# $q$-binomial coefficient congruences

**CARMA Analysis and Number Theory Seminar**

**University of Newcastle**

**Armin Straub**

August 23, 2011

Tulane University, New Orleans

# Our first $q$-analogs

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

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

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

# Our first $q$-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:

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

D1

# A $q$-binomial coefficient

**Example**

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

- Let us understand the first term a bit better!

# Cyclotomic polynomials

The $n$th cyclotomic polynomial:

$$\Phi_n(q) = \prod_{\substack{1 \leqslant k < n \\ (k,n)=1}} (q - \zeta^k) \qquad \text{where } \zeta = e^{2\pi i/n}$$

- This is an **irreducible** polynomial with **integer** coefficients.

  irreducibility due to Gauss — nontrivial

# Cyclotomic polynomials

The $n$th cyclotomic polynomial:

$$\Phi_n(q) = \prod_{\substack{1 \leqslant k < n \\ (k,n)=1}} (q - \zeta^k) \qquad \text{where } \zeta = e^{2\pi i/n}$$

- This is an **irreducible** polynomial with **integer** coefficients.
  irreducibility due to Gauss — nontrivial
- $[n]_q = \dfrac{q^n - 1}{q - 1} = \prod_{\substack{1 < d \leqslant n \\ d|n}} \Phi_d(q)$ For primes: $[p]_q = \Phi_p(q)$

# Cyclotomic polynomials

The $n$th cyclotomic polynomial:

$$\Phi_n(q) = \prod_{\substack{1 \leqslant k < n \\ (k,n)=1}} (q - \zeta^k) \qquad \text{where } \zeta = e^{2\pi i/n}$$

- This is an **irreducible** polynomial with **integer** coefficients.
  irreducibility due to Gauss — nontrivial
- $[n]_q = \dfrac{q^n - 1}{q - 1} = \prod_{\substack{1 < d \leqslant n \\ d \mid n}} \Phi_d(q)$ For primes: $[p]_q = \Phi_p(q)$
- An irreducible monic integral polynomial is cyclotomic if and only if its Mahler measure $\prod \max(|\alpha|, 1)$ is $1$.

# Some cyclotomic polynomials exhibited

- $\Phi_{mn}(q) = \Phi_n(q^m)$ if $m|n$
- $\Phi_{2n}(q) = \Phi_n(-q)$ for odd $n > 1$
- $\Phi_n(q)$ is palindromic

**Example**

$$\Phi_2(q) = q + 1$$

$$\Phi_3(q) = q^2 + q + 1$$

$$\Phi_6(q) = q^2 - q + 1$$

$$\Phi_9(q) = q^6 + q^3 + 1$$

$$\Phi_{21}(q) = q^{12} - q^{11} + q^9 - q^8 + q^6 - q^4 + q^3 - q + 1$$

$$\vdots$$

$$\Phi_{102}(q) = q^{32} + q^{31} - q^{29} - q^{28} + q^{26} + q^{25} - q^{23} - q^{22} + q^{20} + q^{19} - q^{17} - q^{16} - q^{15} + q^{13} + q^{12} - q^{10} - q^9 + q^7 + q^6 - q^4 - q^3 + q + 1$$

# Some cyclotomic polynomials exhibited

**Example**

- $\Phi_{mn}(q) = \Phi_n(q^m)$ if $m|n$
- $\Phi_{2n}(q) = \Phi_n(-q)$ for odd $n > 1$
- $\Phi_n(q)$ is palindromic

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

# Back to $q$-binomials

- $[n]_q = \dfrac{q^n - 1}{q - 1} = \prod_{\substack{1 < d \leqslant n \\ d | n}} \Phi_d(q)$
- $\binom{n}{k}_q = \dfrac{[n]_q [n-1]_q \cdots [n-k+1]_q}{[k]_q [k-1]_q \cdots [1]_q}$
- 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

- $[n]_q = \dfrac{q^n - 1}{q - 1} = \prod_{\substack{1<d\leqslant n \\ d|n}} \Phi_d(q)$
- $\dbinom{n}{k}_q = \dfrac{[n]_q [n-1]_q \cdots [n-k+1]_q}{[k]_q [k-1]_q \cdots [1]_q}$
- 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**
  - $\dbinom{n}{k}_q$ 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:

**Example**

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

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

**What is the degree of the $q$-binomial?**

- All coefficients are positive!

# The coefficients of $q$-binomial coefficients

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

**Example**

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

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

**What is the degree of the $q$-binomial?** It is $(n-k)k$.

- All coefficients are positive!

