A q-analog of Ljunggren’s binomial congruence

Midwest Number Theory Conference for Graduate Students and Recent Ph.D IX

University of Illinois at Urbana–Champaign

Armin Straub

October 13, 2012

University of Illinois at Urbana–Champaign
Our goal today

• Following a question of Andrews we seek a $q$-analog of:

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

For primes $p \geq 5$.

**George Andrews**

$q$-analogs of the binomial coefficient congruences of Babbage, Wolstenholme and Glaisher

Discrete Mathematics 204, 1999
Basic $q$-analogs

- The natural number $n$ has the $q$-analog:

  $$[n]_q = \frac{q^n - 1}{q - 1} = 1 + q + \ldots q^{n-1}$$

In the limit $q \to 1$ a $q$-analog reduces to the classical object.
Basic \(q\)-analogs

- The natural number \(n\) has the \(q\)-analog:

\[
[n]_q = \frac{q^n - 1}{q - 1} = 1 + q + \ldots q^{n-1}
\]

In the limit \(q \to 1\) a \(q\)-analog reduces to the classical object.

- The \(q\)-factorial:

\[
[n]_q! = [n]_q [n - 1]_q \cdots [1]_q
\]

- The \(q\)-binomial coefficient:

\[
\binom{n}{k}_q = \frac{[n]_q!}{[k]_q! [n - k]_q!} = \binom{n}{n - k}_q
\]
A $q$-binomial coefficient

\[
\binom{6}{2} = \frac{6 \cdot 5}{2} = 3 \cdot 5
\]

\[
\binom{6}{2}_q = \frac{(1 + q + q^2 + q^3 + q^5)(1 + q + q^2 + q^3 + q^4)}{1 + q}
\]
A $q$-binomial coefficient

\[
\binom{6}{2} = \frac{6 \cdot 5}{2} = 3 \cdot 5
\]

\[
\binom{6}{2}_q = \frac{(1 + q + q^2 + q^3 + q^5)(1 + q + q^2 + q^3 + q^4)}{1 + q} = (1 - q + q^2)(1 + q + q^2)(1 + q + q^2 + q^3 + q^4)
\]

\[
= \frac{[3]_q}{[5]_q}
\]

The cyclotomic polynomial $\Phi_6(q)$ becomes 1 for $q = 1$ and hence invisible in the classical world.

A $q$-analog of Ljuenggren's binomial congruence

Armin Straub
The cyclotomic polynomial $\Phi_6(q)$ becomes 1 for $q = 1$ and hence invisible in the classical world.
The $n$th cyclotomic polynomial:

$$
\Phi_n(q) = \prod_{1 \leq k < n \atop (k,n)=1} (q - \zeta^k)
$$

where $\zeta = e^{2\pi i/n}$

- This is an **irreducible** polynomial with **integer** coefficients.
  irreducibility due to Gauss — nontrivial
The $n$th cyclotomic polynomial:

$$\Phi_n(q) = \prod_{1 \leq k < n \atop (k,n) = 1} (q - \zeta^k)$$

where $\zeta = e^{2\pi i/n}$

- This is an **irreducible** polynomial with **integer** coefficients.
  - Irreducibility due to Gauss — nontrivial

- $[n]_q = \frac{q^n - 1}{q - 1} = \prod_{1 < d \mid n} \Phi_d(q)$

For primes: $[p]_q = \Phi_p(q)$
Some cyclotomic polynomials exhibited

\[\Phi_2(q) = q + 1\]
\[\Phi_3(q) = q^2 + q + 1\]
\[\Phi_6(q) = q^2 - q + 1\]
\[\Phi_9(q) = q^6 + q^3 + 1\]
\[\Phi_{21}(q) = q^{12} - q^{11} + q^9 - q^8 + q^6 - q^4 + q^3 - q + 1\]
\[\vdots\]
\[\Phi_{102}(q) = q^{32} + q^{31} - q^{29} - q^{28} + q^{26} + q^{25} - q^{23} - q^{22} + q^{20} + q^{19} - q^{17} - q^{16} - q^{15} + q^{13} + q^{12} - q^{10} - q^9 + q^7 + q^6 - q^4 - q^3 + q + 1\]
Some cyclotomic polynomials exhibited

\[ \Phi_2(q) = q + 1 \]
\[ \Phi_3(q) = q^2 + q + 1 \]
\[ \Phi_6(q) = q^2 - q + 1 \]
\[ \Phi_9(q) = q^6 + q^3 + 1 \]
\[ \Phi_{21}(q) = q^{12} - q^{11} + q^9 - q^8 + q^6 - q^4 + q^3 - q + 1 \]
\[ \vdots \]
\[ \Phi_{105}(q) = q^{48} + q^{47} + q^{46} - q^{43} - q^{42} - 2q^{41} - q^{40} - q^{39} + q^{36} + q^{35} + q^{34} + q^{33} + q^{32} + q^{31} - q^{28} - q^{26} - q^{24} - q^{22} - q^{20} + q^{17} + q^{16} + q^{15} + q^{14} + q^{13} + q^{12} - q^9 - q^8 - 2q^7 - q^6 - q^5 + q^2 + q + 1 \]
Back to $q$-binomials

- $\lfloor n \rfloor_q = \frac{q^n - 1}{q - 1} = \prod_{1<d\leq n; d|n} \Phi_d(q)$

- $\binom{n}{k}_q = \frac{[n]_q [n-1]_q \cdots [n-k+1]_q}{[k]_q [k-1]_q \cdots [1]_q}$

