Séminaire Lotharingien de Combinatoire **78B** (2017)
Article #54, 12 pp.

Proceedings of the 29th Conference on Formal Power Series and Algebraic Combinatorics (London)

Congruences modulo cyclotomic polynomials and algebraic independence for q-series

B. Adamczewski[1], J. P. Bell[2], É. Delaygue[1] and F. Jouhet*[1]

[1]*Univ Lyon, Université Claude Bernard Lyon 1, CNRS UMR 5208, Institut Camille Jordan, F-69622 Villeurbanne Cedex, France*
[2]*Department of Pure Mathematics, University of Waterloo, Waterloo, ON, Canada*

Abstract. We prove congruence relations modulo cyclotomic polynomials for multisums of q-factorial ratios, therefore generalizing many well-known p-Lucas congruences. Such congruences connect various classical generating series to their q-analogs. Using this, we prove a propagation phenomenon: when these generating series are algebraically independent, this is also the case for their q-analogs.

Résumé. Nous démontrons des relations de congruences modulo des polynômes cyclotomiques pour des sommes multiples de quotients de q-factorielles, ce qui généralise de nombreuses congruences p-Lucas. Ces congruences relient des familles classiques de séries génératrices et leurs q-analogues. Nous en déduisons un phénomène de propagation : l'indépendance algébrique de telles séries génératrices se transmet systématiquement à leurs q-analogues.

Keywords: cyclotomic polynomials, congruences, q-analogs, algebraic independence.

1 Introduction and main results

After the seminal work of Lucas [9], a great attention has been paid on congruences modulo prime numbers p satisfied by various combinatorial sequences related to binomial coefficients. A typical example of these so-called p-Lucas congruences is given by:

$$\binom{2(m+np)}{m+np}^r \equiv \binom{2m}{m}^r \binom{2n}{n}^r \mod p, \tag{1.1}$$

where $0 \leq m \leq p-1$, $r \geq 1$, and $n \geq 0$. In terms of generating series these congruences (1.1) translate as

$$g_r(x) \equiv A(x) g_r(x^p) \mod p\mathbb{Z}[[x]], \tag{1.2}$$

where

$$g_r(x) := \sum_{n=0}^{\infty} \binom{2n}{n}^r x^n$$

*jouhet@math.univ-lyon1.fr

and $A(x)$ is a polynomial (depending on r and p) in $\mathbb{Z}[x]$ of degree at most $p-1$. This functional point of view led the authors of [2] to define general sets of multivariate power series including the following one which is of particular interest for our purpose.

Definition 1.1. *Let d be a positive integer and $\mathbf{x} = (x_1, \dots, x_d)$ be a vector of indeterminates. We let $\mathfrak{L}_d$ denote the set of all power series $g(\mathbf{x})$ in $\mathbb{Z}[[\mathbf{x}]]$ with constant term equal to 1 and such that for every prime number p:*

(i) *there exist a positive integer k and a polynomial A in $\mathbb{Z}[\mathbf{x}]$ satisfying*

$$g(\mathbf{x}) \equiv A(\mathbf{x})g\left(\mathbf{x}^{p^k}\right) \mod p\mathbb{Z}[[\mathbf{x}]].$$

(ii) $\deg_{x_i}(A) \leq p^k - 1$ *for all i, $1 \leq i \leq d$.*

Using p-adic computations inspired by works of Christol and Dwork, it was proved in [2] that a large family of multivariate generalized hypergeometric series belongs to $\mathfrak{L}_d$. This provides, by specialization, a unified way to reprove most of known p-Lucas congruences as well as to find many new ones. In addition, a general method to prove algebraic independence of power series whose coefficients satisfy p-Lucas type congruences was developed. Let us illustrate this approach with the following example. In 1980, Stanley [13] conjectured that the series g_r are transcendental over $\mathbb{C}(x)$ except for $r = 1$, in which case we have $g_1(x) = (\sqrt{1-4x})^{-1}$. He also proved the transcendence for r even. The conjecture was solved independently by Flajolet [6] through asymptotic considerations and by Sharif and Woodcock [12] by using the previously mentioned Lucas congruences. Incidentally, this result is also a consequence of the interlacing criterion proved by Beukers and Heckman [3] for generalized hypergeometric series. Though there are three different ways to obtain the transcendence of g_r for $r \geq 2$, not much was apparently known about their algebraic independence, until Congruence (1.1) was used in [1, 2] to prove the following result: *all elements of the set $\{g_r(x) : r \geq 2\}$ are algebraically independent over $\mathbb{C}(x)$.*

