A q-analog of Ljunggren's binomial congruence

Armin Straub

▶ **To cite this version:**

Armin Straub. A q-analog of Ljunggren's binomial congruence. 23rd International Conference on Formal Power Series and Algebraic Combinatorics (FPSAC 2011), 2011, Reykjavik, Iceland. pp.897-902, 10.46298/dmtcs.2962 . hal-01215062

HAL Id: hal-01215062
https://inria.hal.science/hal-01215062v1

Submitted on 13 Oct 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

FPSAC 2011, Reykjavík, Iceland DMTCS proc. **AO**, 2011, 897–902

A q-analog of Ljunggren's binomial congruence

Armin Straub[1†]

[1] *Tulane University, New Orleans, LA, USA*

Abstract. We prove a q-analog of a classical binomial congruence due to Ljunggren which states that

$$\binom{ap}{bp} \equiv \binom{a}{b}$$

modulo p^3 for primes $p \geqslant 5$. This congruence subsumes and builds on earlier congruences by Babbage, Wolstenholme and Glaisher for which we recall existing q-analogs. Our congruence generalizes an earlier result of Clark.

Résumé. Nous démontrons un q-analogue d'une congruence binomiale classique de Ljunggren qui stipule:

$$\binom{ap}{bp} \equiv \binom{a}{b}$$

modulo p^3 pour p premier tel que $p \geqslant 5$. Cette congruence s'inspire d'une précédente congruence prouvée par Babbage, Wolstenholme et Glaisher pour laquelle nous présentons les q-analogues existantes. Notre congruence généralise un précédent résultat de Clark.

Keywords: q-analogs, binomial coefficients, binomial congruence

1 Introduction and notation

Recently, q-analogs of classical congruences have been studied by several authors including (Cla95), (And99), (SP07), (Pan07), (CP08), (Dil08). Here, we consider the classical congruence

$$\binom{ap}{bp} \equiv \binom{a}{b} \mod p^3 \tag{1}$$

which holds true for primes $p \geqslant 5$. This also appears as Problem 1.6 (d) in (Sta97). Congruence (1) was proved in 1952 by Ljunggren, see (Gra97), and subsequently generalized by Jacobsthal, see Remark 6.

†Partially supported by grant NSF-DMS 0713836. astraub@tulane.edu

1365–8050 © 2011 Discrete Mathematics and Theoretical Computer Science (DMTCS), Nancy, France

Let $[n]_q := 1 + q + \ldots q^{n-1}$, $[n]_q! := [n]_q[n-1]_q \cdots [1]_q$ and

$$\binom{n}{k}_q := \frac{[n]_q!}{[k]_q![n-k]_q!}$$

denote the usual q-analogs of numbers, factorials and binomial coefficients respectively. Observe that $[n]_1 = n$ so that in the case $q = 1$ we recover the usual factorials and binomial coefficients as well. Also, recall that the q-binomial coefficients are polynomials in q with nonnegative integer coefficients. An introduction to these q-analogs can be found in (Sta97).

We establish the following q-analog of (1):

Theorem 1 *For primes $p \geqslant 5$ and nonnegative integers a, b,*

$$\binom{ap}{bp}_q \equiv \binom{a}{b}_{q^{p^2}} - \binom{a}{b+1}\binom{b+1}{2}\frac{p^2-1}{12}(q^p-1)^2 \mod [p]_q^3. \tag{2}$$

The congruence (2) and similar ones to follow are to be understood over the ring of polynomials in q with integer coefficients. We remark that $p^2 - 1$ is divisible by 12 for all primes $p \geqslant 5$.

Observe that (2) is indeed a q-analog of (1): as $q \to 1$ we recover (1).

Example 2 Choosing $p = 13$, $a = 2$, and $b = 1$, we have

$$\binom{26}{13}_q = 1 + q^{169} - 14(q^{13}-1)^2 + (1+q+\ldots+q^{12})^3 f(q)$$

where $f(q) = 14 - 41q + 41q^2 - \ldots + q^{132}$ is an irreducible polynomial with integer coefficients. Upon setting $q = 1$, we obtain $\binom{26}{13} \equiv 2$ modulo 13^3.