- How often does $\Phi_d(q)$ appear in this?
  - It appears $\left\lfloor \frac{n}{d} \right\rfloor - \left\lfloor \frac{n-k}{d} \right\rfloor - \left\lfloor \frac{k}{d} \right\rfloor$ times
Back to $q$-binomials

- $[n]_q = \frac{q^n - 1}{q - 1} = \prod_{\substack{1 < d \leq n \\ d | n}} \Phi_d(q)$

- $\binom{n}{k}_q = \frac{[n]_q [n-1]_q \cdots [n-k+1]_q}{[k]_q [k-1]_q \cdots [1]_q}$

- How often does $\Phi_d(q)$ appear in this?
  - It appears $\left\lfloor \frac{n}{d} \right\rfloor - \left\lfloor \frac{n-k}{d} \right\rfloor - \left\lfloor \frac{k}{d} \right\rfloor$ times
  - Obviously nonnegative: the $q$-binomials are indeed polynomials
  - Also at most one: square-free
  - $\binom{n}{k}_q$ always contains $\Phi_n(q)$ if $0 < k < n$.

- Good way to compute $q$-binomials
  and even get them factorized for free
The coefficients of $q$-binomial coefficients

- Here’s some $q$-binomials in **expanded** form:

  $${6 \choose 2}_q = q^8 + q^7 + 2q^6 + 2q^5 + 3q^4 + 2q^3 + 2q^2 + q + 1$$

  $${9 \choose 3}_q = q^{18} + q^{17} + 2q^{16} + 3q^{15} + 4q^{14} + 5q^{13} + 7q^{12}$$
  $$+ 7q^{11} + 8q^{10} + 8q^9 + 8q^8 + 7q^7 + 7q^6 + 5q^5$$
  $$+ 4q^4 + 3q^3 + 2q^2 + q + 1$$

- The degree of the $q$-binomial is $k(n - k)$.
- All coefficients are positive!
- In fact, the coefficients are **unimodal**.

Sylvester, 1878
The $q$-binomials can be built from the $q$-Pascal rule:

\[
\binom{n}{k}_q = \binom{n-1}{k-1}_q + q^k \binom{n-1}{k}_q
\]
The $q$-binomials can be build from the $q$-Pascal rule:

$$\binom{n}{k}_q = \binom{n-1}{k-1}_q + q^k \binom{n-1}{k}_q$$

$$\begin{array}{cccc}
1 \\
1 & 1 \\
1 & 1 + q & 1 \\
1 & 1 + q(1 + q) & (1 + q) + q^2 & 1 \\
& \vdots
\end{array}$$

$$\binom{4}{2}_q = 1 + q + q^2 + q^2(1 + q + q^2) = 1 + q + 2q^2 + q^3 + q^4$$
\[ \binom{n}{k}_q = \sum_{S \in \binom{n}{k}} q^{w(S)} \quad \text{where } w(S) = \sum_j s_j - j \]

where \( w(S) \) is the "normalized sum of \( S \)".

\[ \binom{4}{2}_q = 1 + q + 2q^2 + q^3 + q^4 \]

**EG**

\[
\begin{array}{cccccc}
\{1, 2\} & \{1, 3\} & \{1, 4\} & \{2, 3\} & \{2, 4\} & \{3, 4\} \\
\rightarrow 0 & \rightarrow 1 & \rightarrow 2 & \rightarrow 2 & \rightarrow 3 & \rightarrow 4
\end{array}
\]
\[
\binom{n}{k}_q = \sum_{S \in \binom{n}{k}} q^{w(S)} \quad \text{where } w(S) = \sum_j s_j - j
\]

\[
\binom{4}{2}_q = 1 + q + 2q^2 + q^3 + q^4
\]

The coefficient of \( q^m \) in \( \binom{n}{k}_q \) counts the number of

- \( k \)-element subsets of \( n \) whose normalized sum is \( m \)
\[ \binom{n}{k}_q = \sum_{S \in \binom{n}{k}} q^{w(S)} \text{ where } w(S) = \sum_{j} s_j - j \]

\[ w(S) = \text{“normalized sum of } S\text{”} \]

\[
\begin{align*}
\{1, 2\} & \rightarrow 0 \\
\{1, 3\} & \rightarrow 1 \\
\{1, 4\} & \rightarrow 2 \\
\{2, 3\} & \rightarrow 2 \\
\{2, 4\} & \rightarrow 3 \\
\{3, 4\} & \rightarrow 4 \\
\end{align*}
\]

\[
\binom{4}{2}_q = 1 + q + 2q^2 + q^3 + q^4
\]

The coefficient of \( q^m \) in \( \binom{n}{k}_q \) counts the number of

- \( k \)-element subsets of \( n \) whose normalized sum is \( m \)
- partitions \( \lambda \) of \( m \) whose Ferrer’s diagram fits in a \( k \times (n - k) \) box
Different representations make different properties apparent!

- Chu-Vandermonde: \( \binom{m+n}{k} = \sum_j \binom{m}{j} \binom{n}{k-j} \)
Different representations make different properties apparent!

- **Chu-Vandermonde:**
  \[
  \binom{m+n}{k} = \sum_j \binom{m}{j} \binom{n}{k-j}
  \]

- **Purely from the combinatorial representation:**
  \[
  \left[ \binom{m+n}{k} \right]_q = \sum_{S \in \binom{m+n}{k}} q^{\sum S - k(k+1)/2}
  \]
Different representations make different properties apparent!