# The coefficients of $q$-binomial coefficients

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

**Example**

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

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

**What is the degree of the $q$-binomial?** It is $(n-k)k$.

- All coefficients are positive!
- In fact, the coefficients are **unimodal**.

Sylvester, 1878

# $q$-binomials: Pascal's triangle

Define the $q$-binomials via the $q$-Pascal rule:

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

D2

# $q$-binomials: Pascal's triangle

Define the $q$-binomials via the $q$-Pascal rule:

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

D2

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

# $q$-binomials: Pascal's triangle

Define the $q$-binomials via the $q$-Pascal rule:

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

D2

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

**Example**

$$\binom{4}{2}_q = 1+q+q^2+q^2(1+q+q^2) = 1+q+2q^2+q^3+q^4$$

$$\binom{n}{k}_q = \sum_{S \in \binom{n}{k}} q^{w(S)} \quad \text{where } w(S) = \sum_j s_j - j$$

D3

$w(S) =$ "normalized sum of $S$"

**Example**

$$\underbrace{\{1,2\}}_{\to 0}, \underbrace{\{1,3\}}_{\to 1}, \underbrace{\{1,4\}}_{\to 2}, \underbrace{\{2,3\}}_{\to 2}, \underbrace{\{2,4\}}_{\to 3}, \underbrace{\{3,4\}}_{\to 4}$$

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

$$\binom{n}{k}_q = \sum_{S \in \binom{n}{k}} q^{w(S)} \qquad \text{where } w(S) = \sum_j s_j - j$$

D3

$w(S) =$ "normalized sum of $S$"

**Example**

$$\underbrace{\{1,2\}}_{\to 0}, \underbrace{\{1,3\}}_{\to 1}, \underbrace{\{1,4\}}_{\to 2}, \underbrace{\{2,3\}}_{\to 2}, \underbrace{\{2,4\}}_{\to 3}, \underbrace{\{3,4\}}_{\to 4}$$

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

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

- $k$-element subsets of $n$ whose normalized sum is $m$

$$\binom{n}{k}_q = \sum_{S \in \binom{n}{k}} q^{w(S)} \quad \text{where } w(S) = \sum_j s_j - j$$

D3

$w(S) =$ "normalized sum of $S$"

**Example**

$$\underbrace{\{1,2\}}_{\to 0}, \underbrace{\{1,3\}}_{\to 1}, \underbrace{\{1,4\}}_{\to 2}, \underbrace{\{2,3\}}_{\to 2}, \underbrace{\{2,4\}}_{\to 3}, \underbrace{\{3,4\}}_{\to 4}$$

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

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

- $k$-element subsets of $n$ whose normalized sum is $m$
- words made from $k$ ones and $n-k$ twos which have $m$ inversions

$$\binom{n}{k}_q = \sum_{S \in \binom{n}{k}} q^{w(S)} \quad \text{where } w(S) = \sum_j s_j - j$$

D3

$w(S) =$ "normalized sum of $S$"

**Example**

$$\underbrace{\{1,2\}}_{\to 0}, \underbrace{\{1,3\}}_{\to 1}, \underbrace{\{1,4\}}_{\to 2}, \underbrace{\{2,3\}}_{\to 2}, \underbrace{\{2,4\}}_{\to 3}, \underbrace{\{3,4\}}_{\to 4} \qquad \binom{4}{2}_q = 1 + q + 2q^2 + q^3 + q^4$$

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

- $k$-element subsets of $n$ whose normalized sum is $m$
- words made from $k$ ones and $n-k$ twos which have $m$ inversions
- partitions $\lambda$ of $m$ whose Ferrer's diagram fits in a $k \times (n-k)$ box

# $q$-Chu-Vandermonde

Different representations make different properties apparent!

