) \).

**PROOF.** It is known that

\[
\binom{n}{k}(q) = \frac{(q^{n-1})(q^{n-1}-1) \ldots (q^{n-k+1}-1)}{(q^{k-1})(q^{k-1}-1) \ldots (q-1)}
\]

is a polynomial over the rationals. The irreducible factors of the polynomial \( q^i - 1 \) are the cyclotomic polynomials \( \Phi_d(q) \) where \( d \) is a positive divisor of \( i \) (see, e.g., Jacobson [4], Th. 4.17, p. 272). Hence the numerator of (7) is the product of \( \Phi_d(q) \) where \( d \) divides \( i \) for \( i \in \{n-k+1, \ldots, n-1,n\} \) and the denominator is the product of \( \Phi_d(q) \) where \( d \) divides \( i \) for \( i \in \{1, \ldots, k\} \). Since \( \binom{n}{k}(q) \) is a polynomial, by unique factorization in the ring of rational polynomials in \( q \), each factor \( \Phi_d(q) \) in the denominator must be cancelled by a factor \( \Phi_d(q) \) in the numerator. Since \( n \) does not divide \( i \) for \( i \in \{1, \ldots, k\} \), \( \Phi_n(q) \) is not cancelled and so appears in the factorization of \( \binom{n}{k}(q) \).

It remains to show that the irreducible factors of \( \binom{n}{k}(q) \) are distinct, that is, for each \( d \) the number of factors of the form \( \Phi_d(q) \) in the numerator is at most one more than in the denominator. To see this let
The numbers in \[ \{1, \ldots, k\} \] divisible by \( d \) are
\[ d, 2d, 3d, \ldots, ad \] (10)
and the numbers in \[ \{n-k+1, \ldots, n\} \] divisible by \( d \) are
\[ md, (m+1)d, \ldots, bd \] (11)
where \( m \) is the least positive integer such that
\[ n - k + 1 \leq md. \] (12)

Now suppose (11) contains at least 2 more elements than (10), i.e., suppose
\[ b - m + 1 \geq a + 2. \]
then from (8) and (9) we have
\[ \frac{n-t}{d} - m + 1 \geq \frac{k-r}{d} + 2. \]
Then \( n - t - dm +d \geq k - r + 2d \) and \( n - k + r - t \geq dm + d \). It follows that
\[ dm + d \leq n - k + d - 1 \] so \( dm \leq n - k - 1 \), which contradicts (12). This proves the lemma.

REMARK. Our proof of (2) does not require that the factors in (6) are distinct, only that \( \binom{n}{k} \) is divisible by \( \Phi_n(q) \), but the fact that each irreducible factor has multiplicity one is perhaps worth noting, since the binomial coefficients are generally not square free

PROOF OF (2). By Lemma 2 since \( a \geq 2 \) the only terms on the right side of (4) that are not divisible by \( \Phi_n(q)^2 \) are those where \( c_j = n \) for \( b \) choices of \( j \) and \( c_j = 0 \) otherwise. Let \( \{i_1, i_2, \ldots, i_b\} \) be a \( b \)-subset of \( \{1, 2, \ldots, a\} \) and let
\[ c_j = \begin{cases} n & \text{for } j \in \{i_1, \ldots, i_b\} \\ 0 & \text{otherwise} \end{cases} \]
Assume that \( 1 \leq i_1 < i_2 < \ldots < i_b \leq a \), then
\[ f(c_1, \ldots, c_a \mid n) = n((i_1 - 1)n + (i_2 - 1)n + \ldots + (i_b - 1)n) - \binom{b}{2} n^2 = n^2((i_1 - 1) + (i_2 - 2) + \ldots + (i_b - b)). \]
Hence the right side of (4) is congruent modulo \( \Phi_n(q)^2 \) to
\[ \sum_{1 \leq i_1 < \ldots < i_b \leq a} n^2((i_1 - 1) + \ldots + (i_b - b)) = \sum_{0 \leq j_1 \leq \ldots \leq j_b \leq a - b} n^2(j_1 + \ldots + j_b) \] (13)
Now as is well-known [1, 3], the generating function of partitions with at most \( b \) parts each not exceeding \( a - b \) is given by
This shows that (13) may be written as

\[
\binom{a}{b}(q^n) = \sum_{0 \leq i_1 \leq \cdots \leq i_b \leq a-b} \binom{j_1 + \cdots + j_b}{x}
\]

which completes the proof of (2).

ACKNOWLEDGEMENT. I wish to thank Mourad Ismail for stimulating my interest in q-binomial coefficients and Vilmos Totik for a useful remark concerning partitions.

REFERENCES


Submit your manuscripts at
http://www.hindawi.com