- **Chu-Vandermonde**: \( \binom{m+n}{k} = \sum_j \binom{m}{j} \binom{n}{k-j} \)

- **Purely from the combinatorial representation**:

\[
\binom{m+n}{k}_q = \sum_{S \in \binom{m+n}{k}} q^{\sum S - k(k+1)/2} \\
= \sum_j \sum_{S_1 \in \binom{m}{j}} \sum_{S_2 \in \binom{n}{k-j}} q^{\sum S_1 + \sum S_2 + (k-j)m - k(k+1)/2}
\]
Different representations make different properties apparent!

- Chu-Vandermonde: \( \binom{m+n}{k} = \sum_j \binom{m}{j} \binom{n}{k-j} \)

- Purely from the combinatorial representation:

\[
\binom{m+n}{k}_q = \sum_{S \in \binom{m+n}{k}} q^\sum S - k(k+1)/2
\]
\[
= \sum_j \sum_{S_1 \in \binom{m}{j}} \sum_{S_2 \in \binom{n}{k-j}} q^\sum S_1 + \sum S_2 + (k-j)m - k(k+1)/2
\]
\[
= \sum_j \binom{m}{j}_q \binom{n}{k-j}_q q^{(m-j)(k-j)}
\]
Let \( q \) be a prime power.

\[
\binom{n}{k}_q = \text{number of } k\text{-dim. subspaces of } \mathbb{F}_q^n
\]

\[D4\]
Let $q$ be a prime power.

$$\binom{n}{k}_q = \text{number of } k\text{-dim. subspaces of } \mathbb{F}_q^n$$

- Number of ways to choose $k$ linearly independent vectors in $\mathbb{F}_q^n$:

$$ (q^n - 1)(q^n - q) \cdots (q^n - q^{k-1}) $$
Let $q$ be a prime power.

\[
\binom{n}{k}_q = \text{number of } k\text{-dim. subspaces of } \mathbb{F}_q^n
\]

- Number of ways to choose $k$ linearly independent vectors in $\mathbb{F}_q^n$:

\[
(q^n - 1)(q^n - q)\cdots(q^n - q^{k-1})
\]

- Hence the number of $k$-dim. subspaces of $\mathbb{F}_q^n$ is:

\[
\frac{(q^n - 1)(q^n - q)\cdots(q^n - q^{k-1})}{(q^k - 1)(q^k - q)\cdots(q^k - q^{k-1})} = \binom{n}{k}_q
\]
Suppose $yx = qxy$ where $q$ commutes with $x, y$. Then:

$$(x + y)^n = \sum_{j=0}^{n} \binom{n}{j}_q x^j y^{n-j}$$

D5
Suppose $yx = qxy$ where $q$ commutes with $x, y$. Then:

$$(x + y)^n = \sum_{j=0}^{n} \binom{n}{j}_q x^j y^{n-j}$$

$$\binom{4}{2}_q x^2 y^2 = xxyy + xyxy + xyyx + yxxy + yxyx + yyxx$$

$$= (1 + q + q^2 + q^2 + q^3 + q^4) x^2 y^2$$
Suppose $yx = qxy$ where $q$ commutes with $x, y$. Then:

$$(x + y)^n = \sum_{j=0}^{n} \binom{n}{j} q^j y^{n-j} x^{j}$$

\[\binom{4}{2} q^2 y^2 = xxyy + xyxy + xyyx + yxxx + yxyx + yyxx\]

\[= (1 + q + q^2 + q^3 + q^4)x^2y^2\]

- Let $X \cdot f(x) = xf(x)$ and $Q \cdot f(x) = f(qx)$. Then:

$$QX \cdot f(x) = qx f(qx) = qXQ \cdot f(x)$$
Summary: the $q$-binomial coefficient

- The $q$-binomial coefficient:

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

- Via a $q$-version of Pascal’s rule
- **Combinatorially**, as the generating function of the element sums of $k$-subsets of an $n$-set
- **Algebraically**, as the number of $k$-dimensional subspaces of $\mathbb{F}_q^n$
- Via a binomial theorem for noncommuting variables
- Not touched here:
  - **analytical** definition via $q$-integral representations
  - **quantum groups** arising in representation theory and physics
Classical binomial congruences

John Wilson (1773, Lagrange):

\[(p - 1)! \equiv -1 \pmod{p}\]

Charles Babbage (1819):

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

Joseph Wolstenholme (1862):

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

James W.L. Glaisher (1900):

\[\binom{mp - 1}{p - 1} \equiv 1 \pmod{p^3}\]

Wilhelm Ljunggren (1952):

\[\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^3}\]
Wilson’s congruence

\[(p - 1)! \equiv -1 \mod p\]

- known to Ibn al-Haytham, ca. 1000 AD
- congruence holds if and only if \(p\) is a prime
- not great as a practical primality test though...

"The problem of distinguishing prime numbers from composite numbers... is known to be one of the most important and useful in arithmetic. ... The dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated.

C. F. Gauss, *Disquisitiones Arithmeticae*, 1801"
Babbage’s congruence

\[(n - 1)! + 1 \text{ is divisible by } n \text{ if and only if } n \text{ is a prime number}\]

“\n
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 . . . Charles Babbage is led to: \n


Mathematical Note:

For primes \(p \geq 3\):

\[
\frac{(2p - 1)}{p - 1} \equiv 1 \pmod{p^2}
\]

"
Babbage’s congruence

\((n - 1)! + 1\) 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 . . . Charles Babbage is led to:

For primes \(p \geq 3\):

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

\[
\binom{2n - 1}{n - 1} = \frac{(n + 1)(n + 2) \cdots (2n - 1)}{1 \cdot 2 \cdots (n - 1)}
\]
Babbage’s congruence

\[(n - 1)! + 1 \text{ is divisible by } n \text{ if and only if } n \text{ is a prime number}\]

"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 . . . Charles Babbage is led to:

For primes \(p \geq 3\):

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

- \(\binom{2n - 1}{n - 1} = \frac{(n + 1)(n + 2) \cdots (2n - 1)}{1 \cdot 2 \cdots (n - 1)}\)
- Does not quite characterize primes!