In the present work, we aim at generalizing the approach of [2] in the setting of q-series. It started with the following observation which can be derived from [7, 11, 14]:

$$\begin{bmatrix} 2(m+nb) \\ m+nb \end{bmatrix}_q^r \equiv \begin{bmatrix} 2m \\ m \end{bmatrix}_q^r \binom{2n}{n}^r \mod \phi_b(q)\mathbb{Z}[q]\,, \tag{1.3}$$

where n, m, b, r are nonnegative integers with $b \geq 1$, $0 \leq m \leq b-1$, and $\phi_b(x) := \prod_{k \wedge b = 1}(x - \mathrm{e}^{2ik\pi/b})$ denotes the bth cyclotomic polynomial over $\mathbb{Q}$. Here, for every complex number q, the central q-binomial coefficients are defined as

$$\begin{bmatrix} 2n \\ n \end{bmatrix}_q := \frac{[2n]_q!}{[n]_q!^2} \in \mathbb{N}[q], \text{ where } [n]_q! := \prod_{i=1}^{n} \frac{1-q^i}{1-q}$$

is the q-analog of $n!$. It is implicitly considered as a polynomial in q so that the formula is still valid for $q = 1$. In particular, one has $[n]_1! = n!$ and the congruence (1.3) allows one to recover (1.1) since $\phi_p(1) = p$. Moreover, congruences like (1.3) do not seem to be true in general if the cyclotomic polynomials are replaced by other polynomials, like for instance $(1-x^b)/(1-x)$. This convinced us that considering congruences modulo cyclotomic polynomials might be the correct point of view to generalize p-Lucas congruences. Again in terms of generating series, (1.3) translates as

$$f_r(q;x) \equiv A(q;x) g_r(x^b) \mod \phi_b(q)\mathbb{Z}[q]\,[[x]]\,, \tag{1.4}$$

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

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

This provides an arithmetic connection between the generating series $g_r(x)$ and its q-analog $f_r(q;x)$. It leads us to associate a set $\mathcal{D}(q;g)$ of q-deformations with every element g in $\mathfrak{L}_d$. We stress that $\mathcal{D}(q;g)$ is closed under q-derivation.

Definition 1.2. Let q be a fixed nonzero complex number. Let $g(\mathbf{x})$ be a power series in $\mathfrak{L}_d$. We let $\mathcal{D}(q;g)$ denote the set of all nonzero power series $f(q;\mathbf{x})$ in $\mathbb{Z}[q][[\mathbf{x}]]$ such that for all integers $b \geq 1$ there exists a polynomial $A(q;\mathbf{x})$ with coefficients in $\mathbb{Z}[q]$ satisfying:

$$f(q;\mathbf{x}) \equiv A(q;\mathbf{x}) g\left(\mathbf{x}^b\right) \mod \phi_b(q)\mathbb{Z}[q][[\mathbf{x}]].$$

Our first result shows a propagation phenomenon of algebraic independence from generating series in $\mathfrak{L}_d$ to their q-analogs. We stress that, in comparison with [2], some extra difficulties arise from the fact that $\mathbb{Z}[q]$ is in general not a Dedekind domain. We derive suitable properties for the ring $\mathbb{Z}[q]$ (see Proposition 4.2) from the S-unit theorem (respectively Chebotarev's theorem) when q is algebraic (respectively transcendental).

Theorem 1.3. *Let q be a nonzero complex number. Let $g_1(\mathbf{x}), \dots, g_n(\mathbf{x})$ be power series in $\mathfrak{L}_d$, which are algebraically independent over $\mathbb{C}(\mathbf{x})$. Then for any $f_i(q;\mathbf{x})$ in $\mathcal{D}(q;g_i)$, $1 \leq i \leq n$, the series $f_1(q;\mathbf{x}), \dots, f_n(q;\mathbf{x})$ are also algebraically independent over $\mathbb{C}(\mathbf{x})$.*

This immediately implies that all elements of the set $\{f_r(q;x) : r \geq 2\}$ are algebraically independent over $\mathbb{C}(x)$ for all nonzero complex numbers q. More generally, there is a long tradition for combinatorists in studying q-analogs of famous sequences of natural numbers, as the additional variable q gives the opportunity to refine the enumeration of combinatorial objects counted by the $q=1$ case. To some extent, the nature of a generating series reflects the underlying structure of the objects it counts [4]. By nature, we mean for instance whether the generating series is rational, algebraic, or D-finite. In the same line, algebraic (in)dependence of generating series can be considered as a reasonable way to measure how distinct families of combinatorial objects may be (un)related.

