Congruences modulo cyclotomic polynomials and algebraic independence for q-series

Frédéric Jouhet

Institut Camille Jordan - University Lyon 1

Séminaire Flajolet, IHP, September 2018

(joint work with B. Adamczewski, É. Delaygue, and J. Bell)

The p-Lucas congruences

After Lucas (1878), a great attention has been paid on congruences modulo prime numbers p satisfied by various combinatorial sequences related to binomial coefficients.

Example.

$$\binom{2(pn+m)}{pn+m}^r \equiv \binom{2m}{m}^r \binom{2n}{n}^r \mod p,$$

where $0 \leq m \leq p-1$ and $n \geq 0, r \geq 1$.

Definition

For a prime number p, a sequence $(a(\mathbf{n}))_{\mathbf{n}\in\mathbb{N}^d}$ with integral values is p-Lucas if for any $\mathbf{n} \in \mathbb{N}^d$

$$a(p\mathbf{n}+\mathbf{m}) \equiv a(\mathbf{m})\, a(\mathbf{n}) \mod p \qquad \text{for all} \quad \mathbf{m} \in \{0, \dots, p-1\}^d.$$

Other examples

Binomial coefficients $\binom{n}{k}$, $\binom{2n}{n}^r$

Factorial ratios $\dfrac{(10n)!}{(5n)!(3n)!n!^2}$

Apéry sequences $\displaystyle\sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2$

Franel numbers $\displaystyle\sum_{k=0}^{n} \binom{n}{k}^3$

Or $\displaystyle\sum_{\substack{k=0 \\ k\equiv n \bmod 2}}^{\lfloor n/3 \rfloor} 2^k 3^{\frac{n-3k}{2}} \binom{n}{k} \binom{n-k}{\frac{n-k}{2}} \binom{\frac{n-k}{2}}{k}.$

Objectives

We will consider the following problems :

- Find an explanation to the omnipresence of sequences satisfying such congruences.
- Get a general result allowing us to derive all these congruences and generalize them to congruences modulo cyclotomic polynomials.
- Prove algebraic independence results for the generating series associated with such sequences.

A generating series approach

Define $g_r(x) := \sum_{n=0}^{\infty} \binom{2n}{n}^r x^n$. Then we have

$$\begin{aligned} g_r(x) &\equiv \sum_{m=0}^{p-1} \sum_{n=0}^{+\infty} \binom{2m}{m}^r \binom{2n}{n}^r x^{pn+m} \mod p\mathbb{Z}[[x]] \\ &\equiv \left(\sum_{m=0}^{p-1} \binom{2m}{m}^r x^m \right) g_r(x^p) \mod p\mathbb{Z}[[x]]. \end{aligned}$$

The p-Lucas property of the coefficients is actually equivalent to

$$g_r(x) \equiv A(x) g_r(x^p) \mod p\mathbb{Z}[[x]],$$

where $A(x) \in \mathbb{Z}[x]$ depends on r and p, and has degree at most $p-1$.

This means that the reduction modulo p of $g_r(x)$ satisfies an Ore equation of order 1, for all prime numbers p.

Motivations

Furstenberg (1967) and Deligne (1983) proved that the diagonal of a multivariate algebraic power series $f(\mathbf{x}) \in \mathbb{Q}[[\mathbf{x}]]$ is algebraic modulo p for almost all prime numbers p.

Adamczewski–Bell (2013) proved that when $f(\mathbf{x}) \in \mathbb{Z}[[\mathbf{x}]]$ the reductions modulo p of such diagonals satisfy an Ore equation of an order r independant of p : there exist $A_i(x) \in \mathbb{F}_p[x]$ such that

$$A_0(x)\Delta(f)_{|p}(x) + A_1(x)\Delta(f)_{|p}(x)^p + \cdots + A_r(x)\Delta(f)_{|p}(x)^{p^r} = 0.$$

Christol (1985) conjectured that any power series in $\mathbb{Z}[[x]]$, D-finite and with a positive radius of convergence, is the diagonal of a rational fraction.

Adamczewski–Bell–Delaygue (2016) proved that a large class of functions satisfy, as $g_r(x)$, a linear equation of order 1 with respect to (an iteration of) the Frobenius, for all prime numbers p.

q-series and cyclotomic polynomials

Fix a complex number q. Recall the classical q-analogues

$$[n]_q := \frac{1-q^n}{1-q} \quad \text{so that} \quad [n]_q! := \prod_{i=1}^{n} \frac{1-q^i}{1-q}$$

tends to $n!$ when $q \to 1$.