\(n = 16843^2\)
A simple combinatorial proof

• We have

\[
\binom{2p}{p} = \sum_k \binom{p}{k} \binom{p}{p-k}
\]

• Note that \(p\) divides \(\binom{p}{k}\) unless \(k = 0\) or \(k = p\).
• We have

\[
\binom{2p}{p} = \sum_k \binom{p}{k} \binom{p}{p-k} \\
\equiv 1 + 1 \pmod{p^2}
\]

• Note that \( p \) divides \( \binom{p}{k} \) unless \( k = 0 \) or \( k = p \).
A simple combinatorial proof

- We have

\[ \binom{2p}{p} = \sum_k \binom{p}{k} \binom{p}{p-k} \equiv 1 + 1 \mod p^2 \]

- Note that \( p \) divides \( \binom{p}{k} \) unless \( k = 0 \) or \( k = p \).

- \( \binom{2p-1}{p-1} = \frac{1}{2} \binom{2p}{p} \) which is only trouble when \( p = 2 \)
A $q$-analog of Babbage’s congruence

- Using $q$-Chu-Vandermonde

\[
\binom{2p}{p}_q = \sum_k \binom{p}{k}_q \binom{p}{p-k}_q q^{(p-k)^2} \\
\equiv q^{p^2} + 1 \quad \mod [p]_q^2
\]

- Again, $[p]_q$ divides $\binom{p}{k}_q$ unless $k = 0$ or $k = p$. 

A $q$-analog of Babbage’s congruence

- Using $q$-Chu-Vandermonde

$$
\binom{2p}{p}_q = \sum_k \binom{p}{k}_q \binom{p}{p-k}_q q^{(p-k)^2} 
\equiv q^{p^2} + 1 \quad \mod [p]^2_q
$$

- Again, $[p]^2_q$ divides $\binom{p}{k}_q$ unless $k = 0$ or $k = p$.

**THM**

$$
\binom{2p}{p}_q \equiv [2] q^{p^2} \quad \mod [p]^2_q
$$
Extending the $q$-analog

- Actually, the same argument shows:

\[
\binom{ap}{bp}_q \equiv \binom{a}{b}_{q^p} \mod [p]^2_q
\]
Extending the $q$-analog

- Actually, the same argument shows:

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

- Sketch of the corresponding classical congruence:

$$\binom{ap}{bp} = \sum_{k_1 + \ldots + k_a = bp} \binom{p}{k_1} \cdots \binom{p}{k_a}$$

$$\equiv \binom{a}{b} \mod p^2$$

- We get a contribution whenever $b$ of the $a$ many $k$'s are $p$. 

[THM Clark 1995]

George Andrews: $q$-analogs of the binomial coefficient congruences of Babbage, Wolstenholme and Glaisher
Discrete Mathematics 204, 1999
Extending the $q$-analog

- Actually, the same argument shows:

$$\binom{ap}{bp}_q \equiv \binom{a}{b}_q \pmod{[p]^2_q}$$

- Sketch of the corresponding classical congruence:

$$\binom{ap}{bp} = \sum_{k_1 + \ldots + k_a = bp} \binom{p}{k_1} \ldots \binom{p}{k_a} \equiv \binom{a}{b}_q \pmod{p^2}$$

- We get a contribution whenever $b$ of the $a$ many $k$'s are $p$.

No restriction on $p$ — the argument is combinatorial.
Extending the $q$-analog

- Actually, the same argument shows:

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

No restriction on $p$ — the argument is combinatorial.

Similar results by Andrews; e.g.:

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

**George Andrews**

$q$-analogs of the binomial coefficient congruences of Babbage, Wolstenholme and Glaisher

*Discrete Mathematics* 204, 1999

- We get a contribution whenever $b$ of the $a$ many $k$'s are $p$. 
• Amazingly, the congruences hold modulo $p^3$!

For primes $p \geq 5$:

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

---


“... for several cases, in testing numerically a result of certain investigations, and after some trouble succeeded in proving it to hold universally ...”
Wolstenholme and Ljunggren

- Amazingly, the congruences hold modulo $p^3$!

**THM** Wolstenholme 1862

For primes $p \geq 5$:

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

"...for several cases, in testing numerically a result of certain investigations, and after some trouble succeeded in proving it to hold universally..."

**THM** Ljunggren 1952

For primes $p \geq 5$:

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

- Note the restriction on $p$ — proofs are **algebraic**.
Proof of Wolstenholme’s congruence

\[
\binom{2p - 1}{p - 1} = \frac{(2p - 1)(2p - 2) \cdots (p + 1)}{1 \cdot 2 \cdots (p - 1)}
\]

\[
= (-1)^{p-1} \prod_{k=1}^{p-1} \left( 1 - \frac{2p}{k} \right)
\]
Proof of Wolstenholme’s congruence

\[
\binom{2p - 1}{p - 1} = \frac{(2p - 1)(2p - 2) \cdots (p + 1)}{1 \cdot 2 \cdots (p - 1)}
\]
\[
= (-1)^{p-1} \prod_{k=1}^{p-1} \left(1 - \frac{2p}{k}\right)
\]
\[
\equiv 1 - 2p \sum_{0<i<p} \frac{1}{i} + 4p^2 \sum_{0<i<j<p} \frac{1}{ij} \mod p^3
\]
Proof of Wolstenholme’s congruence