It is known from [2] that many generating series g of multisums of factorial ratios belong to $\mathfrak{L}_d$. For such series g, we will define q-analogs and prove that they lie in the set $\mathcal{D}(q;g)$. This will yield at once algebraic independence results, but also many generalizations of Congruence (1.3). Finding congruences with respect to cyclotomic polynomials is actually not a recent problem (see for instance [11, 8, 10] and the references cited there).

Our second result below is a general congruence relation extending (1.3) to the multidimensional case, by considering q-factorial ratios in the spirit of the ones in [15]. For positive integers d,u,v, let $e=(\mathbf{e}_1,\ldots,\mathbf{e}_u)$ and $f=(\mathbf{f}_1,\ldots,\mathbf{f}_v)$ be tuples of vectors in $\mathbb{N}^d$. For $\mathbf{n}\in\mathbb{N}^d$, we define a q-analog of multidimensional factorial ratios (see Section 2 for precise notations) by:

$$\mathcal{Q}_{e,f}(q;\mathbf{n}):=\frac{[\mathbf{e}_1\cdot\mathbf{n}]_q!\cdots[\mathbf{e}_u\cdot\mathbf{n}]_q!}{[\mathbf{f}_1\cdot\mathbf{n}]_q!\cdots[\mathbf{f}_v\cdot\mathbf{n}]_q!}\,.$$

Furthermore, we consider the Landau step function $\Delta_{e,f}$ defined on $\mathbb{R}^d$ by

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

We also define $|e|=\sum_{i=1}^{u}\mathbf{e}_i$, $|f|=\sum_{j=1}^{v}\mathbf{f}_j$, and set:

$$\mathcal{D}_{e,f}:=\left\{\mathbf{x}\in[0,1)^d\,:\,\text{there is }\mathbf{t}\text{ in }e\text{ or }f\text{ such that }\mathbf{t}\cdot\mathbf{x}\geq 1\right\}.$$

Proposition 1.4. *Let e and f be two tuples of vectors in $\mathbb{N}^d$ such that $|e|=|f|$ and $\Delta_{e,f}$ is greater than or equal to 1 on $\mathcal{D}_{e,f}$. Then, for every positive integer b, every $\mathbf{a}$ in $\{0,\ldots,b-1\}^d$ and every $\mathbf{n}$ in $\mathbb{N}^d$, we have $\mathcal{Q}_{e,f}(q;\mathbf{n})\in\mathbb{Z}[q]$ and*

$$\mathcal{Q}_{e,f}(q;\mathbf{a}+\mathbf{n}b)\equiv\mathcal{Q}_{e,f}(q;\mathbf{a})\mathcal{Q}_{e,f}(1;\mathbf{n})\mod\phi_b(q)\mathbb{Z}[q].$$

Proposition 1.4 extends many known results, both for q-analogs and p-Lucas congruences. For instance, choosing $d=1$, $u=1$, $v=2$, $e_1=2$, and $f_1=f_2=1$ yields (1.3), while taking b prime and $q=1$ allows one to recover Proposition 8.7 in [2]. As we will see in Section 3, Proposition 1.4 also leads to congruences for (multi-)sums of q-factorial ratios. As an illustration, we provide below two examples connected to the famous Apéry sequences.

Proposition 1.5. *Consider for a given nonnegative integer t the following q-analogs of the Apéry sequences*

$$a_n(q):=\sum_{k=0}^{n}q^{tk}\begin{bmatrix}n\\k\end{bmatrix}_q^2\begin{bmatrix}n+k\\k\end{bmatrix}_q\quad\text{and}\quad b_n(q):=\sum_{k=0}^{n}q^{tk}\begin{bmatrix}n\\k\end{bmatrix}_q^2\begin{bmatrix}n+k\\k\end{bmatrix}_q^2.$$

Then, for all nonnegative integers n,m,b with $b\geq 1$, $0\leq m\leq b-1$, we have

$$a_{m+nb}(q)\equiv a_m(q)a_n(1)\mod\phi_b(q)\mathbb{Z}[q]\quad\text{and}\quad b_{m+nb}(q)\equiv b_m(q)b_n(1)\mod\phi_b(q)\mathbb{Z}[q].$$

