ADVANCES IN MATHEMATICS 95, 127–143 (1992)

Congruence Properties of q-Analogs

BRUCE E. SAGAN*

Department of Mathematics, Michigan State University, East Lansing, Michigan 48824-1027

Using group actions and generating functions, we derive various arithmetic properties of the q-binomial coefficients and q-Stirling numbers. These include recurrence relations and computation of residues modulo a cyclotomic polynomial. We also obtain periodicity and non-periodicity results.

1. INTRODUCTION AND DEFINITIONS

Let $\mathbf{N}$ stand for the non-negative integers. If $n \in \mathbf{N}$ then let

$$\hat{n} = \{1, 2, ..., n\}.$$

We can define the *q-binomial coefficients* or *Gaussian polynomials* as follows. Given any word $\omega = b_1 b_2 \cdots b_n$, where the b_i are integers, an *inversion of* ω is a pair (b_i, b_j) which is out of order, i.e., $i < j$ and $b_i > b_j$. The *inversion statistic for words* is

$$\text{inv } \omega = \text{the number of inversions in } \omega.$$

For example,

$$\omega = 3\,1\,4\,5\,2\,5$$

has inversions

$$(3, 1), \quad (3, 2), \quad (4, 2), \quad \text{and} \quad (5, 2)$$

so

$$\text{inv } \omega = 4.$$

* Supported in part by NSF Grant 8805574.

0001-8708/92 $9.00

Now consider the set of all bit strings of length n with k 0's, denoted $\binom{\hat{n}}{k}$. Then the corresponding *q-binomial coefficient* is the generating function

$$\begin{bmatrix} n \\ k \end{bmatrix} = \sum_{\omega \in \binom{\hat{n}}{k}} q^{\text{inv } \omega},$$

where q is an indeterminate.

For the (*signless*) *q-Stirling numbers of the first kind* we look at the set $c[\hat{n}, k]$ of all permutations of $\hat{n}$ having exactly k disjoint cycles. If $\sigma \in c[\hat{n}, k]$, say

$$\sigma = c_1 c_2 \cdots c_k,$$

where the c_i are the cycles of σ, then we always write σ in *standard form* meaning that each c_i is written with its minimal element first and

$$1 = \min c_1 < \min c_2 < \cdots < \min c_k.$$

Now define inversions exactly as for the Gaussian polynomials (the cycle parentheses are ignored and the elements of σ treated as a linear array). To illustrate, if

$$\sigma = (1, 6, 2)(3, 5)(4)$$

then its inversions are

$$(6, 2), \quad (6, 3), \quad (6, 5), \quad (6, 4), \quad \text{and} \quad (5, 4)$$

and

$$\text{inv } \sigma = 5.$$

Taking generating functions again we obtain the q-Stirling numbers of the first kind

$$c[n, k] = \sum_{\sigma \in c[\hat{n}, k]} q^{\text{inv } \sigma}.$$

Similar considerations apply for the *q-Stirling numbers of the second kind.* This time the set is $S[\hat{n}, k]$, all partitions of $\hat{n}$ into k subsets (also called *blocks*). The *standard form* for partitions is

$$\pi = B_1/B_2/\cdots/B_k,$$

where the blocks B_i are arranged in increasing order of their minima. Here

an *inversion* is an element-block pair (b, B_j) such that $b \in B_i$, where $i < j$ and $b > \min B_j$. As an example, the partition

$$\pi = 1,\ 2,\ 6/3,\ 5/4 = B_1/B_2/B_3$$

has the inversions

$$(6, B_2), \qquad (6, B_3), \qquad \text{and} \qquad (5, B_3)$$

thus

$$\operatorname{inv} \pi = 3.$$

The generating function gives us the q-Stirling numbers of the second kind

$$S[n, k] = \sum_{\pi \in S[n, k]} q^{\operatorname{inv} \pi}.$$

As their name suggests, the Gaussian coefficients have a long and venerable history going back to Gauss. See the survey article of Blass [3] for more information. The q-Stirling numbers of the first kind were introduced in Gould's paper [15] and given an interpretation in terms of inversions by Gessel [13]. Versions of the q-Stirling numbers of the second kind were first studied by Carlitz [4, 5] and Gould [15]. Later, Milne [19] gave (essentially) the definition above. For other combinatorial descriptions of the Stirling polynomials see [11, 17, 18, 24, 28].

In the next three sections we derive various congruences for these polynomials. Our principal tool will be the use of group actions. The results will include recurrence relations, computation of residues, and (for the q-binomial coefficients) the q-analog of Lucas' theorem. Sections 5 through 7 will consider the periodicity of certain sequences of Gaussian polynomials and q-Stirling numbers. Here generating functions will come into play. Our final section will contain some open questions.

