Transferts d'indépendance algébrique et congruences à la Lucas

Frédéric Jouhet

Institut Camille Jordan - University Lyon 1

Équations fonctionnelles et interactions, Anglet, June 2019

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

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 $\mathbf{n} \in \mathbb{N}^d$

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

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.

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

A set of generalized p-Lucas series

Definition (Adamczewski–Bell–Delaygue, 2016)

Let R be a Dedekind domain and K be its field of fractions. Let $\mathcal{S}$ be a set of maximal ideals of R and $R_{\mathfrak{p}}$ the localization of R at a maximal ideal $\mathfrak{p}$. Let $\mathbf{x} = (x_1, \dots, x_d)$ and $\mathcal{L}_d(R, \mathcal{S})$ denote the set of all power series $f(\mathbf{x})$ in $K[[\mathbf{x}]]$ with constant term equal to 1 and such that for every $\mathfrak{p} \in \mathcal{S}$:

(i) $f(\mathbf{x}) \in R_{\mathfrak{p}}[[\mathbf{x}]]$.

(ii) The residue field $R/\mathfrak{p}$ is finite (of characteristic p).

(iii) There exist a positive integer $k_{\mathfrak{p}}$ and a rational fraction $A_{\mathfrak{p}} \in K(\mathbf{x}) \cap R_{\mathfrak{p}}[[\mathbf{x}]]$ satisfying

$$f(\mathbf{x}) \equiv A_{\mathfrak{p}}(\mathbf{x}) f\left(\mathbf{x}^{p^{k_{\mathfrak{p}}}}\right) \mod \mathfrak{p} R_{\mathfrak{p}}[[\mathbf{x}]].$$

(iv) The height of $A_{\mathfrak{p}}$ satisfies $H(A_{\mathfrak{p}}) \leq C p^{k_{\mathfrak{p}}}$ for some constant C independent of $\mathfrak{p}$.

An algebraic independence result

Theorem (Adamczewski–Bell–Delaygue, 2016)

Let $f_1(\mathbf{x}), \ldots, f_r(\mathbf{x})$ be series in $\mathcal{L}_d(R, \mathcal{S})$, where $\mathcal{S}$ is infinite. These series are algebraically dependent over $K(\mathbf{x})$ if and only if there exist integers $a_1, \ldots, a_r$, not all zero, such that

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

Corollary

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 $\mathbb{C}(x)$.

Properties of the sets $\mathcal{L}_d(R, \mathcal{S})$

The sets $\mathcal{L}_d(R, \mathcal{S})$ satisfy the following properties :

- They have a structure of multiplicative group with respect to the usual Cauchy product.
- They are closed under pullback of rational functions.
- They allow one to deal with power series, such as some hypergeometric series, which satisfy p-Lucas congruences only for some infinite subsets of prime numbers.
- They are well-behaved under various specializations of power series in several variables.

However the sets $\mathcal{L}_d(R, \mathcal{S})$ are not necessarily closed under formal derivative.

Remark. If $f(x) \equiv A(x)f(x^p) \mod p\mathbb{Z}[[x]]$, then

$$f'(x) \equiv A'(x)f(x^p) \mod p\mathbb{Z}[[x]].$$

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

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

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

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

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

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

Recall

$$g_r'(x) \equiv A'(1;x) g_r(x^p) \mod p\mathbb{Z}[[x]].$$

The p-Lucas algebras

We first extend the framework and sets $\mathcal{L}_d(R,\mathcal{S})$ of ABD. Let R be a domain and $\mathcal{S}$ be an infinite set of maximal ideals of R. We say that $\mathcal{S}$ satisfies the *zero intersection property* (ZIP) if for each infinite subset $\mathcal{S}'$ of $\mathcal{S}$, we have $\bigcap_{\mathfrak{p}\in\mathcal{S}'} \mathfrak{p} = \{0\}$.

Definition

Let $g(\mathbf{x}) \in \mathcal{L}_d(R,\mathcal{S})$, where R is a domain and $\mathcal{S}$ satisfies the ZIP. For a sequence $b = (b_\mathfrak{p})_{\mathfrak{p}\in\mathcal{S}}$ of positive integers, let $\mathcal{A}(g,R,\mathcal{S},b)$ denote the set of all power series $f(\mathbf{x}) \in K[[\mathbf{x}]]$ for which there exists a positive integer $\mathfrak{m}$ such that for almost all maximal ideals $\mathfrak{p} \in \mathcal{S}$:

(i) $f(\mathbf{x}) \in R_\mathfrak{p}[[\mathbf{x}]]$.