Since our treatment very much parallels the classical case, we give a brief history of the congruence (1) in the next section before turning to the proof of Theorem 1.

2 A bit of history

A classical result of Wilson states that $(n-1)! + 1$ is divisible by n if and only if n is a prime number. "In attempting to discover some analogous expression which should be divisible by n^2, whenever n is a prime, but not divisible if n is a composite number", (Bab19), Babbage is led to the congruence

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

for primes $p \geqslant 3$. In 1862 Wolstenholme, (Wol62), discovered (3) to hold modulo p^3, "for several cases, in testing numerically a result of certain investigations, and after some trouble succeeded in proving it to hold universally" for $p \geqslant 5$. To this end, he proves the fractional congruences

$$\sum_{i=1}^{p-1} \frac{1}{i} \equiv 0 \mod p^2, \tag{4}$$

$$\sum_{i=1}^{p-1} \frac{1}{i^2} \equiv 0 \mod p \tag{5}$$

for primes $p \geqslant 5$. Using (4) and (5) he then extends Babbage's congruence (3) to hold modulo p^3:

$$\binom{2p-1}{p-1} \equiv 1 \mod p^3 \tag{6}$$

for all primes $p \geqslant 5$. Note that (6) can be rewritten as $\binom{2p}{p} \equiv 2$ modulo p^3. The further generalization of (6) to (1), according to (Gra97), was found by Ljunggren in 1952. The case $b = 1$ of (1) was obtained by Glaisher, (Gla00), in 1900.

In fact, Wolstenholme's congruence (6) is central to the further generalization (1). This is just as true when considering the q-analogs of these congruences as we will see here in Lemma 5.

A q-analog of the congruence of Babbage has been found by Clark (Cla95) who proved that

$$\binom{ap}{bp}_q \equiv \binom{a}{b}_{q^{p^2}} \mod [p]_q^2. \tag{7}$$

We generalize this congruence to obtain the q-analog (2) of Ljunggren's congruence (1). A result similar to (7) has also been given by Andrews in (And99).

Our proof of the q-analog proceeds very closely to the history just outlined. Besides the q-analog (7) of Babbage's congruence (3) we will employ q-analogs of Wolstenholme's harmonic congruences (4) and (5) which were recently supplied by Shi and Pan, (SP07):

Theorem 3 *For primes $p \geqslant 5$,*

$$\sum_{i=1}^{p-1} \frac{1}{[i]_q} \equiv -\frac{p-1}{2}(q-1) + \frac{p^2-1}{24}(q-1)^2[p]_q \mod [p]_q^2 \tag{8}$$

as well as

$$\sum_{i=1}^{p-1} \frac{1}{[i]_q^2} \equiv -\frac{(p-1)(p-5)}{12}(q-1)^2 \mod [p]_q. \tag{9}$$

This generalizes an earlier result (And99) of Andrews.

3 A q-analog of Ljunggren's congruence

In the classical case, the typical proof of Ljunggren's congruence (1) starts with the Chu-Vandermonde identity which has the following well-known q-analog:

Theorem 4

$$\binom{m+n}{k}_q = \sum_j \binom{m}{j}_q \binom{n}{k-j}_q q^{j(n-k+j)}.$$

We are now in a position to prove the q-analog of (1).