2. Congruences: Gaussian Coefficients

Combinatorial proofs of congruences using group actions have been extensively studied in [12, 14, 22, 23]. The basic idea is as follows. Let a group G act on a finite set S. Then the orbits $\mathcal{O}$ of the action partition S. Now suppose d is an integer such that $d \mid \#\mathcal{O}$ for every orbit with $\#\mathcal{O} > 1$, where the pound sign denotes cardinality. Then

$$\#S \equiv \#S^G \pmod{d},$$

where S^G is the fixed-point set of the action.

To use the same technique for q-analogs, consider a weighting wt $S \to \mathbf{N}[q]$ of S. If $T \subseteq S$ then we let the *weight of* T be

$$[T] = \sum_{t \in T} \text{wt } t.$$

Now if $p(q)$ is a polynomial such that $p(q)$ divides $[\mathcal{O}]$ for every orbit with at least two elements, then

$$[S] \equiv [S^G] \qquad (\text{mod } p(q)). \tag{1}$$

All the congruences in this and the next two sections will be obtained by specializing Eq. (1) to various sets and groups.

Let $G = C_d$ be the cyclic group of order d and pick a generator g of G. If $\omega = b_1 b_2 \cdots b_n$ is a word of length $n \geqslant d$ then we can let g act by right rotation of the first d digits

$$g\omega = b_d b_1 b_2 \cdots b_{d-1} b_{d+1} \cdots b_n.$$

This action will provide us with a recurrence for the q-binomial coefficients. In what follows, $\Phi_d = \Phi_d(q)$ is the dth cyclotomic polynomial. All congruences will be modulo Φ_d unless stated otherwise. It is interesting to note that the q-recursion holds for all d and not just primes.

THEOREM 2.1. *For all $n \geqslant d$ we have*

$$\begin{bmatrix} n \\ k \end{bmatrix} \equiv \begin{bmatrix} n-d \\ k-d \end{bmatrix} + \begin{bmatrix} n-d \\ k \end{bmatrix} \qquad (\text{mod } \Phi_d).$$

Proof. Let $S = \binom{n}{k}$ with the action above. If $\omega \in \binom{n}{k}$ then write

$$\omega = \omega_1 \omega_2,$$

where ω_1 is the first d bits of ω and ω_2 is the remaining suffix.

First we must show that $[S^G]$ is given by the right side of the recurrence. Pick $\omega \in S^G$. Then ω_1 is either all 0's or all 1's. In the former case

$$\text{inv } \omega = \text{inv } \omega_2$$

and in the latter

$$\text{inv } \omega = \text{inv } \omega_2 + kd.$$

Thus we always have

$$q^{\text{inv } \omega} \equiv q^{\text{inv } \omega_2}$$

since working mod Φ_d sets q to be a primitive dth root of unity. Furthermore,

$$\omega_2 \in \widehat{\binom{n-d}{k-d}}$$

in the first case and

$$\omega_2 \in \widehat{\binom{n-d}{k}}$$

in the second. Hence $[S^G]$ does give the right generating function.

Finally we show that any other orbit $\mathcal{O}$ has weight divisible by Φ_d. Take $\omega \in \mathcal{O}$ and suppose ω_1 contains l zeros. Then for the generator g of C_d we have

$$\operatorname{inv} g\omega \equiv \operatorname{inv} \omega + l \pmod{d} \tag{2}$$

since the number of inversions either goes up by l or goes down by $d-l$. Now if $m = \#\mathcal{O}$ then

$$[\mathcal{O}] = q^{\operatorname{inv} \omega}(q^l + q^{2l} + \cdots + q^{ml}). \tag{3}$$

But $\omega = g^m\omega$ forces $d \mid ml$ by repeated application of Eq. (2). Thus the right side of (3) is divisible by Φ_d. ∎

The q-Lucas theorem may have been known to Gauss himself, but the first published proof that we are aware of occurs in [21]. The result was subsequently rediscovered [8, 3] and a different q-analog is given in [10]. All of these proofs are algebraic in nature. The combinatorial demonstration that we give below was found earlier by Strehl and alluded to in [26]. We thank him for letting us reproduce it here. We also thank Ira Gessel for bringing some of these references to our attention.

THEOREM 2.2. *Divide n and k by d to obtain*

$$n = n_1 d + n_0,$$
$$k = k_1 d + k_0,$$

where $0 \leqslant n_0, k_0 < d$. Then

$$\begin{bmatrix} n \\ k \end{bmatrix} \equiv \binom{n_1}{k_1} \begin{bmatrix} n_0 \\ k_0 \end{bmatrix} \pmod{\Phi_d}.$$

Proof. It is easy to give an inductive proof of this result using the previous theorem. Alternatively, one can come up with a new group action.