\[
\binom{2p - 1}{p - 1} = \frac{(2p - 1)(2p - 2) \cdots (p + 1)}{1 \cdot 2 \cdots (p - 1)}
\]

\[
= (-1)^{p-1} \prod_{k=1}^{p-1} \left(1 - \frac{2p}{k}\right)
\]

\[
\equiv 1 - 2p \sum_{0 < i < p} \frac{1}{i} + 4p^2 \sum_{0 < i < j < p} \frac{1}{ij} \mod p^3
\]

\[
= 1 - 2p \sum_{0 < i < p} \frac{1}{i} + 2p^2 \left(\sum_{0 < i < p} \frac{1}{i}\right)^2 - 2p^2 \sum_{0 < i < p} \frac{1}{i^2}
\]
• Wolstenholme’s congruence therefore follows from the fractional congruences

\[
\sum_{i=1}^{p-1} \frac{1}{i} \equiv 0 \mod p^2,
\]

\[
\sum_{i=1}^{p-1} \frac{1}{i^2} \equiv 0 \mod p
\]
Wolstenholme’s congruence therefore follows from the fractional congruences

\[
\sum_{i=1}^{p-1} \frac{1}{i} \equiv 0 \mod p^2,
\]

\[
\sum_{i=1}^{p-1} \frac{1}{i^2} \equiv 0 \mod p
\]

If \( n \) is not a multiple of \( p - 1 \) then, using a primitive root \( g \),

\[
\sum_{0<i<p} i^n \equiv \sum_{0<i<p} (gi)^n \equiv gn \sum_{0<i<p} i^n \equiv 0 \mod p
\]
Congruences for $q$-harmonic numbers

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

\[ \sum_{i=1}^{p-1} \frac{1}{[i]^2_q} \equiv -\frac{(p-1)(p-5)}{12} (q-1)^2 \pmod{[p]_q} \]
Congruences for $q$-harmonic numbers

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

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

\[ \sum_{i=1}^{4} \frac{1}{[i]_q^2} = \frac{(q^4 + q^3 + q^2 + q + 1) \left( q^6 + 3q^5 + 7q^4 + 9q^3 + 11q^2 + 6q + 4 \right)}{(q + 1)^2 (q^2 + 1)^2 (q^2 + q + 1)^2} \]
Congruences for $q$-harmonic numbers

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

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

EG

$\begin{array}{c}
\sum_{i=1}^{4} \frac{1}{[i]^2_q} = \frac{(q^4 + q^3 + q^2 + q + 1) \left(q^6 + 3q^5 + 7q^4 + 9q^3 + 11q^2 + 6q + 4\right)}{(q + 1)^2 (q^2 + 1)^2 (q^2 + q + 1)^2}
\end{array}$

- Equivalent congruences can be given for $\sum_{i=1}^{p-1} \frac{q^i}{[i]^n_q}$
  This choice actually appears a bit more natural.
An exemplary proof

• We wish to prove

\[
\sum_{i=1}^{p-1} \frac{q^i}{[i]^2_q} \equiv -\frac{p^2 - 1}{12} (1 - q)^2 \pmod{[p]_q}
\]
An exemplary proof

- We wish to prove

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

- Write:

\[
\sum_{i=1}^{p-1} \frac{q^i}{[i]^2_q} = (1 - q)^2 \sum_{i=1}^{p-1} \frac{q^i}{(1 - q^i)^2}
\]

\[
=: G(q)
\]
An exemplary proof

• We wish to prove

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

• Write:

\[ \sum_{i=1}^{p-1} \frac{q^i}{\left[ i \right]_q^2} = (1 - q)^2 \left\{ \sum_{i=1}^{p-1} \frac{q^i}{(1 - q^i)^2} \right\} =: G(q) \]

• Hence we need to prove: \( G(\zeta^m) = -\frac{p^2 - 1}{12} \) for \( m = 1, 2, \ldots, p - 1 \)
An exemplary proof

- We wish to prove

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

- Write:

\[
\sum_{i=1}^{p-1} \frac{q^i}{[i]^2_q} = (1 - q)^2 \sum_{i=1}^{p-1} \frac{q^i}{(1 - q^i)^2} =: G(q)
\]

- Hence we need to prove: \( G(\zeta^m) = -\frac{p^2 - 1}{12} \) for \( m = 1, 2, \ldots, p - 1 \)

- \( G(\zeta^m) = \sum_{i=1}^{p-1} \frac{\zeta^m}{(1 - \zeta^m)^2} = \sum_{i=1}^{p-1} \frac{\zeta^i}{(1 - \zeta^i)^2} = G(\zeta) \)

Ling-Ling Shi and Hao Pan
A q-Analogue of Wolstenholme’s Harmonic Series Congruence
The American Mathematical Monthly, 144(6), 2007
Define $G(q, z) = \sum_{i=1}^{p-1} \frac{q^i}{(1 - q^i z)^2}$.