Setting

$$F_{e,f}(q;\mathbf{x}) := \sum_{\mathbf{n}\in\mathbb{N}^d} \mathcal{Q}_{e,f}(q;\mathbf{n})\mathbf{x}^{\mathbf{n}}$$

and assuming the conditions of Proposition 1.4, we obtain that $F_{e,f}(q;\mathbf{x})$ belongs to $\mathcal{D}(q;F_{e,f}(1;\mathbf{x}))$, as $F_{e,f}(1;\mathbf{x})$ is in $\mathfrak{L}_d$ by [2, Proposition 8.1]. Theorem 1.3 therefore implies that algebraic independence among series $F_{e,f}(1;\mathbf{x})$ propagates to their corresponding q-analogs $F_{e,f}(q;\mathbf{x})$. As noticed before, this holds for the series $g_r(x)$ and their q-analogs $f_r(q;x)$. Proposition 1.4 and a result about specializations of the series $F_{e,f}(q;\mathbf{x})$ (stated in Section 3) actually provide much more general results, such as the following one.

Proposition 1.6. *For a fixed nonzero complex number q, let $\mathcal{F}_q$ be the set formed by 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 $\mathbb{C}(x)$.

Proposition 1.6 is derived from Proposition 1.2 in [2], which corresponds to the case $q=1$.

In the next section, we fix some notation and recall basic facts about Dedekind domains. In Section 3, we focus on congruence relations modulo cyclotomic polynomials and prove Proposition 1.4. We also show how to derive results like Propositions 1.5 and 1.6. Finally, the last section is devoted to a sketch of proof of Theorem 1.3.

2 Background and notations

Let us introduce some notation and basic facts that will be used throughout this extended abstract. Let d be a positive integer. Given d-tuples of real numbers $\mathbf{m}=(m_1,\ldots,m_d)$ and $\mathbf{n}=(n_1,\ldots,n_d)$, we set $\mathbf{m}+\mathbf{n} := (m_1+n_1,\ldots,m_d+n_d)$ and $\mathbf{m}\cdot\mathbf{n} := m_1n_1+\cdots+m_dn_d$. If moreover λ is a real number, then we set $\lambda\mathbf{m} := (\lambda m_1,\ldots,\lambda m_d)$. We write $\mathbf{m}\geq\mathbf{n}$ if we have $m_k\geq n_k$ for all k in $\{1,\ldots,d\}$. We also set $\mathbf{0} := (0,\ldots,0)$ and $\mathbf{1} := (1,\ldots,1)$.

Polynomials. Given a d-tuple of natural numbers $\mathbf{n}=(n_1,\ldots,n_d)$ and a vector of indeterminates $\mathbf{x}=(x_1,\ldots,x_d)$, we will denote by $\mathbf{x}^{\mathbf{n}}$ the monomial $x_1^{n_1}\cdots x_d^{n_d}$. The (total) degree of such a monomial is the nonnegative integer $n_1+\cdots+n_d$. Given a ring R and a polynomial P in $R[\mathbf{x}]$, we denote by $\deg P$ the (total) degree of P, that is the maximum of the total degrees of the monomials appearing in P with nonzero coefficient. The partial degree of P with respect to the indeterminate x_i is denoted by $\deg_{x_i}(P)$.

Algebraic power series and algebraic independence. Let K be a field. We denote by $K[[\mathbf{x}]]$ the ring of formal power series with coefficients in K and associated with the vector of indeterminates $\mathbf{x}$. We say that a power series $f(\mathbf{x}) \in K[[\mathbf{x}]]$ is algebraic if it is algebraic over the field of rational functions $K(\mathbf{x})$, that is, if there exist polynomials $A_0, \ldots, A_m$ in $K[\mathbf{x}]$, not all zero, such that $A_0(\mathbf{x}) + A_1(\mathbf{x})f(\mathbf{x}) + \cdots + A_m(\mathbf{x})f(\mathbf{x})^m = 0$. Otherwise, f is said to be transcendental. Let $f_1, \ldots, f_n$ be in $K[[\mathbf{x}]]$. We say that $f_1, \ldots, f_n$ are algebraically dependent if they are algebraically dependent over the field $K(\mathbf{x})$, that is, if there exists a nonzero polynomial $P(Y_1, \ldots, Y_n)$ in $K[\mathbf{x}][Y_1, \ldots, Y_n]$ such that $P(f_1, \ldots, f_n) = 0$. When there is no algebraic relation between them, the power series $f_1, \ldots, f_n$ are said to be algebraically independent (over $K(\mathbf{x})$).