Break $\omega = b_1 b_2 \cdots b_n \in \binom{\hat{n}}{k}$ into subwords of length d,

$$\omega = \omega_1 \omega_2 \cdots \omega_{n_1} \omega_0, \tag{4}$$

where $\omega_1 = b_1 \cdots b_d$, $\omega_2 = b_{d+1} \cdots b_{2d}$, ... and $\omega_0 = b_{n_1 d+1} \cdots b_n$. Now find the first ω_i with $i \geqslant 1$ where not all the digits are equal (if any). Let

$$g\omega = \omega_1 \cdots \omega_{i-1} \omega_i' \omega_{i+1} \cdots \omega_0,$$

where ω_i' is the rightward rotation of ω_i. If no such ω_i exists, then ω is a fixed point. For example, taking $d = 3$ and

$$\omega = 1\,1\,1,\ 0\,0\,0,\ 0\,0\,0,\ 1\,1\,0,\ 1\,0\,0,\ 1$$

we have

$$g\omega = 1\,1\,1,\ 0\,0\,0,\ 0\,0\,0,\ 0\,1\,1,\ 1\,0\,0,\ 1$$

(commas have been inserted to distinguish the ω_i).

Now consider a fixed point ω. Because the ones in $\omega_1 \cdots \omega_{n_1}$ occur in blocks of size dividible by d,

$$q^{\operatorname{inv} \omega} = q^{\operatorname{inv} \omega_0}.$$

Also, there must be k_0 zeros among the n_0 bits in ω_0 and k_1 zeros among the the remaining n_1 bits. Hence

$$[S^G] \equiv (\#\text{ of } \omega_1 \cdots \omega_{n_1}) \sum_{\omega_0 \in \binom{\hat{n}_0}{k_0}} q^{\operatorname{inv} \omega_0}$$

$$= \binom{n_1}{k_1} \begin{bmatrix} n_0 \\ k_0 \end{bmatrix}.$$

The fact that $\Phi_d \mid [\mathcal{O}]$ for larger orbits is the same as in Theorem 2.1. ∎

Everyting we have done can be extended to q-multinomial coefficients. Suppose $k_1 + k_2 + \cdots + k_l = n$; then $\binom{\hat{n}}{k_1, k_2, \ldots, k_l}$ denotes the set of all $\omega = b_1 b_2 \cdots b_n$ containing k_i copies of the integer i, $1 \leqslant i \leqslant l$. With the inversion number defined as before, let

$$\begin{bmatrix} n \\ k_1, k_2, \ldots, k_l \end{bmatrix} = \sum_{\omega \in \binom{\hat{n}}{k_1, k_2, \ldots, k_l}} q^{\operatorname{inv} \omega}.$$

It is convenient also to define

$$\begin{bmatrix} n \\ k_1, k_2, \ldots, k_l \end{bmatrix} = 0 \qquad \text{if} \quad k_1 + k_2 + \cdots + k_l \neq n.$$

As in the $q=1$ case, the multinomials factor in terms of q-binomial coefficients:

$$\begin{bmatrix} n \\ k_1, k_2, \ldots, k_l \end{bmatrix} = \begin{bmatrix} n \\ k_1 \end{bmatrix} \begin{bmatrix} n-k_1 \\ k_2 \end{bmatrix} \begin{bmatrix} n-k_1-k_2 \\ k_3 \end{bmatrix} \cdots. \tag{5}$$

THEOREM 2.3. *For all $n \geqslant d$ we have*

$$\begin{bmatrix} n \\ k_1, k_2, \ldots, k_l \end{bmatrix} \equiv \sum_{i=1}^{l} \begin{bmatrix} n-d \\ k_1, \ldots, k_i - d, \ldots, k_l \end{bmatrix} \pmod{\Phi_d}.$$

Proof. This result follows from Theorem 2.1 and Eq. (5). The proof can be given a combinatorial interpretation in terms of group actions.

As usual, write $\omega = \omega_1 \omega_2$, where ω_1 is the first d digits. Let m be the smallest integer in ω_1. Define

$$g\omega = \omega_1' \omega_2, \tag{6}$$

where ω_1' is obtained from ω_1 by the following sequence of steps.

1. Replace each element $>m$ in ω_1 by the symbol ∞.
2. Rotate the resulting word to the right one place.
3. Replace the ∞'s with the elements removed in the *same* order in which they occur in ω_1.