We need $G(\zeta, 1) = -\frac{p^2 - 1}{12}$.
An exemplary proof II

• Define \( G(q, z) = \sum_{i=1}^{p-1} \frac{q^i}{(1 - q^i z)^2} \)

• We need \( G(\zeta, 1) = -\frac{p^2 - 1}{12} \)

\[
G(\zeta, z) = \sum_{i=1}^{p-1} \zeta^i \sum_{k=0}^{\infty} \zeta^{ki} (k + 1) z^k
\]
An exemplatory proof II

- Define $G(q, z) = \sum_{i=1}^{p-1} \frac{q^i}{(1 - q^i z)^2}$

- We need $G(\zeta, 1) = -\frac{p^2 - 1}{12}$

\[
G(\zeta, z) = \sum_{i=1}^{p-1} \zeta^i \sum_{k=0}^{\infty} \zeta^{ki} (k + 1) z^k
\]

\[
= \sum_{k=1}^{\infty} k z^{k-1} \sum_{i=1}^{p-1} \zeta^{ki}
\]
An exemplary proof II

- Define $G(q, z) = \sum_{i=1}^{p-1} \frac{q^i}{(1 - q^i z)^2}$

- We need $G(\zeta, 1) = -\frac{p^2 - 1}{12}$

\[
G(\zeta, z) = \sum_{i=1}^{p-1} \zeta^i \sum_{k=0}^{\infty} \zeta^{ki} (k + 1) z^k
\]

\[
= \sum_{k=1}^{\infty} k z^{k-1} \sum_{i=1}^{p-1} \zeta^{ki}
\]

\[
= p \sum_{k=1}^{\infty} p k z^{k-1} - \sum_{k=1}^{\infty} k z^{k-1}
\]

\[
\sum_{i=1}^{p-1} \zeta^{ki} = \begin{cases} 
  p - 1 & \text{if } p \mid k \\
  -1 & \text{otherwise}
\end{cases}
\]
**An exemplary proof II**

- Define $G(q, z) = \sum_{i=1}^{p-1} \frac{q^i}{(1 - q^i z)^2}$
- We need $G(\zeta, 1) = -\frac{p^2 - 1}{12}$

\[
G(\zeta, z) = \sum_{i=1}^{p-1} \zeta^i \sum_{k=0}^{\infty} \zeta^{ki} (k + 1) z^k
\]

\[
= \sum_{k=1}^{\infty} k z^{k-1} \sum_{i=1}^{p-1} \zeta^{ki}
\]

\[
= p \sum_{k=1}^{\infty} p^k z^{k-1} - \sum_{k=1}^{\infty} k z^{k-1}
\]

\[
= \frac{p^2 z^{p-1}}{(1 - z p)^2} - \frac{1}{(1 - z)^2}
\]
Define $G(q, z) = \sum_{i=1}^{p-1} \frac{q^i}{(1 - q^i z)^2}$

We need $G(\zeta, 1) = -\frac{p^2 - 1}{12}$

$$G(\zeta, z) = \sum_{i=1}^{p-1} \zeta^i \sum_{k=0}^{\infty} \zeta^{ki} (k + 1) z^k$$

$$= \sum_{k=1}^{\infty} k z^{k-1} \sum_{i=1}^{p-1} \zeta^{ki}$$

$$= p \sum_{k=1}^{\infty} p^k z^{k-1} - \sum_{k=1}^{\infty} k z^{k-1}$$

$$= \frac{p^2 z^{p-1}}{(1 - zp)^2} - \frac{1}{(1 - z)^2}$$

as $z \to 1 \quad \Rightarrow \quad -\frac{p^2 - 1}{12}$
An exemplary proof II

- Define $G(q, z) = \sum_{i=1}^{p-1} \frac{q^i}{1 - q^i z^2}$

- We need $G(\zeta, 1) = -\frac{p^2 - 1}{12}$

\[
G(\zeta, z) = \sum_{i=1}^{p-1} \zeta^i \sum_{k=0}^{\infty} \zeta^{ki (1 - \zeta^{-1}) k} \\
= \sum_{k=1}^{\infty} k z^{k-1} \\
= p \sum_{k=1}^{\infty} p k z^{k-1} - \sum_{k=1}^{\infty} k z^{k-1} \\
= \frac{p^2 z^{p-1}}{(1 - z p)^2} - \frac{1}{(1 - z)^2}
\]

\[
\sum_{i=1}^{p-1} \zeta^{ki} = \begin{cases} 
  p - 1 & \text{if } p | k \\
  -1 & \text{otherwise}
\end{cases}
\]

This is beautifully generalized in:

**Karl Dilcher**

*Determinant expressions for q-harmonic congruences and degenerate Bernoulli numbers*

For primes $p \geq 5$:

$$\left(\begin{array}{c} ap \\ bp \end{array}\right)_q \equiv \left(\begin{array}{c} a \\ b \end{array}\right)_{q^p^2} - \left(\begin{array}{c} a \\ b + 1 \end{array}\right) \left(\begin{array}{c} b + 1 \\ 2 \end{array}\right) \frac{p^2 - 1}{12} (q^p - 1)^2 \mod [p]^3_q$$
For primes $p \geq 5$:

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

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.
A \(q\)-analog of Ljunggren’s congruence

**THM S 2011**

For primes \(p \geq 5\):

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

**EG**

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 \(f(q) = 14 - 41a + 41a^2 - \ldots + q^{132}\) is an irreducible polynomial with integer coefficients.
\[
\binom{ap}{bp}_q \equiv \binom{a}{b}_{q^{p^2}} - \binom{a}{b+1} \binom{b+1}{2} \frac{p^2 - 1}{12} (q^p - 1)^2 \mod [p]_q^3
\]

- Ernst Jacobsthal (1952) proved that Ljunggren’s classical congruence holds modulo \( p^{3+r} \) where \( r \) is the \( p \)-adic valuation of

\[
a b (a - b) \binom{a}{b} = 2a \binom{a}{b+1} \binom{b+1}{2}.
\]

- It would be interesting to see if this generalization has a nice analog in the \( q \)-world.
The case of composite numbers