Proof of Theorem 1: As in (Cla95) we start with the identity

$$\binom{ap}{bp}_q = \sum_{c_1+\ldots+c_a=bp} \binom{p}{c_1}_q \binom{p}{c_2}_q \cdots \binom{p}{c_a}_q q^{p\sum_{1\leqslant i\leqslant a}(i-1)c_i - \sum_{1\leqslant i<j\leqslant a} c_i c_j} \tag{10}$$

which follows inductively from the q-analog of the Chu-Vandermonde identity given in Theorem 4. The summands which are not divisible by $[p]_q^2$ correspond to the c_i taking only the values 0 and p. Since each such summand is determined by the indices $1 \leqslant j_1 < j_2 < \ldots < j_b \leqslant a$ for which $c_i = p$, the total contribution of these terms is

$$\sum_{1 \leqslant j_1 < \ldots < j_b \leqslant a} q^{p^2 \sum_{k=1}^{b} (j_k - 1) - p^2 \binom{b}{2}} = \sum_{0 \leqslant i_1 \leqslant \ldots \leqslant i_b \leqslant a-b} q^{p^2 \sum_{k=1}^{b} i_k} = \binom{a}{b}_{q^{p^2}}.$$

This completes the proof of (7) given in (Cla95).

To obtain (2) we now consider those summands in (10) which are divisible by $[p]_q^2$ but not divisible by $[p]_q^3$. These correspond to all but two of the c_i taking values 0 or p. More precisely, such a summand is determined by indices $1 \leqslant j_1 < j_2 < \ldots < j_b < j_{b+1} \leqslant a$, two subindices $1 \leqslant k < \ell \leqslant b+1$, and $1 \leqslant d \leqslant p-1$ such that

$$c_i = \begin{cases} d \text{ for } i = j_k, \\ p - d \text{ for } i = j_\ell, \\ p \text{ for } i \in \{j_1, \ldots, j_{b+1}\} \backslash \{j_k, j_\ell\}, \\ 0 \text{ for } i \notin \{j_1, \ldots, j_{b+1}\}. \end{cases}$$

For each fixed choice of the j_i and k, ℓ the contribution of the corresponding summands is

$$\sum_{d=1}^{p-1} \binom{p}{d}_q \binom{p}{p-d}_q q^{p \sum_{1 \leqslant i \leqslant a} (i-1) c_i - \sum_{1 \leqslant i < j \leqslant a} c_i c_j}$$

which, using that $q^p \equiv 1$ modulo $[p]_q$, reduces modulo $[p]_q^3$ to

$$\sum_{d=1}^{p-1} \binom{p}{d}_q \binom{p}{p-d}_q q^{d^2} = \binom{2p}{p}_q - [2]_{q^{p^2}}.$$

We conclude that

$$\binom{ap}{bp}_q \equiv \binom{a}{b}_{q^{p^2}} + \binom{a}{b+1} \binom{b+1}{2} \left(\binom{2p}{p}_q - [2]_{q^{p^2}} \right) \mod [p]_q^3. \tag{11}$$

The general result therefore follows from the special case $a = 2$, $b = 1$ which is separately proved next. □

4 A q-analog of Wolstenholme's congruence

We have thus shown that, as in the classical case, the congruence (2) can be reduced, via (11), to the case $a = 2$, $b = 1$. The next result therefore is a q-analog of Wolstenholme's congruence (6).

Lemma 5 *For primes $p \geqslant 5$,*

$$\binom{2p}{p}_q \equiv [2]_{q^{p^2}} - \frac{p^2 - 1}{12} (q^p - 1)^2 \mod [p]_q^3.$$

Proof: Using that $[an]_q = [a]_{q^n}[n]_q$ and $[n+m]_q = [n]_q + q^n[m]_q$ we compute

$$\binom{2p}{p}_q = \frac{[2p]_q[2p-1]_q\cdots[p+1]_q}{[p]_q[p-1]_q\cdots[1]_q} = \frac{[2]_{q^p}}{[p-1]_q!}\prod_{k=1}^{p-1}\left([p]_q + q^p[p-k]_q\right)$$

which modulo $[p]_q^3$ reduces to (note that $[p-1]_q!$ is relatively prime to $[p]_q^3$)

$$[2]_{q^p}\left(q^{(p-1)p} + q^{(p-2)p}\sum_{1\leqslant i\leqslant p-1}\frac{[p]_q}{[i]_q} + q^{(p-3)p}\sum_{1\leqslant i<j\leqslant p-1}\frac{[p]_q[p]_q}{[i]_q[j]_q}\right). \tag{12}$$