For example, if

$$\omega_1 = 2\ 2\ 3\ 5\ 2\ 4$$

then rotate

$$2\ 2\ \infty\ \infty\ 2\ \infty$$

to

$$\infty\ 2\ 2\ \infty\ \infty\ 2$$

and finally

$$\omega_1' = 3\ 2\ 2\ 5\ 4\ 2.$$

Now the proof follows that of Theorem 2.1. ∎

The multinomial q-Lucas theorem is

THEOREM 2.4. *Write*

$$n = n_1 d + n_0,$$
$$k_i = k_{i1} d + k_{i0},$$

where $0 \leqslant n_0,\ k_{i0} < d$ *for* $1 \leqslant i \leqslant l$. *Then*

$$\begin{bmatrix} n \\ k_1, k_2, \ldots, k_l \end{bmatrix} \equiv \binom{n_1}{k_{11}, k_{21}, \ldots, k_{l1}} \begin{bmatrix} n_0 \\ k_{10}, k_{20}, \ldots, k_{l0} \end{bmatrix} \pmod{\Phi_d}.$$

Proof. Three proofs are possible with the results at hand. One is as a corollary to Theorem 2.2 and Eq. (5). Another is by induction using Theorem 2.3. Finally, the group action used in Eq. (6) could be modified to act on the decomposition of ω in (4). Details are left to the reader. ∎

3. Congruences: q-Stirling Numbers of the Second Kind

The usual *q-analog of* $n \in \mathbf{N}$ is the polynomial

$$[n] = 1 + q + q^2 + \cdots + q^{n-1}.$$

For $n \geqslant 1$, the q-Stirling numbers of the second kind satisfy the recursion

$$S[n, k] = S[n-1, k-1] + [k]\, S[n-1, k]. \tag{7}$$

Reducing this equation modulo $[d]$ we get

Proposition 3.1. *If*

$$k \equiv k_0 \pmod{d}$$

then

$$S[n, k] \equiv S[n-1, k-1] + [k_0]\, S[n-1, k] \pmod{[d]}. \quad \blacksquare$$

We can also give a group action proof of Proposition 3.1, based on the usual combinatorial demonstration of Eq. (7), by letting the group C_d rotate the element n through the blocks of $\pi \in S[\hat{n}, k]$. This motivates the method used to derive the following somewhat more complicated recurrence.

Theorem 3.2. *For all* $n \geqslant d$ *we have*

$$S[n, k] \equiv \sum_{m=d}^{n} S[m-1, d-1]\, S[n-m, k-d] \pmod{[d]}.$$

Proof. Let g generate C_d. Given $\pi = B_1/B_2/\cdots/B_k \in S[\hat{n}, k]$, let m be the maximum element among blocks $B_1, \ldots, B_d$. If m is in block B_i then define

$$g\pi = B_1/\cdots/B_i - \{m\}/B_{i+1} \cup \{m\}/\cdots/B_k,$$

where $i+1$ is taken mod d. As an example, take $d=3$ and

$$\pi = 1,\ 2,\ 5/3,\ 8/4,\ 6/7,\ 9$$

so that $m=8$ with

$$g\pi = 1,\ 2,\ 5/3/4,\ 6,\ 8/7,\ 9$$

and

$$g^2\pi = 1,\ 2,\ 5,\ 8/3/4,\ 6/7,\ 9.$$

The only time when the action is not well-defined is when $B_d = \{m\}$, for then $g\pi$ will not have k blocks. In this case, make π a fixed point.

If π is not fixed then clearly

$$\text{inv } g\pi \equiv \text{inv } \pi - 1 \pmod{d}.$$

So $[d]$ divides $[\mathcal{O}]$, where $\mathcal{O}$ is π's orbit. If π is fixed, then the fact that $B_d = \{m\}$ with π in standard form implies that the elements in $B_1, \ldots, B_{d-1}$ are precisely $1, \ldots, m-1$. These fixed points yield the right side of the desired congruence. ∎

Equation (7) can be used to prove that the $S[n, k]$ have the generating function

$$\sum_{n \geq 0} S[n, k]\, x^n = \frac{x^k}{(1-x)(1-[2]x)\cdots(1-[k]x)}. \tag{8}$$

Theorem 3.2 can also be proved by partially reducing the last $k-d$ factors in this product. Full reduction results in the following theorem which also has a combinatorial proof.

