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

\[
\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^3}
\]

modulo \(p^3\) for primes \(p \geq 5\). 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:

\[
\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^3}
\]

modulo \(p^3\) pour \(p\) premier tel que \(p \geq 5\). 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

\[
\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^3}
\]

which holds true for primes \(p \geq 5\). 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.

\(^{1}\)Partially supported by grant NSF-DMS 0713836. astrub@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 \(q\)-analsogs 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.

An introduction to these \(q\)-analogs can be found in (Sta97).

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

**Theorem 1** For primes \(p \geq 5\) and nonnegative integers \(a, b\),
\[
\binom{ap}{bp}_q \equiv \binom{a}{b}_q \cdot \left(\frac{a}{b} + \frac{a+1}{b+1}\right) \frac{p^2-1}{12} (q^p - 1)^2 \mod [p]^3.
\]
(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 \(p \geq 5\).

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 \(\binom{26}{13}_q \equiv 2\) 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
\[
\binom{2p}{p}_q \equiv 1 \mod p^2
\]
(3)
for primes \(p \geq 3\). 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 \(p \geq 5\). To this end, he proves the fractional congruences
\[
\sum_{i=1}^{p-1} \frac{1}{i} \equiv 0 \mod p^2,
\]
(4)
\[
\sum_{i=1}^{p-1} \frac{1}{i^2} \equiv 0 \mod p
\]
(5)
A $q$-analogue of Ljunggren’s binomial congruence

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

\[
\binom{2p-1}{p-1} \equiv 1 \mod p^3
\]  

(6)

for all primes $p \geq 5$. Note that (6) can be rewritten as $\binom{2p}{p} \equiv 2 \mod p^3$. 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 $q$-analogue of the congruence of Babbage has been found by Clark (Cla95) who proved that

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

(7)

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

Our proof of the $q$-analogue proceeds very closely to the history just outlined. Besides the $q$-analogue (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 $p \geq 5$,

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

(8)

as well as

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

(9)

This generalizes an earlier result (And99) of Andrews.

### 3 A $q$-analogue 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 $q$-analogue:

**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 $q$-analogue of (1).

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

\[
\binom{ap}{bp}_q = \sum_{c_1+\ldots+c_a=bp} \binom{p}{c_1}_q \binom{p}{c_2}_q \ldots \binom{p}{c_a}_q q^{\sum_{i_1<\ldots<i_{a-1}} (i_{a-1}-i_{a-2}) - \sum_{i_1<\ldots<i_{a}} c_{i_1} + c_{i_a}}
\]

(10)
which follows inductively from the $q$-analog of the Chu-Vandermonde identity given in Theorem 4. The summands which are not divisible by $[p]^2_q$ correspond to the $c_i$ taking only the values 0 and $p$. Since each such summand is determined by the indices $1 \leq j_1 < j_2 < \ldots < j_b \leq a$ for which $c_i = p$, the total contribution of these terms is

$$
\sum_{1 \leq j_1 < \ldots < j_b \leq a} q^b \sum_{k=1}^{j_k-1} q^2 \binom{a}{b} = \sum_{0 \leq i_1 < \ldots < i_b \leq a-b} q^b \sum_{k=1}^{i_k} = \binom{a}{b} q^{i^2}.
$$

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

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

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

For each fixed choice of the $j_i$ and $k, \ell$ the contribution of the corresponding summands is

$$
\sum_{d=1}^{p-1} \binom{p}{d} q^p \sum_{1 \leq i_1 \leq a} (i-1)^{c_i} - \sum_{1 \leq i \leq j_b} c_i d
$$

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

$$
\sum_{d=1}^{p-1} \binom{p}{d} q^p \sum_{1 \leq i_1 \leq a} (i-1)^{c_i} - \sum_{1 \leq i \leq j_b} c_i d
\equiv \binom{2p}{p} q^d - [2] q^{d^2}.
$$

We conclude that

$$
\binom{ap}{bp} q^a \equiv \binom{a}{b} q^{i^2} + \binom{a}{b+1} \binom{b+1}{2} \binom{2p}{p} q^d - [2] q^{d^2} \mod [p]^3_q.
$$

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

\vspace{1em}

4 \hspace{1em} 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 $p \geq 5$,

$$
\binom{2p}{p} q^a \equiv [2] q^{i^2} - \frac{p^2 - 1}{12} (q^p - 1)^2 \mod [p]^3_q.
$$
A q-analog of Ljunggren’s binomial congruence

Proof: Using that \([an]_q = [a]_q^n [n]_q\) and \([n + m]_q = [n]_q + q^n [m]_q\) we compute

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

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

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

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

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

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

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

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 \([2]_{qp} = 1 + q^p\) 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

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

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

\[
ab(a - b) \left( \frac{a}{b} \right) = 2a \left( \frac{a}{b+1} \right) \left( \frac{b+1}{2} \right).
\]

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