Dedekind domains. Let R be a Dedekind domain; that is, R is Noetherian, integrally closed, and every nonzero prime ideal of R is a maximal ideal. Furthermore, any nonzero element of R belongs to at most a finite number of maximal ideals of R. In other words, given an infinite set $\mathcal{S}$ of maximal ideals of R, then one always has $\bigcap_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p} = \{0\}$. For every power series $f(\mathbf{x}) = \sum_{\mathbf{n}\in\mathbb{N}^d} a(\mathbf{n})\mathbf{x}^{\mathbf{n}}$ with coefficients in R, we set

$$f_{|\mathfrak{p}}(\mathbf{x}) := \sum_{\mathbf{n}\in\mathbb{N}^d} \big(a(\mathbf{n}) \bmod \mathfrak{p}\big)\mathbf{x}^{\mathbf{n}} \in (R/\mathfrak{p})[[\mathbf{x}]]\,.$$

The power series $f_{|\mathfrak{p}}$ is called the reduction of f modulo $\mathfrak{p}$. Let K denote the field of fractions of R. The localization of R at a maximal ideal $\mathfrak{p}$ is denoted by $R_{\mathfrak{p}}$. Recall here that $R_{\mathfrak{p}}$ can be seen as the following subset of K:

$$R_{\mathfrak{p}} = \{a/b \,:\, a \in R, b \in R \setminus \mathfrak{p}\}\,.$$

Then $R_{\mathfrak{p}}$ is a discrete valuation ring and the residue field $R_{\mathfrak{p}}/\mathfrak{p}$ is equal to $R/\mathfrak{p}$.

3 Some general congruences and applications

We first give the detailed proof of Proposition 1.4, and we will then see how to derive results like Propositions 1.5 and 1.6.

Proof of Proposition 1.4. In this proof, we write $\mathcal{Q}$ for $\mathcal{Q}_{e,f}$, Δ for $\Delta_{e,f}$ and $\mathcal{D}$ for $\mathcal{D}_{e,f}$. Recall that for all nonnegative integers n we have

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

from which we deduce, by definition of the step function Δ,

$$\mathcal{Q}(q;\mathbf{n}) = \prod_{b=2}^{\infty} \phi_b(q)^{\Delta(\mathbf{n}/b)}. \tag{3.1}$$

As $|e| = |f|$, the function Δ is 1-periodic in each of its variable and one easily obtains from (3.1) that $\mathcal{Q}(q;\mathbf{n})$ is in $\mathbb{Z}[q]$ for every $\mathbf{n}$ in $\mathbb{N}^d$ if, and only if Δ is nonnegative over $\mathbb{R}^d$. This proves the first part of our proposition.

Let x be a complex variable. As $|e| = |f|$, we derive

$$\mathcal{Q}(x;\mathbf{a}+\mathbf{n}b) = \mathcal{Q}(x;\mathbf{n}b)\frac{\prod_{i=1}^{u}\prod_{k=1}^{\mathbf{e}_i\cdot\mathbf{a}}(1-x^{\mathbf{e}_i\cdot\mathbf{n}b+k})}{\prod_{j=1}^{v}\prod_{k=1}^{\mathbf{f}_j\cdot\mathbf{a}}(1-x^{\mathbf{f}_j\cdot\mathbf{n}b+k})}.$$

If $\mathbf{a}/b$ is not in $\mathcal{D}$, then for each $\mathbf{t}$ in e or f, no element of $\{1,\dots,\mathbf{t}\cdot\mathbf{a}\}$ is divisible by b. Hence, if ξ_b is a complex primitive bth root of unity, then we have

$$\mathcal{Q}(\xi_b;\mathbf{a}+\mathbf{n}b) = \mathcal{Q}(\xi_b;\mathbf{n}b)\frac{\prod_{i=1}^{u}\prod_{k=1}^{\mathbf{e}_i\cdot\mathbf{a}}(1-\xi_b^k)}{\prod_{j=1}^{v}\prod_{k=1}^{\mathbf{f}_j\cdot\mathbf{a}}(1-\xi_b^k)} = \mathcal{Q}(\xi_b;\mathbf{n}b)\mathcal{Q}(\xi_b;\mathbf{a}),$$

so that

$$\mathcal{Q}(x;\mathbf{a}+\mathbf{n}b) \equiv \mathcal{Q}(x;\mathbf{n}b)\mathcal{Q}(x;\mathbf{a}) \mod \phi_b(x)\mathbb{Z}[x]. \tag{3.2}$$

