Internat. J. Math. & Math. Sci.
VOL. 18 NO. 1 (1995) 197-200

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:

$$\binom{pa}{pb} \equiv \binom{a}{b} \pmod{p^2} \tag{1}$$

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 $a \geq 2$

$$\begin{bmatrix} na \\ nb \end{bmatrix}(q) \equiv \begin{bmatrix} a \\ b \end{bmatrix}(q^{n^2}) \pmod{\Phi_n(q)^2} \tag{2}$$

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

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

2. PROOF OF (2).

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

$$\binom{na}{nb} \equiv \binom{a}{b} \pmod{\Phi_n(1)^2} \tag{3}$$

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 $\begin{bmatrix} n \\ k \end{bmatrix}$ in place of $\begin{bmatrix} n \\ k \end{bmatrix}(q)$ when q is fixed.

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

$$\begin{bmatrix} na \\ nb \end{bmatrix} = \sum_{c_1 + c_2 + \dots c_a = nb} \begin{bmatrix} n \\ c_1 \end{bmatrix}\begin{bmatrix} n \\ c_2 \end{bmatrix} \cdots \begin{bmatrix} n \\ c_a \end{bmatrix} q^{f(c_1,\dots,c_a,n)} \tag{4}$$

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

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:

$$\begin{bmatrix} na \\ x \end{bmatrix} = \sum_{c_1 + c_2 = x} \begin{bmatrix} n \\ c_1 \end{bmatrix}\begin{bmatrix} n(a-1) \\ c_2 \end{bmatrix} q^{f(c_1, c_2; n)} \tag{5}$$

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

$$\begin{bmatrix} na \\ x \end{bmatrix} = \sum_{c_1 + c_2 + \dots c_k = x} \begin{bmatrix} n \\ c_1 \end{bmatrix}\begin{bmatrix} n \\ c_2 \end{bmatrix} \cdots \begin{bmatrix} n \\ c_{k-1} \end{bmatrix}\begin{bmatrix} n(a-k+1) \\ c_k \end{bmatrix} q^{f(c_1, \dots, c_k; n)}$$

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

LEMMA 2. If $1 \leq k \leq n-1$, then

$$\begin{bmatrix} n \\ k \end{bmatrix}(q) = \Phi_n(q)\Phi_{d_1}(q)\dots\Phi_{d_s}(q) \tag{6}$$

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

PROOF. It is known that

$$\begin{bmatrix} n \\ k \end{bmatrix}(q) = \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)} \tag{7}$$

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 $i \in \{n-k+1, \dots, n-1,n\}$ and the denominator is the product of $\Phi_d(q)$ where d divides i for $i \in \{1, \dots, k\}$. Since $\begin{bmatrix} n \\ k \end{bmatrix}$ 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 $i \in \{1, \dots, k\}$, $\Phi_n(q)$ is not cancelled and so appears in the factorization of $\begin{bmatrix} n \\ k \end{bmatrix}$

It remains to show that the irreducible factors of $\begin{bmatrix} n \\ k \end{bmatrix}$ 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

$$k = da + r, \quad 0 \le r \le d-1 \tag{8}$$

$$n = db + t, \quad 0 \le t \le d-1. \tag{9}$$

The numbers in $\{1, \ldots, k\}$ divisible by d are

$$d, 2d, 3d, \ldots, ad \tag{10}$$

and the numbers in $\{n-k+1, \ldots, n-1, n\}$ divisible by d are

$$md, (m+1)d, \ldots, bd \tag{11}$$

where m is the least positive integer such that

$$n - k + 1 \le md. \tag{12}$$

Now supose (11) contains at least 2 more elements than (10), i. e., suppose

$$b - m + 1 \ge a + 2.$$

then from (8) and (9) we have

$$\frac{n-t}{d} - m + 1 \ge \frac{k-r}{d} + 2.$$

Then $n - t - dm + d \ge k - r + 2d$ and $n - k + r - t \ge dm + d$. It follows that $dm + d \le n - k + d - 1$ so $dm \le n - k - 1$, which contradicts (12). This proves the lemma.

REMARK. Our proof of (2) does not require that the factors in (6) are distinct, only that $\begin{bmatrix} n \\ k \end{bmatrix}$ 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 $a \ge 2$ 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 $1 \le i_1 < i_2 < \ldots < i_b \le a$, then

$$\begin{aligned} f(c_1, \ldots, c_a; n) &= n((i_1 - 1)n + (i_2 - 1)n + \ldots + (i_b - 1)n) - \binom{b}{2} n^2 \\ &= n^2((i_1 - 1) + (i_2 - 2) + \ldots + (i_b - b)). \end{aligned}$$

Hence the right side of (4) is congruent modulo $\Phi_n(q)^2$ to

$$\sum_{1 \le i_1 < \ldots < i_b \le a} q^{n^2((i_1 - 1) + \ldots + (i_b - b))} = \sum_{0 \le j_1 \le \ldots \le j_b \le a-b} q^{n^2(j_1 + \ldots + j_b)} \tag{13}$$

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

$$\begin{bmatrix} a \\ b \end{bmatrix}(x) = \sum_{0 \le j_1 \le \ldots \le j_b \le a-b} x^{(j_1 + \ldots + j_b)}$$

This shows that (13) may be written as

$$\begin{bmatrix} a \\ b \end{bmatrix}(q^{n^2})$$

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

1. STANLEY, R. P., **Enumerative Combinatorics Volume I**, Wadsworth & Brooks/Cole, California, 1986.

2. LIDL, R. and NIEDERREITER, H., **Finite Fields, Encyclopedia of Mathematics and its Applications Volume 20,** Addison-Wesley Pub. Co., Massachusetts, 1983.

3. ANDREWS, G. E., **The Theory of Partitions, Encyclopedia of Mathematics and its Applications Volume 2** , Addison-Wesley Pub. Co., Massachusetts, 1976.

4. JACOBSON, N., **Basic Algebra I (Second Edition)**, W. H. Freeman and Company, New York, 1985.