The classical q-binomial coefficients are

$$\begin{bmatrix} n \\ k \end{bmatrix}_q := \frac{[n]_q!}{[n-k]_q![k]_q!} \in \mathbb{N}[q] \cdot$$

For a positive integer b, recall the b-th cyclotomic polynomial

$$\phi_b(q) := \prod_{\substack{0 \le k < b-1 \\ (k,b)=1}} (q - e^{2ik\pi/b}).$$

Extension of the p-Lucas property

In 1967, Fray proved that for all nonnegative integers n and $0 \leq i, j \leq b-1$:

$$\begin{bmatrix} bn+i \\ bk+j \end{bmatrix}_q \equiv \begin{bmatrix} i \\ j \end{bmatrix}_q \binom{n}{k} \bmod \phi_b(q)\mathbb{Z}[q] \,.$$

Definition

For a positive integer b, a sequence $(a_q(\mathbf{n}))_{\mathbf{n}\in\mathbb{N}^d}$ with values in $\mathbb{Z}[q]$ is ϕ_b-Lucas if

$$a_q(b\mathbf{n}+\mathbf{m}) \equiv a_q(\mathbf{m})\, a_1(\mathbf{n}) \bmod \phi_b(q)\mathbb{Z}[q] \quad \text{for all} \quad \mathbf{m} \in \{0, \ldots, b-1\}^d.$$

Remark. If $(a_q(\mathbf{n}))_{\mathbf{n}\in\mathbb{N}^d}$ is ϕ_b-Lucas for all b, then $(a_1(\mathbf{n}))_{\mathbf{n}\in\mathbb{N}^d}$ is p-Lucas for all primes p. This comes from

$$\phi_p(1) = p.$$

Another example

We have by Fray (1967), Strehl (1982), Sagan (1992) :

$$\begin{bmatrix} 2(m+nb) \\ m+nb \end{bmatrix}_q^r \equiv \begin{bmatrix} 2m \\ m \end{bmatrix}_q^r \binom{2n}{n}^r \mod \phi_b(q)\mathbb{Z}[q]\,,$$

where n, m, b, r are nonnegative integers with $b, r \geq 1$ and $0 \leq m \leq b-1$.

In terms of generating series, this is equivalent to

$$f_r(q;x) \equiv A(q;x) g_r(x^b) \mod \phi_b(q)\mathbb{Z}[q]\,[[x]]\,,$$

where $A(q;x) \in \mathbb{Z}[q][x]$ of degree (in x) at most $b-1$ and

$$f_r(q;x) := \sum_{n=0}^{\infty} \begin{bmatrix} 2n \\ n \end{bmatrix}_q^r x^n, \quad g_r(x) = f_r(1;x).$$

q-factorial ratios and the Landau function

Given d-tuples of positive integers $\mathbf{e}_1, \ldots, \mathbf{e}_u$ and $\mathbf{f}_1, \ldots, \mathbf{f}_v$, set :

$$\mathcal{Q}(q;\mathbf{n}) = \mathcal{Q}_{e,f}(q;\mathbf{n}) := \frac{[\mathbf{e}_1 \cdot \mathbf{n}]_q! \cdots [\mathbf{e}_u \cdot \mathbf{n}]_q!}{[\mathbf{f}_1 \cdot \mathbf{n}]_q! \cdots [\mathbf{f}_v \cdot \mathbf{n}]_q!} \quad \text{for} \quad \mathbf{n} \in \mathbb{N}^d.$$

Define the Landau function on $\mathbb{R}^d$ by :

$$\Delta(\mathbf{x}) = \Delta_{e,f}(\mathbf{x}) := \sum_{i=1}^{u} \lfloor \mathbf{e}_i \cdot \mathbf{x} \rfloor - \sum_{j=1}^{v} \lfloor \mathbf{f}_j \cdot \mathbf{x} \rfloor .$$

We assume that $\sum_{i=1}^{u} \mathbf{e}_i = \sum_{j=1}^{v} \mathbf{f}_j$, denoted $|e| = |f|$. Therefore Δ is 1-periodic in all directions.