We shall prove that this congruence also holds when $\mathbf{a}/b$ belongs to $\mathcal{D}$. Indeed, in this case we have $\Delta(\mathbf{a}/b) \geq 1$ by assumption. By (3.1), the $\phi_b(x)$-valuation of $\mathcal{Q}(x;\mathbf{a}+\mathbf{n}b)$ is $\Delta(\frac{\mathbf{a}}{b}+\mathbf{n}) = \Delta(\mathbf{a}/b) \geq 1$, and the $\phi_b(x)$-valuation of $\mathcal{Q}(x;\mathbf{a})$ is also $\Delta(\mathbf{a}/b) \geq 1$. Hence both polynomials are divisible by $\phi_b(x)$ and (3.2) holds.

Now we shall prove that

$$\mathcal{Q}(x;\mathbf{n}b) \equiv \mathcal{Q}(1;\mathbf{n}) \mod \phi_b(x)\mathbb{Z}[x]. \tag{3.3}$$

We have

$$\mathcal{Q}(x;\mathbf{n}b) = \frac{\prod_{i=1}^{u}\prod_{k=1}^{\mathbf{e}_i\cdot\mathbf{n}b}(1-x^k)}{\prod_{j=1}^{v}\prod_{k=1}^{\mathbf{f}_j\cdot\mathbf{n}b}(1-x^k)} = \frac{\prod_{i=1}^{u}\prod_{k=1}^{\mathbf{e}_i\cdot\mathbf{n}}(1-x^{kb})}{\prod_{j=1}^{v}\prod_{k=1}^{\mathbf{f}_j\cdot\mathbf{n}}(1-x^{kb})} \times \prod_{\ell=1}^{b-1}\frac{\prod_{i=1}^{u}\prod_{k=1}^{\mathbf{e}_i\cdot\mathbf{n}-1}(1-x^{\ell+kb})}{\prod_{j=1}^{v}\prod_{k=1}^{\mathbf{f}_j\cdot\mathbf{n}-1}(1-x^{\ell+kb})}.$$

From $|e| = |f|$, we also derive

$$\frac{\prod_{i=1}^{u}\prod_{k=1}^{\mathbf{e}_i\cdot\mathbf{n}}(1-x^{kb})}{\prod_{j=1}^{v}\prod_{k=1}^{\mathbf{f}_j\cdot\mathbf{n}}(1-x^{kb})} = \frac{\prod_{i=1}^{u}\prod_{k=1}^{\mathbf{e}_i\cdot\mathbf{n}}\frac{1-x^{kb}}{1-x^b}}{\prod_{j=1}^{v}\prod_{k=1}^{\mathbf{f}_j\cdot\mathbf{n}}\frac{1-x^{kb}}{1-x^b}},$$

which is a rational fraction without pole at $x = \xi_b$ and whose value at ξ_b equals $\mathcal{Q}(1;\mathbf{n})$. Furthermore, for each ℓ in $\{1,\dots,b-1\}$, we have

$$\frac{\prod_{i=1}^{u}\prod_{k=1}^{\mathbf{e}_i\cdot\mathbf{n}-1}(1-\xi_b^{\ell+kb})}{\prod_{j=1}^{v}\prod_{k=1}^{\mathbf{f}_j\cdot\mathbf{n}-1}(1-\xi_b^{\ell+kb})} = (1-\xi_b^{\ell})^{(|e|-|f|)\cdot\mathbf{n}} = 1.$$

Since $\mathcal{Q}(x;\mathbf{n}b) \in \mathbb{Z}[x]$ and $\mathcal{Q}(\xi_b;\mathbf{n}b) = \mathcal{Q}(1;\mathbf{n})$, we obtain (3.3) as expected.

$\square$

We now show how Proposition 1.4 yields on the one hand congruences through a specialization rule, and on the other hand algebraic independence results.