THEOREM 3.3. *If*

$$k = k_1 d + k_0,$$

where $0 \leqslant k_0 < d$, *then*

$$\sum_{n \geqslant 0} S[n, k]\, x^n \equiv \frac{x^k}{\{(1-x)\cdots(1-[d-1]x)\}^{k_1}(1-x)\cdots(1-[k_0]x)} \pmod{[d]}.$$

Proof. Take $\pi = B_1/B_2/\cdots/B_k \in S[\hat{n}, k]$ and consider intervals of blocks

$$B_1/\cdots/B_d,\ B_{d+1}/\cdots/B_{2d},\ \ldots,\ B_{k_1 d+1}/\cdots/B_n.$$

Find the first interval with d blocks (if any) that is not fixed by the action of $g \in C_d$ as defined in the previous proof. Redefine $g\pi$ by letting g act on this interval or by fixing π if no such interval exists. The verification of the above identity should now be routine. ∎

In the case $d=2$ we can actually extract the coefficient of x^n on both sides of Theorem 3.3. This is an exercise in Stanley's text [25, p. 46, Problem 17] where he asks for a combinatorial demonstration. We provide such a proof next. A different combinatorial approach has been given by Collins and Hovey [6].

THEOREM 3.4. *For r real, let $\lfloor r \rfloor$ denote the largest integer less than or equal to r. Then*

$$S[n, k] \equiv \binom{n - \lfloor k/2 \rfloor - 1}{n-k} \pmod{[2]}.$$

Proof. Let C_2 act on $S[\hat{n}, k]$ as in Theorem 3.3. If π is a fixed point, then it must have the form

$$\pi = B_1/\{m_2\}/B_3/\{m_4\}/\cdots,$$

where B_{2i+1} consists of all elements between m_{2i} and m_{2i+2}. Thus the number of π is just the number of compositions (ordered partitions)

$$n_1 + 1 + n_3 + 1 + \cdots = n,$$

where $n_{2i+1} = \# B_{2i+1}$. But then

$$\overbrace{n_1 + n_3 + \cdots}^{\lceil k/2 \rceil} = n - \lfloor k/2 \rfloor$$

and the number of such compositions is well known to be

$$\binom{n - \lfloor k/2 \rfloor - 1}{\lceil k/2 \rceil - 1} = \binom{n - \lfloor k/2 \rfloor - 1}{n-k}. \quad \blacksquare$$

4. CONGRUENCES: q-STIRLING NUMBERS OF THE FIRST KIND

The q-Stirling numbers of the first kind satisfy

$$c[n, k] = c[n-1, k-1] + [n-1]\, c[n-1, k]. \tag{9}$$

This is proved by inserting n in every possible place in a permutation on

$n-1$ elements (while preserving standardness) and counting inversions. Modulo $[d]$ this recurrence becomes

PROPOSITION 4.1. *If*

$$n-1 \equiv m \pmod{d}$$

then

$$c[n, k] \equiv c[n-1, k-1] + [m]\, c[n-1, k] \pmod{[d]}. \quad \blacksquare$$

Proposition 4.1 can be proved by group actions in a manner similar to that for Proposition 3.1. However, we can only get an analog of the recurrence in Theorem 2.1 for $d=2$ (even though an analog exists for any prime d in the case $q=1$, see [23]).

THEOREM 4.2. *We have*

$$c[n, k] \equiv c[n-2, k-2] + c[n-2, k-1] \pmod{[2]}.$$

Proof. Consider $\sigma \in c[\hat{n}, k]$, g the generator of C_2, and the transposition $\tau = \tau_n = (n, n-1)$. Define

$$g\sigma = \tau\sigma\tau.$$

If σ is not fixed by g then

$$\operatorname{inv} g\sigma = \operatorname{inv} \sigma \pm 1$$

giving an orbit with weight divisible by $[2]$.

If σ is fixed by this action, then it must end with the cycles $(n-1)(n)$ or with $(n-1, n)$ (since σ is in standard form). These two choices give the two terms in the above recursion. $\blacksquare$

The $c[n, k]$ also satisfy the generating function

$$\sum_{k \geq 0} c[n, k]\, x^k = x(x+[1])(x+[2]) \cdots (x+[n-1]).$$

Reducing this equation modulo $[2]$ and taking coefficients of x^k (as is done in Wilf's text [29]) yields another identity that we can prove combinatorially.