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

# $q$-Chu-Vandermonde

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:

$$\binom{m+n}{k}_q = \sum_{S\in\binom{m+n}{k}} q^{\sum S - k(k+1)/2}$$

# $q$-Chu-Vandermonde

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:

$$\begin{aligned}\binom{m+n}{k}_q &= \sum_{S\in\binom{m+n}{k}} q^{\sum S - k(k+1)/2} \\ &= \sum_j \sum_{S_1\in\binom{m}{j}} \sum_{S_2\in\binom{n}{k-j}} q^{\sum S_1 + \sum S_2 + (k-j)m - k(k+1)/2}\end{aligned}$$

# $q$-Chu-Vandermonde

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:

$$\begin{aligned}\binom{m+n}{k}_q &= \sum_{S \in \binom{m+n}{k}} q^{\sum S - k(k+1)/2} \\ &= \sum_j \sum_{S_1 \in \binom{m}{j}} \sum_{S_2 \in \binom{n}{k-j}} q^{\sum S_1 + \sum S_2 + (k-j)m - k(k+1)/2} \\ &= \sum_j \binom{m}{j}_q \binom{n}{k-j}_q q^{(m-j)(k-j)}\end{aligned}$$

# 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]=
$$\mathrm{SUM}[k] == \frac{\left(1 - q^{1-k+m+n}\right)\,\mathrm{SUM}[-1+k]}{1 - q^k}$$


**P. Paule and A. Riese**
*A Mathematica q-Analogue of Zeilberger's Algorithm Based on an Algebraically Motivated Approach to q-Hypergeometric Telescoping*
Fields Inst. Commun., Vol. 14, 1997

# 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]= $\mathrm{SUM}[k] == \dfrac{\left(1 - q^{1-k+m+n}\right)\,\mathrm{SUM}[-1+k]}{1 - q^{k}}$

- **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*

Fields Inst. Commun., Vol. 14, 1997

Let $q$ be a prime power.

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

D4

# $q$-binomials: algebraic

Let $q$ be a prime power.

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

D4

- 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.

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

D4

- 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:

$$\frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})} = \binom{n}{k}_q$$

# $q$-binomials: noncommuting variables

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:

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

D5

**Example**

$$\binom{4}{2}_q x^2 y^2 = xxyy + xyxy + xyyx + yxxy + yxyx + yyxx$$
$$= (1 + q + q^2 + q^2 + q^3 + q^4)x^2 y^2$$

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

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

D5

**Example**

$$\binom{4}{2}_q x^2y^2 = xxyy + xyxy + xyyx + yxxy + yxyx + yyxx$$
$$= (1 + q + q^2 + q^2 + q^3 + q^4)x^2y^2$$

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

$$QX \cdot f(x) = qxf(qx) = qXQ \cdot f(x)$$

# $q$-calculus

It all starts with the $q$-**derivative**:

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

It all starts with the $q$-**derivative**:

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

**Example**

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

It all starts with the $q$-**derivative**:

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

**Example**

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

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

- $D_q e_q^x = e_q^x$
- $e_q^x \cdot e_q^y \neq e_q^{x+y}$
  unless $yx = qxy$
- $e_q^x \cdot e_{1/q}^{-x} = 1$

It all starts with the $q$-**derivative**:

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

**Example**

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

- Define $e_q^x = \sum_{n=0}^{\infty} \frac{x^n}{[n]_q!}$
- **Homework:** Define $\cos_q(x)$, $\sin_q(x)$, ... and develop some $q$-trigonometry.

- $D_q e_q^x = e_q^x$
- $e_q^x \cdot e_q^y \neq e_q^{x+y}$ unless $yx = qxy$
- $e_q^x \cdot e_{1/q}^{-x} = 1$

# $q$-calculus: the $q$-integral

- Formally inverting $D_q F(x) = f(x)$ gives:

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

## $q$-calculus: the $q$-integral

- Formally inverting $D_q F(x) = f(x)$ gives:

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

**Theorem (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 $(0, a]$.*

# $q$-calculus: special functions

- Define the $q$-gamma function as

$$\Gamma_q(s) = \int_0^\infty x^{s-1} e_{1/q}^{-qx} d_q x$$

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

# $q$-calculus: special functions

- Define the $q$-gamma function as

$$\Gamma_q(s) = \int_0^\infty x^{s-1} e_{1/q}^{-qx} d_q x$$

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

D6

$q$-beta function:

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

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

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

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

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

# 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
- Analytically, via $q$-integral representations
- We have not touched: quantum groups arising in representation theory and physics

# Classical binomial congruences

John Wilson (1773, Lagrange): $(p-1)! \equiv -1 \mod p$

Charles Babbage (1819): $\binom{2p-1}{p-1} \equiv 1 \mod p^2$

Joseph Wolstenholme (1862): $\binom{2p-1}{p-1} \equiv 1 \mod p^3$

James W.L. Glaisher (1900): $\binom{mp-1}{p-1} \equiv 1 \mod p^3$

Wilhelm Ljunggren (1952): $\binom{ap}{bp} \equiv \binom{a}{b} \mod p^3$

# Wilson's congruence

**Wilson's congruence (Lagrange, 1773)**

$$(p-1)! \equiv -1 \mod p$$

- known to Ibn al-Haytham, ca. 1000 AD
- This 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