Recall that, under the conditions of Proposition 1.4, we have

$$F_{e,f}(q;\mathbf{x}) = \sum_{\mathbf{n}\in\mathbb{N}^d} \mathcal{Q}_{e,f}(q;\mathbf{n})\mathbf{x}^{\mathbf{n}} \in \mathbb{Z}[q][[\mathbf{x}]] \,.$$

Then the congruence relation in Proposition 1.4 is equivalent to

$$F_{e,f}(q;\mathbf{x}) \equiv A(q;\mathbf{x})F_{e,f}(1;\mathbf{x}^b) \mod \phi_b(q)\mathbb{Z}[q][[\mathbf{x}]]$$

for every positive integer b and with the additional condition that $A(q;\mathbf{x})$ in $\mathbb{Z}[q][\mathbf{x}]$ satisfies $\deg_{x_i} A(q;\mathbf{x}) \leq b-1$ for all i, $1 \leq i \leq d$. The following proposition is the key to prove congruences for multisums of q-factorial ratios as in Proposition 1.6.

Proposition 3.1. *Assume the conditions of Proposition 1.4 are satisfied. Moreover, 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* $\Delta_{e,f}(\mathbf{x}) \geq 1$*. Then, for every positive integer* b*, we have:*

$$F_{e,f}(q;q^{t_1}x^{m_1},\ldots,q^{t_d}x^{m_d}) \equiv B(q;x)F_{e,f}(1;x^{bm_1},\ldots,x^{bm_d}) \mod \phi_b(q)\mathbb{Z}[q][[\mathbf{x}]],$$

where $B(q;x)$ *is a one variable polynomial in* $\mathbb{Z}[q][x]$ *satisfying* $\deg_x B(q;x) \leq b-1$.

Choosing $e = \big((2,1),(1,1)\big)$ and $f = \big((1,0),(1,0),(1,0),(0,1),(0,1)\big)$, we get that

$$F_{e,f}(q;x,y) = \sum_{n_1,n_2\geq 0} \frac{[2n_1+n_2]_q![n_1+n_2]_q!}{[n_1]_q!^3[n_2]_q!^2} x^{n_1}y^{n_2} \,.$$

By Proposition 2 in [5], the function $\Delta_{e,f}$ is greater than or equal to 1 on $\mathcal{D}_{e,f}$ so that the conditions of Proposition 1.4 are satisfied. Furthermore, we can use Proposition 3.1 with $\mathbf{t} = (t,0)$ and $\mathbf{m} = (1,1)$ which yields

$$F_{e,f}(q;q^t x,x) \equiv B(q;x)F_{e,f}(1;x^b,x^b) \mod \phi_b(q)\mathbb{Z}[q][[\mathbf{x}],$$

where $B(q;x)$ is a polynomial in $\mathbb{Z}[q][x]$ satisfying $\deg_x B(q;x) \leq b-1$. A direct computation shows that

$$F_{e,f}(q;q^t x,x) = \sum_{n=0}^{\infty}\sum_{k=0}^{n} q^{tk} {\begin{bmatrix} n \\ k \end{bmatrix}}_q^2 {\begin{bmatrix} n+k \\ k \end{bmatrix}}_q x^n$$

and

$$F_{e,f}(1;x,x) = \sum_{n=0}^{\infty}\sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k} x^n \,.$$

This yields the congruences for q-analogs of the first Apéry sequence $a_n(q)$ given in Proposition 1.5. The result for the second Apéry sequence $b_n(q)$ is derived along the same line.

To prove Proposition 1.6, we first show by Proposition 3.1 that each series $f(q;x)$ in $\mathcal{F}_q$ belongs to $\mathcal{D}(q;f(1;x))$. For example, we use the following specialization associated with $\mathbf{t}=(0,0)$ and $\mathbf{m}=(1,1)$:

$$\sum_{n=0}^{\infty}\sum_{k=0}^{n}\begin{bmatrix} n \\ k \end{bmatrix}_q^r x^n = F_{e,f}(q;x,x)\,,$$

where

$$F_{e,f}(q;x,y)=\sum_{n_1,n_2\geq 0}\frac{[n_1+n_2]_q!^r}{[n_1]_q!^r[n_2]_q!^r}x^{n_1}y^{n_2}\,.$$

By Proposition 1.2 and Section 9.3 in [2], we know that $\mathcal{F}_1$ (the set of all series $f(1;x)$) is a subset of $\mathfrak{L}_1$ and that all elements of $\mathcal{F}_1$ are algebraically independent over $\mathbb{C}(x)$. Hence Theorem 1.3 implies that, for every nonzero complex number q, all elements of $\mathcal{F}_q$ are algebraically independent over $\mathbb{C}(x)$.