Combining the results (8) and (9) of Shi and Pan, (SP07), given in Theorem 3, we deduce that for primes $p \geqslant 5$,

$$\sum_{1\leqslant i<j\leqslant p-1}\frac{1}{[i]_q[j]_q} \equiv \frac{(p-1)(p-2)}{6}(q-1)^2 \mod [p]_q. \tag{13}$$

Together with (8) this allows us to rewrite (12) modulo $[p]_q^3$ as

$$[2]_{q^p}\left(q^{(p-1)p} + q^{(p-2)p}\left(-\frac{p-1}{2}(q^p-1) + \frac{p^2-1}{24}(q^p-1)^2\right) + \right.$$
$$\left. + q^{(p-3)p}\frac{(p-1)(p-2)}{6}(q^p-1)^2\right).$$

Using the binomial expansion

$$q^{mp} = ((q^p-1)+1)^m = \sum_k\binom{m}{k}(q^p-1)^k$$

to reduce the terms q^{mp} as well as $[2]_{q^p} = 1+q^p$ modulo the appropriate power of $[p]_q$ we obtain

$$\binom{2p}{p}_q \equiv 2 + p(q^p-1) + \frac{(p-1)(5p-1)}{12}(q^p-1)^2 \mod [p]_q^3.$$

Since

$$[2]_{q^{p^2}} \equiv 2 + p(q^p-1) + \frac{(p-1)p}{2}(q^p-1)^2 \mod [p]_q^3$$

the result follows. □

Remark 6 Jacobsthal, see (Gra97), generalized the congruence (1) to hold modulo p^{3+r} where r is the p-adic valuation of

$$ab(a-b)\binom{a}{b} = 2a\binom{a}{b+1}\binom{b+1}{2}.$$

It would be interesting to see if this generalization has a nice analog in the q-world.

Acknowledgements

Most parts of this paper have been written during a visit of the author at Grinnell College. The author wishes to thank Marc Chamberland for his encouraging and helpful support. Partial support of grant NSF-DMS 0713836 is also thankfully acknowledged.

References

[And99] George E. Andrews. q-analogs of the binomial coefficient congruences of Babbage, Wolstenholme and Glaisher. *Discrete Math.*, 204(1):15–25, 1999.

[Bab19] Charles Babbage. Demonstration of a theorem relating to prime numbers. *Edinburgh Philosophical J.*, 1:46–49, 1819.

[Cla95] W. Edwin Clark. q-analogue of a binomial coefficient congruence. *Internat. J. Math. and Math. Sci.*, 18(1):197–200, 1995.

[CP08] Robin Chapman and Hao Pan. q-analogues of Wilson's theorem. *Int. J. Number Theory*, 4(4):539–547, 2008.

[Dil08] Karl Dilcher. Determinant expressions for q-harmonic congruences and degenerate Bernoulli numbers. *Electron. J. Combin.*, 15(1), 2008.

[Gla00] James W. L. Glaisher. Residues of binomial-theorem coefficients with respect to p^3. *Quart. J. Math., Oxford Ser.*, 31:110–124, 1900.

[Gra97] Andrew Granville. Arithmetic properties of binomial coefficients I: Binomial coefficients modulo prime powers. *CMS Conf. Proc.*, 20:253–275, 1997.

[Pan07] Hao Pan. A q-analogue of Lehmer's congruence. *Acta Arith.*, 128(4):303–318, 2007.

[SP07] Ling-Ling Shi and Hao Pan. A q-analogue of Wolstenholme's harmonic series congruence. *Amer. Math. Monthly*, 114(6):529–531, 2007.

[Sta97] Richard P. Stanley. *Enumerative Combinatorics, Volume 1*. Cambridge University Press, 1997.

[Wol62] Joseph Wolstenholme. On certain properties of prime numbers. *Quart. J. Math., Oxford Ser.*, 5:35–39, 1862.