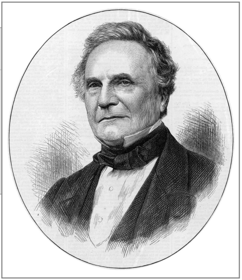
$(n-1)!+1$ is divisible by $n$ if and only if $n$ is a prime number

> *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:

**Theorem (Babbage, 1819)**

*For primes $p \geqslant 3$:*

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



# Babbage's congruence

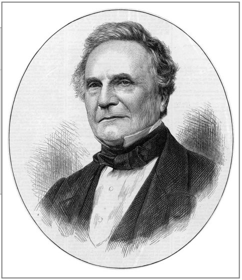
$(n-1)! + 1$ is divisible by $n$ if and only if $n$ is a prime number

> *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:

**Theorem (Babbage, 1819)**

*For primes $p \geqslant 3$:*

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



- $$\binom{2n-1}{n-1} = \frac{(n+1)(n+2)\cdots(2n-1)}{1 \cdot 2 \cdots (n-1)}$$

# Babbage's congruence

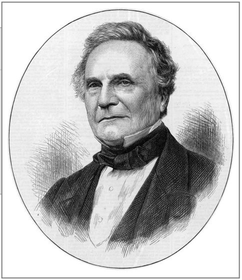
$(n-1)! + 1$ is divisible by $n$ if and only if $n$ is a prime number

> *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:

**Theorem (Babbage, 1819)**

*For primes $p \geqslant 3$:*

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



- $\binom{2n-1}{n-1} = \frac{(n+1)(n+2)\cdots(2n-1)}{1 \cdot 2 \cdots (n-1)}$
- 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 $k = p$.

# 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 $k = p$.

# 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

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

- 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

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

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

**Theorem**

$$\binom{2p}{p}_q \equiv [2]_{q^{p^2}} \mod [p]_q^2$$

# Extending the $q$-analog

- Actually, the same argument shows:

**Theorem (W. Edwin Clark, 1995)**

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

# Extending the $q$-analog

- Actually, the same argument shows:

**Theorem (W. Edwin Clark, 1995)**

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

- 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 $p$.

# Extending the $q$-analog

- Actually, the same argument shows:

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

**Theorem (W. Edwin Clark, 1995)**

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

- Sketch of the corresponding classical congruence:

$$\begin{aligned}\binom{ap}{bp} &= \sum_{k_1+\ldots+k_a=bp} \binom{p}{k_1} \cdots \binom{p}{k_a} \\ &\equiv \binom{a}{b} && \mod p^2\end{aligned}$$

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

# Extending the $q$-analog

- Actually, the same argument shows:

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

**Theorem (W. Edwin Clark, 1995)**

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

Similar results by Andrews; e.g.:

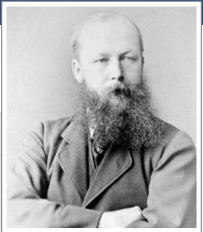
$$\binom{ap}{bp}_q \equiv q^{(a-b)b\binom{p}{2}} \binom{a}{b}_{q^p} \mod [p]_q^2$$

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

$p^2$

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

# Wolstenholme and Ljunggren



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

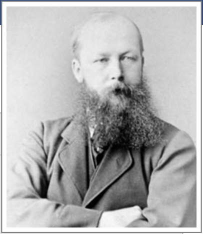
**Theorem (Wolstenholme, 1862)**

*For primes $p \geqslant 5$:* $$\binom{2p-1}{p-1} \equiv 1 \mod p^3$$

“ *. . . 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 $p^3$!



**Theorem (Wolstenholme, 1862)**

*For primes* $p \geqslant 5$*:*
$$\binom{2p-1}{p-1} \equiv 1 \mod p^3$$

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

**Theorem (Ljunggren, 1952)**

*For primes* $p \geqslant 5$*:*
$$\binom{ap}{bp} \equiv \binom{a}{b} \mod p^3$$

- 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

$$\begin{aligned} \binom{2p-1}{p-1} &= \frac{(2p-1)(2p-2)\cdots(p+1)}{1\cdot 2\cdots(p-1)} \\ &= (-1)^{p-1}\prod_{k=1}^{p-1}\left(1-\frac{2p}{k}\right) \\ &\equiv 1-2p\sum_{0<i<p}\frac{1}{i}+4p^2\sum_{0<i<j<p}\frac{1}{ij} \mod p^3 \end{aligned}$$