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

- Note that \( \frac{n^2 - 1}{12} \) is an integer if \((n, 6) = 1\).
The case of composite numbers

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

- Note that \(\frac{n^2 - 1}{12}\) is an integer if \((n, 6) = 1\).
- Ljunggren’s \(q\)-congruence holds modulo \(\Phi_n(q)^3\) over integer coefficient polynomials if \((n, 6) = 1\) — otherwise we get rational coefficients.

\[
\binom{70}{35}_q = 1 + q^{1225} - 102(q^{35} - 1)^2 + \Phi_{35}(q)^3 f(q)
\]

where \(f(q) = 102 + 307q + 617q^2 + \ldots + q^{1152}\)
The case of composite numbers

\[
\begin{align*}
\left( \begin{array}{c} a p \\ b p \end{array} \right)_q & \equiv \left( \begin{array}{c} a \\ b \end{array} \right)_{qp^2} - \left( \begin{array}{c} a \\ b + 1 \end{array} \right)_{2} \frac{p^2 - 1}{12} (q^p - 1)^2 \quad \text{mod } [p]^3_q
\end{align*}
\]

- Note that \( \frac{n^2 - 1}{12} \) is an integer if \((n, 6) = 1\).

- Ljunggren’s \( q \)-congruence holds modulo \( \Phi_n(q)^3 \) over integer coefficient polynomials if \((n, 6) = 1\) — otherwise we get rational coefficients.

\[
\left( \begin{array}{c} 24 \\ 12 \end{array} \right)_q = 1 + q^{144} - \frac{143}{12} (q^{12} - 1)^2 + \frac{1}{12} \left( 1 - q^2 + q^4 \right)^3 \Phi_{12}(q) f(q)
\]

where \( f(q) = 143 + 12q + 453q^2 + \ldots + 12q^{131} \)
Can we do better than modulo $p^3$?

- Are there primes $p$ such that

$$\binom{2p-1}{p-1} \equiv 1 \mod p^4?$$

- Such primes are called **Wolstenholme primes**.
- The only two known are 16843 and 2124679.

McIntosh, 1995: up to $10^9$

---

**C. Helou and G. Terjanian**

*On Wolstenholme’s theorem and its converse*

Journal of Number Theory 128, 2008
Can we do better than modulo $p^3$?

- Are there primes $p$ such that
  \[
  \binom{2p - 1}{p - 1} \equiv 1 \mod p^4?
  \]

- Such primes are called **Wolstenholme primes**.
- The only two known are 16843 and 2124679. \textit{McIntosh, 1995: up to $10^9$}
- Infinitely many Wolstenholme primes are conjectured to exist. However, no primes are conjectured to exist for modulo $p^5$.

\[ \]

C. Helou and G. Terjanian

\textit{On Wolstenholme’s theorem and its converse}

\textit{Journal of Number Theory} 128, 2008
Can we do better than modulo $p^3$?

- Are there primes $p$ such that
  \[
  \binom{2p-1}{p-1} \equiv 1 \pmod{p^4}?
  \]

- Such primes are called \textbf{Wolstenholme primes}.

- The only two known are 16843 and 2124679. \cite{McIntosh1995}

- Infinitely many Wolstenholme primes are conjectured to exist. However, no primes are conjectured to exist for modulo $p^5$.

- Conjecturally, Wolstenholme’s congruence characterizes primes:
  \[
  \binom{2n-1}{n-1} \equiv 1 \pmod{n^3} \iff n \text{ is prime}
  \]

\textbf{C. Helou and G. Terjanian}

\textit{On Wolstenholme’s theorem and its converse}

Journal of Number Theory 128, 2008
Can we do better than modulo $p^3$?

- Are there primes $p$ such that
  \[
  \binom{2p - 1}{p - 1} \equiv 1 \mod p^4?
  \]

- Such primes are called **Wolstenholme primes**.
- The only two known are 16843 and 2124679. McIntosh, 1995: up to $10^9$
- Infinitely many Wolstenholme primes are conjectured to exist. However, no primes are conjectured to exist for modulo $p^5$.
- Conjecturally, Wolstenholme’s congruence characterizes primes:
  \[
  \binom{2n - 1}{n - 1} \equiv 1 \mod n^3 \iff n \text{ is prime}
  \]

- Any insight into these from the $q$-perspective??

_C. Helou and G. Terjanian_  
*On Wolstenholme’s theorem and its converse*  
_Journal of Number Theory 128, 2008_
THANK YOU!

- Slides for this talk will be available from my website: http://arminstraub.com/talks

**Victor Kac and Pokman Cheung**
*Quantum Calculus*
Springer, 2002

**Armin Straub**
*A q-analog of Ljunggren's binomial congruence*
Proceedings of FPSAC, 2011
Some open problems

- Extension to Jacobsthal’s result?
- Extension to
  \[
  \binom{ap}{bp} \equiv \binom{a}{b} \cdot \left[1 - ab(a - b)\frac{p^3}{3}B_{p-3}\right] \mod p^4,
  \]
  and insight into Wolstenholme primes?
- Is there a nice $q$-analog for Gauss’ congruence?
  \[
  \binom{(p - 1)/2}{(p - 1)/4} \equiv 2a \mod p
  \]
  where $p = a^2 + b^2$ and $a \equiv 1 \mod 4$.