A general congruence for q-factorial ratios

Define

$$D := \{\mathbf{x} \in [0,1)^d \ : \ \text{there exists } i \text{ such that } \mathbf{e}_i \cdot \mathbf{x} \geq 1 \text{ or } \mathbf{f}_i \cdot \mathbf{x} \geq 1 \ \}.$$

Proposition (ABDJ, 2017)

If $\Delta \geq 1$ on the set D, then for any $\mathbf{n} \in \mathbb{N}^d$, we have $\mathcal{Q}(q;\mathbf{n}) \in \mathbb{Z}[q]$ and the sequence $\mathcal{Q}(q;\mathbf{n})$ is ϕ_b-Lucas for all positive integers b. In other words for all $b \geq 1$ and $\mathbf{m} \in \{0,\ldots,b-1\}^d$, we have

$$\mathcal{Q}(q; b\mathbf{n}+\mathbf{m}) \equiv \mathcal{Q}(q;\mathbf{m})\,\mathcal{Q}(1;\mathbf{n}) \bmod \phi_b(q)\mathbb{Z}[q].$$

Tools for the proof

We have

$$\frac{1-q^n}{1-q} = \prod_{b\geq 2,\, b|n} \phi_b(q) \Longrightarrow [n]_q! = \prod_{b=2}^{n} \phi_b(q)^{\lfloor n/b \rfloor},$$

and so

$$\mathcal{Q}(q;\mathbf{n}) = \prod_{b=2}^{\infty} \phi_b(q)^{\Delta(\mathbf{n}/b)}.$$

Thus

$$\mathcal{Q}(q;\mathbf{n}) \in \mathbb{Z}[q] \iff \Delta(\mathbf{n}/b) \geq 0 \ \ \forall b \geq 2$$

$$\mathcal{Q}(q;\mathbf{n}) \equiv 0 \bmod \phi_b(q)\mathbb{Z}[q] \iff \Delta(\mathbf{n}/b) \geq 1.$$

Given two polynomials $A(q)$ and $B(q)$, we have

$A(q) \equiv B(q) \bmod \phi_b(q)\mathbb{Z}[q] \Leftrightarrow A(\xi) = B(\xi) \quad \forall\, \xi$ primitive b-th root of 1.

Example

Take $d = 1$, $u = r, v = 2r$, and

$$e_1 = \cdots = e_r = 2, f_1 = \cdots = f_{2r} = 1, \text{ so that } |e| = |f|.$$

We have

$$\mathcal{Q}(q;n) = \frac{[2n]_q!^r}{[n]_q!^{2r}} \quad \text{and} \quad \Delta(x) = r(\lfloor 2x \rfloor - 2\lfloor x \rfloor).$$

As $D = \{x \in [0,1) \, : \, 2x \geq 1\}$, we get that for $0 \leq m \leq b-1$,

$$\begin{bmatrix} 2(bn+m) \\ bn+m \end{bmatrix}_q^r \equiv \begin{bmatrix} 2m \\ m \end{bmatrix}_q^r \binom{2n}{n}^r \mod \phi_b(q)\mathbb{Z}[q].$$

Functional approach

Set $F(q;\mathbf{x}) := \sum_{\mathbf{n}\in\mathbb{N}^d} \mathcal{Q}(q;\mathbf{n})\mathbf{x}^{\mathbf{n}}$. The ϕ_b-Lucas property above is :

$$F(q;\mathbf{x}) \equiv A(q;\mathbf{x})\, F(1;\mathbf{x}^b) \bmod \phi_b(q)\mathbb{Z}[q][[\mathbf{x}]],$$

where $A(q;\mathbf{x}) \in \mathbb{Z}[q][\mathbf{x}]$ has degree at most $b-1$ in each variable.

Proposition (specialization, ABDJ, 2017)

Let $\mathbf{t} \in \mathbb{N}^{\mathbf{d}}$ and $\mathbf{m} \in \mathbb{N}^d$ be such that if $\mathbf{x}$ in $[0,1)^d$ satisfies $\mathbf{m}\cdot\mathbf{x} \geq 1$, then $\Delta(\mathbf{x}) \geq 1$. If $\Delta \geq 1$ on the set D, then the coefficients of the series $F(q; q^{t_1}x^{m_1}, \ldots, q^{t_d}x^{m_d})$ are also ϕ_b-Lucas.

Example

Set

$$F(q;x,y) := \sum_{i,j\geq 0} \frac{[2i+j]_q!^2}{[i]_q!^4[j]_q!^2}\, x^i y^j.$$

Then $e_1, e_2 = (2;1)$; $f_1,\dots,f_4 = (1;0)$; $f_5, f_6 = (0;1)$, and

$\Delta(x,y) = 2\lfloor 2x+y\rfloor \geq 1$ for $(x,y) \in D = \{(x,y)\in[0;1)^2 : 2x+y\geq 1\}$.