# Proof of Wolstenholme's congruence

$$\binom{2p-1}{p-1} = \frac{(2p-1)(2p-2)\cdots(p+1)}{1\cdot 2\cdots(p-1)}$$
$$= (-1)^{p-1}\prod_{k=1}^{p-1}\left(1-\frac{2p}{k}\right)$$
$$\equiv 1 - 2p\sum_{0<i<p}\frac{1}{i} + 4p^2\sum_{0<i<j<p}\frac{1}{ij} \mod p^3$$
$$= 1 - 2p\sum_{0<i<p}\frac{1}{i} + 2p^2\left(\sum_{0<i<p}\frac{1}{i}\right)^2 - 2p^2\sum_{0<i<p}\frac{1}{i^2}$$

# Proof of Wolstenholme's congruence

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

$$= \prod_{k=1}^{p-1} \frac{p+(p-k)}{p-k}$$

$$= \prod_{k=1}^{p-1}\left(1+\frac{p}{k}\right)$$

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

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

$$= 1 - 2p\sum_{0<i<p}\frac{1}{i} + 2p^2\left(\sum_{0<i<p}\frac{1}{i}\right)^2 - 2p^2\sum_{0<i<p}\frac{1}{i^2}$$

# Proof of Wolstenholme's congruence II

- Wolstenholme's congruence therefore follows from the fractional congruences

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

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

# Proof of Wolstenholme's congruence II

- Wolstenholme's congruence therefore follows from the fractional congruences

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

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

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

$$\sum_{0<i<p} i^n \equiv \sum_{0<i<p} (gi)^n \equiv g^n \sum_{0<i<p} i^n \equiv 0 \mod p$$

# Proof of Wolstenholme's congruence II

- Wolstenholme's congruence therefore follows from the fractional congruences

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

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

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

$$\sum_{0<i<p} i^n \equiv \sum_{0<i<p} (gi)^n \equiv g^n \sum_{0<i<p} i^n \equiv 0 \mod p$$

- Comparing the $p^3$ residues on the previous slide now shows (1).

# Congruences for $q$-harmonic numbers

**Theorem (Shi-Pan, 2007)**

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

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

# Congruences for $q$-harmonic numbers

**Theorem (Shi-Pan, 2007)**

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

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

**Example ($p = 5$)**

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

# Congruences for $q$-harmonic numbers

**Theorem (Shi-Pan, 2007)**

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

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

**Example ($p=5$)**

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

- Equivalent congruences can be given for $\displaystyle\sum_{i=1}^{p-1} \frac{q^i}{[i]_q^n}$

  This choice actually appears a bit more natural

# An exemplatory proof

- We wish to prove

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

**Ling-Ling Shi and Hao Pan**
*A q-Analogue of Wolstenholme's Harmonic Series Congruence*
The American Mathematical Monthly, 144(6), 2007

# An exemplatory proof

- We wish to prove

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

- Write:

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

**Ling-Ling Shi and Hao Pan**
*A q-Analogue of Wolstenholme's Harmonic Series Congruence*
The American Mathematical Monthly, 144(6), 2007

# An exemplatory proof

- We wish to prove

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

- Write:

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

$$[p]_q = \prod_{m=1}^{p-1} (q - \zeta^m)$$

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

**Ling-Ling Shi and Hao Pan**
*A q-Analogue of Wolstenholme's Harmonic Series Congruence*
The American Mathematical Monthly, 144(6), 2007

# An exemplatory proof

- We wish to prove

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

- Write:

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

$$[p]_q = \prod_{m=1}^{p-1} (q-\zeta^m)$$

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

**Ling-Ling Shi and Hao Pan**
*A q-Analogue of Wolstenholme's Harmonic Series Congruence*
The American Mathematical Monthly, 144(6), 2007

# An exemplatory proof II

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

# An exemplatory proof II

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

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

# An exemplatory proof II

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

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

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

# An exemplatory proof II

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

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

$$\begin{aligned} G(\zeta,z) &= \sum_{i=1}^{p-1} \zeta^i \sum_{k=0}^{\infty} \zeta^{ki}(k+1)z^k \\ &= \sum_{k=1}^{\infty} k z^{k-1} \sum_{i=1}^{p-1} \zeta^{ki} \\ &= p \sum_{k=1}^{\infty} pk z^{k-1} - \sum_{k=1}^{\infty} k z^{k-1} \\ &= \frac{p^2 z^{p-1}}{(1-z^p)^2} - \frac{1}{(1-z)^2} \end{aligned}$$