THEOREM 4.3. *We have*

$$c[n, k] \equiv \binom{\lfloor n/2 \rfloor}{n-k} \pmod{[2]}.$$

Proof. Let σ and g be as in the proof of the previous theorem. Among the transpositions

$$\tau_n = (n, n-1), \qquad \tau_{n-2} = (n-2, n-3), \ldots$$

find the τ_i with largest index (if any) that does not fix σ and define

$$g\sigma = \tau_i \sigma \tau_i.$$

If σ is a fixed point, then each pair of elements $n-2i$, $n-2i-1$ for $i \geqslant 0$ must appear in a 2-cycle or two 1-cycles. Thus there are $\lfloor n/2 \rfloor$ pairs and of these we must choose $n-k$ to be 2-cycles so that the total number of cycles is k. ∎

5. Periods: Gaussian Coefficients

A sequence $(a_n)_{n \geqslant 0} = a_0, a_1, a_2, \ldots$ has *period* P if $a_{n+P} = a_n$ for all sufficiently large n. The period is *minimum* if P is the smallest positive integer with this property. We allow the elements a_n to come from any ring.

There is a simple technique using generating functions to investigate periodicity which has been used in [16, 20]. Consider $f(x) = \sum_n a_n x^n$. Then $(a_n)_{n \geqslant 0}$ has period P if and only if $(1-x^P) f(x)$ is a polynomial. Furthermore, P is minimum precisely when the factor $1-x^P$ has minimum degree.

The following proposition is not hard to prove using generating functions, or by other means.

Proposition 5.1 (Trench [27], Zabek [30]). *Let p be prime. Then the sequence*

$$\left(\binom{n}{k} \right)_{n \geqslant 0} \pmod{p}$$

has minimum period

$$P = p^m,$$

where m is the least integer such that $p^m > k$. ∎

It is perhaps not surprising that the corresponding sequence of Gaussian coefficients is not periodic modulo $[p]$ (except in special cases).

THEOREM 5.2. *If d is an arbitrary positive integer, then the sequence*

$$\left(\begin{bmatrix} n \\ k \end{bmatrix}\right)_{n \geqslant 0} \pmod{\Phi_d}$$

is not periodic unless $k < d$. In this case the minimum period is

$$P = \begin{cases} 1 & \text{if } k = 0 \\ d & \text{if } 1 \leqslant k < d. \end{cases}$$

Proof. We have the generating function

$$f(x) = \sum_{n \geqslant 0} \begin{bmatrix} n \\ k \end{bmatrix} x^n = \frac{x^k}{(1-x)(1-qx)(1-q^2x)\cdots(1-q^kx)}. \tag{10}$$

If $k \geqslant d$ then the denominator has multiple roots modulo Φ_d. But all the roots of $1 - x^P \pmod{\Phi_d}$ are distinct since it is relatively prime to its derivative. Thus $(1-x^P)f(x)$ cannot possibly be a polynomial in this case.

If $k = 0$ then clearly $P = 1$. For the remaining values of k, note that

$$(1-x)(1-qx)\cdots(1-q^{d-1}x) \equiv 1 - x^d \pmod{\Phi_d}$$

so $(1-x^d)f(x)$ is certainly a polynomial if $1 \leqslant k < d$. The degree is minimal because we always have a factor of $1-qx$ in the denominator and q has multiplicative order d. ∎

To obtain a proper q-analog of Proposition 5.1, we work in the quotient ring $\mathbf{N}[q]/(p, [p])$, where p is a prime integer. Congruences in this ring will be written as (mod p, $[p]$).

THEOREM 5.3. *Let p be prime; then the sequence*

$$\left(\begin{bmatrix} n \\ k \end{bmatrix}\right)_{n \geqslant 0} \pmod{p, [p]}$$

has minimum period

$$P = p^m,$$

where m is the least integer such that $p^m > k$.

Proof. Reducing Eq. (10) modulo $[p]$ we see that each factor in the denominator is repeated at most $\lceil (k+1)/p \rceil \leqslant p^{m-1}$ times. Thus it will factor into

$$1 - x^{p^m} \equiv (1-x^p)^{p^{m-1}} \pmod{p}.$$

To verify that this period is minimum, set $q = 1$. Hence the mod p period of the binomial coefficients must divide P. So from Proposition 5.1 and the previous paragraph they must be the same. ∎

6. Periods: q-Stirling Numbers of the Second Kind

The minimum period of the $S[n, k]$ is computed in [20]. In what follows, $o(i)$ denotes the multiplicative order of i in the integers mod p, and lcm is least common multiple.

Proposition 6.1. *Let p be prime. Then the sequence*

$$(S(n, k))_{n \geq 0} \pmod{p}$$

has minimum period

$$P = \begin{cases} \operatorname{lcm}_{1 \leq i \leq k} o(i) & \text{if } k < p \\ (p-1)\, p^m & \text{if } k \geq p, \end{cases}$$

where m is the greatest integer such that $p^m < k$. ∎

First we have the "non q-analog."