(ii) There exists a polynomial $P(y) \in K(\mathbf{x}) \cap R_\mathfrak{p}[[\mathbf{x}]][y]$, with degree at most $\mathfrak{m}$ and no constant term, such that

$$f(\mathbf{x}) \equiv P\left(g\left(\mathbf{x}^{b_\mathfrak{p}}\right)\right) \mod \mathfrak{p}R_\mathfrak{p}[[\mathbf{x}]] .$$

Properties of the sets $\mathcal{A}(g, R, \mathcal{S}, b)$

The sets $\mathcal{A}(g, R, \mathcal{S}, b)$ have a structure of (non-unitary) $K(\mathbf{x})$-algebra, which are well-behaved under specializations of the vectors of variables.

Moreover :

(a) Let $g(\mathbf{x}) \in \mathcal{L}_d(R, \mathcal{S})$ and ∂ be a derivation defined on $K[[\mathbf{x}]]$. Choosing $b_{\mathfrak{p}} = p^{k_{\mathfrak{p}}}$ for every $\mathfrak{p} \in \mathcal{S}$, $\mathcal{A}(g, R, \mathcal{S}, b)$ endowed with ∂ forms a differential $K(\mathbf{x})$-algebra containing $g(\mathbf{x})$.

(b) Let $g(\mathbf{x}) \in \mathcal{L}_d(\mathbb{Z}, \mathcal{P})$ and q be a non-zero complex number. Then there exist data $(R, \mathcal{S}, b)$ such that $\mathcal{A}(g, R, \mathcal{S}, b)$ endowed with the partial Jackson q-derivative forms a q-difference $K(\mathbf{x})$-algebra.

Finally, there are explicit K-vector subspaces of $\mathcal{A}(g, R, \mathcal{S}, b)$ which are well-behaved under Hadamard product and diagonalization when g is in an explicit subset of $\mathcal{L}_d(R, \mathcal{S})$.

A propagation phenomenon for algebraic independence

Theorem (Adamczewski–Bell–Delaygue–J, 2019)

Let $g_1(\mathbf{x}), \dots, g_n(\mathbf{x})$ be power series in $\mathcal{L}_d(R, \mathcal{S})$, where $\mathcal{S}$ satisfies the *ZIP*. Let K be the field of fractions of R and $b = (b_{\mathfrak{p}})_{\mathfrak{p} \in \mathcal{S}}$ a sequence of positive integers. For every integer $i \in \{1, \dots, n\}$, let $f_i(\mathbf{x})$ be a non-zero element of $\mathcal{A}(g_i, R, \mathcal{S}, b)$. If $f_1(\mathbf{x}), \dots, f_n(\mathbf{x})$ are algebraically dependent over $K(\mathbf{x})$, then there exist $a_1, \dots, a_n \in \mathbb{Z}$, not all zero, such that

$$g_1(\mathbf{x})^{a_1} \cdots g_n(\mathbf{x})^{a_n} \in K(\mathbf{x}).$$

In particular, if $g_1(\mathbf{x}), \dots, g_n(\mathbf{x})$ are algebraically independent over $K(\mathbf{x})$, then $f_1(\mathbf{x}), \dots, f_n(\mathbf{x})$ are algebraically independent over $K(\mathbf{x})$.

Taking R a Dedekind domain, we have $g_i \in \mathcal{A}(g_i, R, \mathcal{S}, b)$ by choosing the sequence $b_{\mathfrak{p}} = 1$ and $P(y) = y$. As for Dedekind domains maximal ideals coincide with primes, the ZIP is satisfied by any infinite family of prime ideals and we derive the algebraic independence criterion of ABD.

A consequence on derivatives

Corollary

For every positive integer r, let $P_r(x, y)$ be a non-zero polynomial in $\overline{\mathbb{Q}}[x, y]$ such that the power series

$$f_r(x) := \sum_{n=0}^{\infty} \sum_{k=0}^{n} P_r(k, n) \binom{n}{k}^{2r} \binom{n+k}{k}^{2r} x^n$$

is non-zero. Then all elements of the set $\mathcal{F} := \{f_r : r \geq 1\}$ are algebraically independent over $\mathbb{C}(x)$.