Generalized to $p^2$ and $p^3$ by Chowla-Dwork-Evans (1986) and by Cosgrave-Dilcher (2010)
It all starts with the $q$-derivative:

$$D_q f(x) = \frac{f(qx) - f(x)}{qx - x}$$
It all starts with the \textit{q-derivative}:

\[
D_q f(x) = \frac{f(qx) - f(x)}{qx - x}
\]

\[
D_q x^s = \frac{(qx)^s - x^s}{qx - x} = \frac{q^s - 1}{q - 1} x^{s-1} = [s]_q x^{s-1}
\]
It all starts with the $q$-derivative:

$$D_q f(x) = \frac{f(qx) - f(x)}{qx - x}$$

$D_q x^s = \frac{(qx)^s - x^s}{qx - x} = \frac{q^s - 1}{q - 1} x^{s-1} = [s]_q x^{s-1}$

- Define $e^x_q = \sum_{n=0}^{\infty} \frac{x^n}{[n]_q!}$

$D_q e^x_q = e^x_q$

$e^x_q \cdot e^y_q \neq e^{x+y}_q$

unless $yx = qxy$

$e^x_q \cdot e^{-x}_{1/q} = 1$
It all starts with the \textit{q-derivative}:

\[ D_q f(x) = \frac{f(qx) - f(x)}{qx - x} \]

\[ D_q x^s = \frac{(qx)^s - x^s}{qx - x} = \frac{q^s - 1}{q - 1} x^{s-1} = [s]_q x^{s-1} \]

- Define \( e^x_q = \sum_{n=0}^{\infty} \frac{x^n}{[n]_q!} \)

- \textbf{Homework:} Define \( \cos_q(x) \), \( \sin_q(x) \), \ldots and develop some \( q \)-trigonometry.

- \( D_q e^x = e^x_q \)
- \( e^x_q \cdot e^y_q \neq e^{x+y}_q \) unless \( yx = qxy \)
- \( e^x_q \cdot e^{-x}_{1/q} = 1 \)
• Formally inverting $D_q F(x) = f(x)$ gives:

$$F(x) = \int_0^x f(x) d_q x := (1 - q) \sum_{n=0}^{\infty} q^n x f(q^n x)$$
Formally inverting $D_q F(x) = f(x)$ gives:

$$F(x) = \int_0^x f(x) d_q x := (1 - q) \sum_{n=0}^{\infty} q^n x f(q^n x)$$

**Fundamental theorem of $q$-calculus:**

Let $0 < q < 1$. Then

$$D_q F(x) = f(x).$$

$F(x)$ is the unique such function continuous at 0 with $F(0) = 0$.

*Fineprint:* one needs for instance that $|f(x)x^\alpha|$ is bounded on some $(0, a]$. 
• Define the $q$-gamma function as

\[ \Gamma_q(s) = \int_0^\infty x^{s-1} e^{-q x} \, dq x \]

\[ \Gamma_q(s + 1) = [s]_q \Gamma_q(s) \]

\[ \Gamma_q(n + 1) = [n]_q ! \]
- Define the $q$-gamma function as

$$
\Gamma_q(s) = \int_0^{\infty} x^{s-1} e^{-qx} \frac{dx}{q}
$$

- $\Gamma_q(s + 1) = [s]_q \Gamma_q(s)$
- $\Gamma_q(n + 1) = [n]_q!$

- $q$-beta function:

$$
B_q(t, s) = \int_0^1 x^{t-1} (1 - qx)_q^{s-1} dx
$$

- $B_q(t, s) = \frac{\Gamma_q(t)\Gamma_q(s)}{\Gamma_q(t + s)}$
- $B_q(t, s) = B_q(s, t)$

- Here, $(x - a)_q^n$ is defined by:

$$
f(x) = \sum_{n \geq 0} (D_q^n f)(a) \frac{(x - a)_q^n}{[n]_q!}
$$

Explicitly: $(x - a)_q^n = (x - a)(x - qa) \cdots (x - q^{n-1} a)$
Automatic proving of \( q \)-identities

\[ \text{In[1]} := \text{\texttt{\textasciitilde docs/math/mathematica/packages/qZeil.m}}; \]

\textbf{q-Zeilberger Package by Axel Riese — © RISC Linz — V 2.42 (02/18/05)}

\[ \text{In[2]} := \text{qZeil[qBinomial[m, j, q] qBinomial[n, k-j, q] q^((m-j)(k-j)), \{j, 0, m+n\}, k, 1]} \]

\[ \text{Out[2]} = \text{SUM[k} = \frac{(1 - q^{1-k+m+n}) \text{SUM[-1 + k]}}{1 - q^k} \text{SUM[-1 + k]} \]

\[ \text{P. Paule and A. Riese} \]

\textit{A Mathematica q-Analogue of Zeilberger’s Algorithm Based on an Algebraically Motivated Approach to q-Hypergeometric Telescoping}

Automatic proving of $q$-identities

In[1]:= << "~/docs/math/mathematica/packages/qZeil.m";

q-Zeilberger Package by Axel Riese — © RISC Linz — V 2.42 (02/18/05)

In[2]:= qZeil[qBinomial[m, j, q] qBinomial[n, k - j, q] q^((m - j) (k - j)), {j, 0, m + n}, k, 1]

Out[2]= SUM[k] = \frac{(1 - q^{1-k+m+n}) \text{SUM}[-1+k]}{1 - q^k}

- **Encoded** implementation in Mathematica at risk of **bit rot**?
  last version of qZeil by Alex Riese from 2005 — many examples don’t work in MMA7 anymore...

- Sage as a solution?

---

**P. Paule and A. Riese**

A Mathematica $q$-Analogue of Zeilberger’s Algorithm Based on an Algebraically Motivated Approach to $q$-Hypergeometric Telescoping