Theorem 6.2. *Let d be an arbitrary positive integer. Then the sequence*

$$(S[n, k])_{n \geq 0} \pmod{[d]}$$

is not periodic unless $k = 0, 1$ or $d = 2, 3$ and $k \leq d$. In these cases the minimum period is

$$P = \begin{cases} 1 & \text{if } k = 0, 1 \text{ or } \quad k = d = 2 \\ 6 & \text{if } k = 2, 3 \text{ and } \quad d = 3. \end{cases}$$

Proof. The generating function of interest is Eq. (8). Its denominator has repeated roots if $k > d$, scuttling periodicity in that case. If $k = 0, 1$ then the period is obviously one.

If $k \geq 2$ then the factor $1 - [2]x$ appears. In order for this to cancel into $1 - x^P$, we must have $1 + q$ equal to zero or a root of unity whenever q itself is a dth root of one. This forces $d = 2$ or 3. Verification of the minimum periods is now a routine matter. ∎

Things are more interesting when we also mod out by p.

THEOREM 6.3. *Let p be prime. Then the sequence*

$$(S[n, k])_{n \geqslant 0} \pmod{p, [p]}$$

has minimum period

$$P = \begin{cases} 1 & \text{if } k = 0, 1 \\ p \operatorname{lcm}_{1 \leqslant i \leqslant k} o(i) & \text{if } 1 < k < p \\ (p-1)\, p^m & \text{if } k \geqslant p, \end{cases}$$

where m is the least integer such that $p^m \geqslant k$.

Proof. For any non-zero $[i]$ we have

$$\begin{aligned} [i]^{p \cdot o(i)} &\equiv (1 + q^p + q^{2p} + \cdots + q^{(i-1)p})^{o(i)} && \pmod{p, [p]} \\ &\equiv i^{o(i)} && \pmod{p, [p]} \\ &\equiv 1 && \pmod{p, [p]}. \end{aligned}$$

Also $\operatorname{lcm}_{1 \leqslant i \leqslant p-1} o(i) = p-1$, so $1 - x^P$ certainly has each $1 - [i]x$ as a factor for $1 \leqslant i \leqslant k$. It also contains enough copies for the maximum multiplicity of such a factor by the same sort of argument as used in Theorem 5.3.

For minimality, first let $q = 1$ to see that P is divisible by the period of Proposition 6.1. This shows that the p-free part is correct. Now set $q = 0$ (before modding out). Thus the right side of Eq. (8) becomes $x^k/(1-x)^k$ which is the generating function for the sequence

$$\left(\binom{n-1}{k-1}\right)_{n \geqslant 0}.$$

By Proposition 5.1, this sequence has period p^m and so the power on p is also as small as possible. ∎

7. PERIODS: q-STIRLING NUMBERS OF THE FIRST KIND

The $c[n, k]$ are periodic in a trivial sort of way.

THEOREM 7.1. *Let $[d]$ be an arbitrary integer. Then*

$$c[n, k] \equiv 0 \pmod{[d]}$$

for $n \geqslant kd + 1$.

Proof. Induct on k. The case $k=0$ is trivial. By the recursion (9) and induction,

$$\begin{aligned} c[kd+1, k] &= c[kd, k-1] + [kd]\, c[kd, k] \\ &\equiv 0 \qquad (\mathrm{mod}\ [d]). \end{aligned}$$

Induction on n now shows that $c[n, k] \equiv 0$ whenever $n > kd+1$. ∎

8. Comments and Open Questions

Various questions are raised by the above work.

It is a pity that most of the congruences of Section 4 only hold modulo $[2]$. Unfortunately, rotating the d largest elements of π does not necessarily produce an orbit whose weight is divisible by $[d]$ (or even Φ_d). Thus it will be necessary to find a better group action for improved results.

Davis and Webb [7] have found a version of Lucas' Theorem that holds for arbitrary prime powers. Their proof is rather complicated and might be simplified and made more combinatorial by the use of group actions. Also, a q-analog needs to be found.

Various authors [1, 8, 9] have found congruences for the q-Eulerian numbers. Furthermore, Andrews and Foata [2] give a combinatorial proof of one of these identities using group actions. This suggests that other results from these papers could be attacked in the same manner.

We can also ask periodicity questions about the coefficients of these polynomials. For example, one can show that (for fixed i) the sequence obtained by extracting the coefficient of q^i in $(S[n, k])_{n \geq 0}$ (mod d) is periodic. Specifically, this follows easily from the recurrence (7) and the fact that there are only a finite number of residues modulo d. However, the proof gives no indication of what the period is. Maybe generating functions can be brought to bear.