Moreover if $0 \leq x, y < 1$ satisfy $x+y\geq 1$, then $\Delta(x;y)\geq 1$. As

$$F(q;x,x) = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q^2 \begin{bmatrix} n+k \\ k \end{bmatrix}_q^2\right) x^n,$$

we derive that $\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q^2 \begin{bmatrix} n+k \\ k \end{bmatrix}_q^2$ is ϕ_b-Lucas.

An algebraic independence result

Recall that the multivariate power series $f_1(\mathbf{x}), \ldots, f_n(\mathbf{x})$ are algebraically dependent over $\mathbb{C}(\mathbf{x})$ if there exists a non-zero polynomial $P(Y_1, \ldots, Y_n)$ in $\mathbb{C}[\mathbf{x}][Y_1, \ldots, Y_n]$ such that $P(f_1, \ldots, f_n) = 0$. Otherwise they are algebraically independent over $\mathbb{C}(\mathbf{x})$.

Adamczewski–Bell–Delaygue developped a general method (alternative to the differential Galois theory) to prove algebraic independence of power series whose coefficients are p-Lucas.

Theorem (Adamczewski–Bell–Delaygue, 2016)

Let $f_1(\mathbf{x}), \ldots, f_r(\mathbf{x})$ be series with coefficients satisfying the p-Lucas property for all primes p. These series are algebraically dependent over $\mathbb{C}(\mathbf{x})$ if and only if there exist integers $a_1, \ldots, a_r$, not all zero, such that

$$f_1(\mathbf{x})^{a_1} \cdots f_r(\mathbf{x})^{a_r} \in \mathbb{Q}(\mathbf{x}).$$

An example

Corollary (Adamczewski–Bell–Delaygue, 2016)

All elements of the set $\left\{ g_r(x) = \sum_{n=0}^{\infty} \binom{2n}{n}^r x^n \, : \, r \geq 2 \right\}$ are algebraically independent over $\mathbb{C}(x)$.

Stanley (1980) conjectured (and proved when r is even) that the series g_r are transcendental over $\mathbb{C}(x)$ except for $r = 1$.

Flajolet (1987) and independently Sharif–Woodcock (1989) proved this conjecture by using the previously mentioned Lucas congruences.

This is also a consequence of the interlacing criterion proved by Beukers–Heckman (1989). Indeed, these series belong to the class of G-function, and are even generalized hypergeometric series.

A propagation phenomenon for algebraic independence

Theorem (ABDJ, 2017)

Let $q \neq 0$ be a complex number. Assume that for $1 \leq i \leq n$, the coefficients of the series $f_i(q; \mathbf{x}) \in \mathbb{Z}[q][[\mathbf{x}]]$ are ϕ_b-Lucas for all positive integers b. If the series $f_1(1; \mathbf{x}), \ldots, f_n(1; \mathbf{x})$ are algebraically independent over $\mathbb{C}(\mathbf{x})$, then their q-analogues $f_1(q; \mathbf{x}), \ldots, f_n(q; \mathbf{x})$ are also algebraically independent over $\mathbb{C}(\mathbf{x})$.

Corollary (ABDJ, 2017)

Let $q \in \mathbb{C}^*$. The series $f_r(q; x) = \sum_{n=0}^{\infty} \begin{bmatrix} 2n \\ n \end{bmatrix}_q^r x^n, \quad r \geq 2$, are algebraically independent over $\mathbb{C}(x)$.

Some consequences

Corollary 2 (ABDJ, 2017)

Let $q \neq 0$ be a complex number and $\mathcal{F}_q$ be the union of the three following sets :

$$\left\{ \sum_{n=0}^{\infty} \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q^r x^n,\ r \geq 3 \right\}, \quad \left\{ \sum_{n=0}^{\infty} \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q^r \begin{bmatrix} n+k \\ k \end{bmatrix}_q^r x^n,\ r \geq 2 \right\},$$

and

$$\left\{ \sum_{n=0}^{\infty} \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q^{2r} \begin{bmatrix} n+k \\ k \end{bmatrix}_q^r x^n,\ r \geq 1 \right\}.$$

Then all elements of $\mathcal{F}_q$ are algebraically independent over $\mathbb{C}(x)$.

Proving the propagation theorem

We need the following tools.

- A Kolchin-like proposition for algebraically dependent power series $f_1, \dots, f_n$ whose coefficients belong to a finite extension of $\mathbb{F}_p$ of degree d_p and which satisfy $f_i(\mathbf{x}) = A_i(\mathbf{x}) f_i(\mathbf{x}^{p^k})$ for some $A_i \in F[\mathbf{x}]$, where $k \mid d_p$ is a fixed positive integer.