# An exemplatory proof II

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

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

$$\begin{aligned} G(\zeta,z) &= \sum_{i=1}^{p-1} \zeta^i \sum_{k=0}^{\infty} \zeta^{ki}(k+1) z^k \\ &= \sum_{k=1}^{\infty} k z^{k-1} \sum_{i=1}^{p-1} \zeta^{ki} \\ &= p \sum_{k=1}^{\infty} pk z^{k-1} - \sum_{k=1}^{\infty} k z^{k-1} \\ &= \frac{p^2 z^{p-1}}{(1-z^p)^2} - \frac{1}{(1-z)^2} \quad \xrightarrow{\text{as } z \to 1} \quad -\frac{p^2-1}{12} \end{aligned}$$

# An exemplatory proof II

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

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

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

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

This is beautifully generalized in:

**Karl Dilcher**
*Determinant expressions for q-harmonic congruences and degenerate Bernoulli numbers*
Electronic Journal of Combinatorics 15, 2008

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

$$= \frac{p^2 z^{p-1}}{(1-z^p)^2} - \frac{1}{(1-z)^2} \xrightarrow{\text{as } z\to 1} -\frac{p^2-1}{12}$$

# A $q$-analog of Ljunggren's congruence

**Theorem (S, 2010)**

*For primes $p \geqslant 5$:*

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

# A $q$-analog of Ljunggren's congruence

**Theorem (S, 2010)**

*For primes $p \geqslant 5$:*

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

**Example**

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.

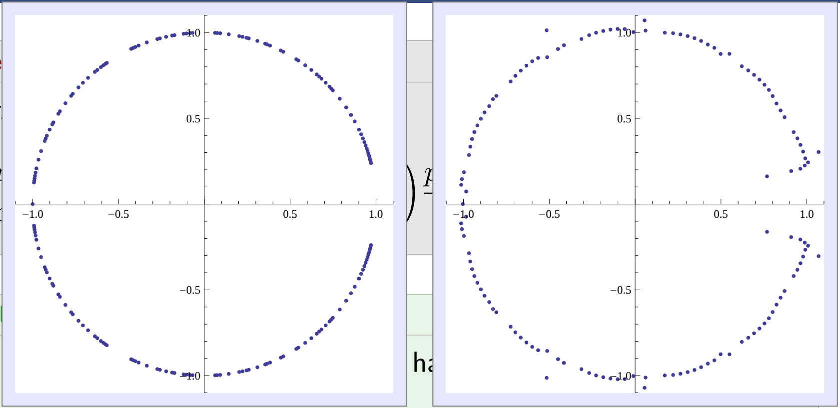
**Theore**

*For pr*

$\binom{a}{b}$ ... $p$

**Exampl**

Choos ... ha




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

where $f(q) = 14 - 41q + 41q^2 - \ldots + q^{132}$ is an irreducible polynomial with integer coefficients.

# Just coincidence?

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

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

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

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

# What happens for composite numbers?

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

**Example ($n = 12$, $a = 2$, $b = 1$)**

$$\binom{24}{12}_q = 1 + q^{144} - \frac{143}{12}(q^{12}-1)^2 + \frac{1}{12}(\underbrace{1 - q^2 + q^4}_{\Phi_{12}(q)})^3 f(q)$$

where $f(q) = 143 + 12q + 453q^2 + \ldots + 12q^{131}$ is an irreducible polynomial with integer coefficients.

# What happens for composite numbers?

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

**Example ($n = 12$, $a = 2$, $b = 1$)**

$$\binom{24}{12}_q = 1 + q^{144} - \frac{143}{12}(q^{12}-1)^2 + \frac{1}{12}(\underbrace{1-q^2+q^4}_{\Phi_{12}(q)})^3 f(q)$$

where $f(q) = 143 + 12q + 453q^2 + \ldots + 12q^{131}$ is an irreducible polynomial with integer coefficients.

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

# 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 $2124679$. 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**
*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:

$$\binom{2n-1}{n-1} \equiv 1 \mod n^3 \quad \iff \quad n \text{ is prime}$$

**C. Helou and G. Terjanian**
*On Wolstenholme's theorem and its converse*
Journal of Number Theory 128, 2008

# 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)

# 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