Proof. Use the series $g_r(x_1, x_2) := \sum_{n_1, n_2 \geq 0} \frac{(2n_1 + n_2)!^{2r}}{n_1!^{4r} n_2!^{2r}} x_1^{n_1} x_2^{n_2}$ and

$$\left(x_1 \frac{\partial}{\partial x_1}\right)^i \left(x_1 \frac{\partial}{\partial x_1}\right)^j (g_r)(x, x) = \sum_{n=0}^{\infty} \sum_{k=0}^{n} k^i (n-k)^j \binom{n}{k}^{2r} \binom{n+k}{n}^{2r} x^n.$$

Consequences on q-analogues

Corollary 1

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 $\mathbb{C}(x)$.

Proof. There are data $R, \mathcal{S}, b$ such that $f_r(q;x)$ belongs to $\mathcal{A}(f_r(1;x), R, \mathcal{S}, b)$.

Corollary 2

Let $q \in \mathbb{C}^*$. The series

$$f_r(q;x) = \sum_{n=0}^{\infty} \sum_{k=0}^{n} q^{r(n-k)^2} \begin{bmatrix} n \\ k \end{bmatrix}_q^{2r} \begin{bmatrix} n+k \\ k \end{bmatrix}_q^{2r} x^n, \quad r \geq 1,$$

are algebraically independent over $\mathbb{C}(x)$.

Algebraic relations within p-Lucas algebras

Let $\mathcal{A}^k(g, R, \mathcal{S}, b)$ denote the set of power series f in $\mathcal{A}(g, R, \mathcal{S}, b)$ for which the polynomial $P(y)$ can be chosen a monomial of degree k in y. Then $\mathcal{A}(g, R, \mathcal{S}, b)$ is a graded algebra :

$$\mathcal{A}(g, R, \mathcal{S}, b) = \bigoplus_{k \geq 1} \mathcal{A}^k(g, R, \mathcal{S}, b) = \bigoplus_{k \geq 1} \mathcal{A}^1(g^k, R, \mathcal{S}, b).$$

Theorem (Adamczewski–Bell–Delaygue–J, 2019)

Let R be a domain, K its field of fractions, $\mathcal{S}$ a set of maximal ideals of R with finite index satisfying the ZIP. Let $g \in \mathcal{L}_d(R, \mathcal{S})$ be transcendental over $K(\mathbf{x})$ and let $b = (b_\mathfrak{p})_{\mathfrak{p} \in \mathcal{S}}$ be a family of positive integers. Consider non-zero power series $f_1, \ldots, f_n$ in $\mathcal{A}^k(g, R, \mathcal{S}, b)$, for some positive integer k. Then the ideal of algebraic relations between $f_1, \ldots, f_n$

$$I := \{P \in K(\mathbf{x})[y_1, \ldots, y_n] \, : \, P(f_1, \ldots, f_n) = 0\}$$

is a homogeneous ideal of $K(\mathbf{x})[y_1, \ldots, y_n]$.

A consequence for G-functions

Proposition

Let R be a domain, K be its field of fractions, and $\mathcal{S}$ a set of maximal ideals of R with finite index satisfying the ZIP. Let $g \in \mathcal{L}_1(R, \mathcal{S})$ be a transcendental power series over $K(x)$ and $b = (b_{\mathfrak{p}})_{\mathfrak{p} \in \mathcal{S}}$ a sequence of positive integers. Let f_1 and f_2 be two power series in $\mathcal{A}^k(g, R, \mathcal{S}, b)$, where k is a positive integer. If f_1 and f_2 are algebraically dependent over $K(x)$, then the ratio f_1/f_2 belongs to $K(x)$.

Corollary

Let K be a number field and $\mathcal{S}$ be an infinite set of maximal ideals of $\mathcal{O}_K$, the ring of integers of K. Let $g(x)$ be a transcendental G-function in $\mathcal{L}_1(\mathcal{O}_K, \mathcal{S})$. Then $g(x)$ and $g'(x)$ are algebraically independent over $K(x)$.