- A property extending the linear dependence over $R/\mathfrak{p}$ of the series $f_{1|\mathfrak{p}}, \dots, f_{n|\mathfrak{p}}$ to the linear dependence of the series $f_1, \dots, f_n$ over the field of fractions of R, where R is a domain and $\mathfrak{p}$ belongs to a set $\mathcal{S}$ of maximal ideals of R whose intersection is reduced to $\{0\}$.

- Algebraic properties of the ring $\mathbb{Z}[q]$, for which we have to distinguish whether q is transcendental or algebraic. These properties are crucial if one aims to reduce modulo prime numbers and cyclotomic polynomials at the same time.

Algebraic properties of the ring $\mathbb{Z}[q]$, q transcendental

Proposition (ABDJ, 2017)

Let q be a transcendental number. Then there exists an infinite set $\mathcal{S}$ of maximal ideals of $R = \mathbb{Z}[q]$ of finite index satisfying

$$\bigcap_{\mathfrak{p} \in \mathcal{S}'} \mathfrak{p} = \{0\} \quad \text{for all infinite subset} \quad \mathcal{S}' \subseteq \mathcal{S}, \tag{1}$$

and such that, for all $\mathfrak{p}$ in $\mathcal{S}$, we have $\phi_{b_\mathfrak{p}}(q)\mathbb{Z}[q] \subset \mathfrak{p}$ for some number $b_\mathfrak{p}$ (depending on $\mathfrak{p}$).

Proof (sketch). Any maximal ideal of $\mathbb{Z}[x]$ is generated by a pair $(p, A(x))$, where p is prime and $A(x) \in \mathbb{Z}[x]$ is irreducible modulo p. For a fixed prime number b, Chebotarev theorem implies that for an infinite number of primes p, $\phi_b(x)$ is irreducible modulo p. Therefore there exists an infinite sequence of maximal ideals of $\mathbb{Z}[x]$ of the form $\mathfrak{p}_n = (p_n, \phi_{b_n}(x))$, where $(p_n)_n$ and $(b_n)_n$ are both increasing sequences of prime numbers.

Algebraic properties of the ring $\mathbb{Z}[q]$, q algebraic

Proposition (ABDJ, 2017)

Set $q \neq 0$ an algebraic number. We let K be the number field $\mathbb{Q}(q)$ and $R = \mathcal{O}(K)$ be its ring of integers. Then there exists an infinite set $\mathcal{S}$ of maximal ideals of R of finite index satisfying (1) and such that, for all $\mathfrak{p} \in \mathcal{S}$, we have $\mathbb{Z}[q] \subset R_\mathfrak{p}$ and $\phi_{b_\mathfrak{p}}(q)\mathbb{Z}[q] \subset \mathfrak{p}R_\mathfrak{p}$ for some number $b_\mathfrak{p}$ (depending on $\mathfrak{p}$).

Proof (sketch). As R is a Dedekind domain, the intersection of any infinite subset of its maximal ideals is reduced to zero.

Moreover $\mathbb{Z}[q] \subset R_\mathfrak{p}$ for all but a finite number of maximal ideals $\mathfrak{p}$ of R.

We thus only need to prove the existence of an infinite set $\mathcal{S}$ of maximal ideals of finite index satisfying the second required inclusion.

Proof for q algebraic

Assume that q is a root of unity : set n such that q is a primitive n-th root of unity. Then $\phi_n(q) = 0$. If p is a prime not dividing n, we also have

$$\phi_{np}(x) = \frac{\phi_n\left(x^p\right)}{\phi_n(x)}\,.$$

Following Dirichlet, there exists an infinite number of primes p such that $p \equiv 1 \mod n$, condition that we suppose from now on. Therefore q is a root of both $\phi_n(x)$ and $\phi_n\left(x^p\right)$. As $\phi_n(x)$ only has simple roots :

$$\phi_{np}(q) = \frac{pq^{p-1}\phi'_n\left(q^p\right)}{\phi'_n(q)} = p\,.$$

For each $p \equiv 1 \mod n$, we let $\mathfrak{p}$ be a maximal ideal of R containing p, having therefore finite index. The set $\mathcal{S}$ of these maximal ideals satisfies the desired inclusion, by choosing $b_{\mathfrak{p}} = np$.

If q is not a root of unity, one can use the S-unit theorem.