References

1. G. E. Andrews and I. Gessel, Divisibility properties of the q-tangent numbers, *Proc. Amer. Math. Soc.* **68** (1978), 380–384.
2. G. E. Andrews and D. Foata, Congruences for q-secant numbers, *European J. Combin.* **1** (1980), 283–287.
3. A. Blass, Gaussian coefficients, an amateur's survey, preprint.
4. L. Carlitz, On Abelian fields, *Trans. Amer. Math. Soc.* **35** (1933), 122–136.
5. L. Carlitz, q-Bernoulli numbers and polynomials, *Duke Math. J.* **15** (1948), 987–1000.
6. K. L. Collins and M. Hovey, A bijective proof for the parity of Stirling numbers, *Ars Combin.* **31** (1991), 31–32.

7. K. S. DAVIS AND W. A. WEBB, Lucas' theorem for prime powers, *European J. Combin.*, to appear.
8. J. DÉSARMÉNIEN, Un analogue des congruences de Kummer pour les q-nombres d'Euler, *European J. Combin.* **3** (1982), 19–28.
9. D. FOATA, Further divisibility properties of the q-tangent numbers, *Proc. Amer. Math. Soc.* **81** (1981), 143–148.
10. R. D. FRAY, Congruence properties of ordinary and q-binomial coefficients, *Duke Math. J.* **34** (1967), 467–480.
11. A. M. GARSIA AND J. B. REMMEL, Q-counting rook configurations and a formula of Frobenius, *J. Combin. Theory Ser. A* **41** (1986), 246–275.
12. F. GARVAN, D. KIM AND D. STANTON, Cranks and t-cores, *Invent. Math.* **101** (1990), 1–17.
13. I. M. GESSEL, A q-analog of the exponential formula, *Discrete Math.* **40** (1982), 69–80.
14. I. M. GESEL, Combinatorial proofs of congruences, *in* "Enumeration and Design" (J. Schram, Ed.), pp. 157–197, Academic Press, Toronto, 1984.
15. H. W. GOULD, The q-Stirling numbers of the first and second kinds, *Duke Math. J.* **28** (1961), 281–289.
16. Y. H. KWONG, "Minimum Periods of Integer Sequences," Ph.D. thesis, University of Pennsylvania, 1987.
17. P. LEROUX, Reduced matrices and q-log-concavity properties of q-Stirling numbers, *J. Combin. Theory Ser. A* **54** (1990), 64–84.
18. S. C. MILNE, A q-analog of restricted growth functions, Dobinski's equality, and Charlier polynomials, *Trans. Amer. Math. Soc.* **245** (1978), 89–118.
19. S. C. MILNE, Restricted growth functions, rank row matchings of partition lattices, and q-Stirling numbers, *Adv. Math.* **43** (1982), 173–196.
20. A. NIJENHUIS AND H. S. WILF, Periodicities of partition functions and Stirling numbers modulo p, *J. Numer Theory* **25** (1987), 308–312.
21. G. OLIVE, Generalized powers, *Amer. Math. Monthly* **72** (1965), 619–627.
22. G.-C. ROTA AND B. E. SAGAN, Congruences derived from group action, *European J. Combin.* **1** (1980), 67–76.
23. B. E. SAGAN, Congruences via Abelian groups, *J. Number Theory* **20** (1985), 210–237.
24. B. E. SAGAN, A maj statistic for set partitions, *European J. Combin.* **12** (1991), 69–79.
25. R. P. STANLEY, "Enumerative Combinatorics, Vol. 1," Brooks/Cole, Monterey, California, 1986.
26. V. STREHL, Zum q-Analogon der Kongruenz von LUCAS, *in* "Séminaire Lotharingien de Combinatoire, 5ème Session" (J. Désarménien, Ed.), pp. 102–104, L'Institut de Recherche Mathématique Avancée, Strasbourg, 1982.
27. F. W. TRENCH, On the periodicities of certain sequences of residues, *Amer. Math. Monthly* **67** (1960), 652–656.
28. M. WACHS AND D. WHITE, p, q-Stirling numbers and set partition statistics, *J. Combin. Theory Ser. A* **56** (1991), 27–46.
29. H. S. WILF, "Generatingsfunctionology," Academic Press, San Diego, 1990.
30. S. ZABEK, Sur la périodicité modulo m des suites des nombres (n_k^n), *Ann. Univ. Mariae Curie-Sklodowska A* **10** (1956), 37–47.

Printed in Belgium
Uitgever: Academic Press, Inc.
Verantwoordelijke uitgever voor België:
Hubert Van Maele
Altenastraat 20, B-8310 Sint-Kruis