4 Sketch of proof of Theorem 1.3

Though Theorem 1.3 holds true for all nonzero complex number q, we will focus here on the case where q is an algebraic number. The case where q is transcendental is actually simpler even if it requires specific considerations we do not want to deal with here for space limitation.

Throughout this section, we fix a nonzero algebraic number q. We let K be the number field $\mathbb{Q}(q)$ and $R:=\mathcal{O}(K)$ be its ring of integers. Recall that R is thus a Dedekind domain.

The proof of Theorem 1.3 relies on the following Kolchin-like proposition which is a special instance of Proposition 4.3 in [2].

Proposition 4.1. *Let p be a prime number, F be a finite extension of degree d_p of $\mathbb{F}_p$, and k be a positive integer such that $d_p \mid k$. Let $f_1,\dots,f_n$ be nonzero power series in $F[[\mathbf{x}]]$ satisfying $f_i(\mathbf{x})=A_i(\mathbf{x})f_i(\mathbf{x}^{p^k})$ for some $A_i\in F[\mathbf{x}]$ and every $1\leq i\leq n$. If $f_1,\dots,f_n$ satisfy a nontrivial polynomial relation of degree d with coefficients in $F(\mathbf{x})$, then there exist $m_1,\dots,m_n\in\mathbb{Z}$, not all zero, and a nonzero $r(\mathbf{x})\in F(\mathbf{x})$ such that*

$$A_1(\mathbf{x})^{m_1}\cdots A_n(\mathbf{x})^{m_n}=r(\mathbf{x})^{p^k-1}\,.$$

Furthermore, $|m_1+\cdots+m_n|\leq d$ and $|m_i|\leq d$ for $1\leq i\leq n$.

We will also need the following result which will enable us to connect reductions modulo prime numbers and modulo cyclotomic polynomials.

Proposition 4.2. *There exist an infinite set $\mathcal{S}$ of maximal ideals of R such that, for all $\mathfrak{p}\in\mathcal{S}$, we have $\mathbb{Z}[q]\subset R_{\mathfrak{p}}$ and $\phi_b(q)\mathbb{Z}[q]\subset\mathfrak{p}R_{\mathfrak{p}}$ for some prime number b (depending on $\mathfrak{p}$).*

For space limitation, Proposition 4.2 will not be proved here. Its proof is elementary when q is a root of unity and relies on the S-unit theorem otherwise. We will also need the two following auxiliary results, the first of which being Lemma 4.4 in [2].

Lemma 4.3. *Let R be a Dedekind domain, K be its field of fractions, and $g_1, \dots, g_n$ be power series in $R[[\mathbf{x}]]$. If $g_{1|\mathfrak{p}}, \dots, g_{n|\mathfrak{p}}$ are linearly dependent over $R/\mathfrak{p}$ for infinitely many maximal ideals $\mathfrak{p}$, then $f_1, \dots, f_n$ are linearly dependent over K.*

Lemma 4.4. *Let K be a commutative field and set b a positive integer. Let $r(\mathbf{x}) \in K(\mathbf{x})$ and $s(\mathbf{x}) \in K(\mathbf{x}) \cap K[[\mathbf{x}]]$ be two rational fractions such that $s(\mathbf{0}) \neq 0$. If there exists a nonzero (mod p if char$(K) = p$) integer m satisfying $s(\mathbf{x}^b) = r(\mathbf{x})^m$, then there exists $t(\mathbf{x})$ in $K(\mathbf{x})$ such that $r(\mathbf{x}) = t(\mathbf{x}^b)$.*

Proof of Theorem 1.3. Let $\mathcal{S}$ be the set of maximal ideals of $R := \mathcal{O}(K)$ given in Proposition 4.2. With all $\mathfrak{p}$ in $\mathcal{S}$, we associate a prime number p such that the residue field $R/\mathfrak{p}$ is a finite field of characteristic p so that $p\mathbb{Z} \subset \mathfrak{p}$. Let $d_\mathfrak{p}$ be the degree of the field extension $R/\mathfrak{p}$ over $\mathbb{F}_p$. Since g_i belongs to $\mathcal{L}_d$, there exists a polynomial $A_i \in \mathbb{Z}[\mathbf{x}]$ such that

$$g_i(\mathbf{x}) \equiv A_i(\mathbf{x}) g_i(\mathbf{x}^{p^{k_i}}) \mod \mathfrak{p}[[\mathbf{x}]]$$

with $\deg_{x_j} A_i \leq p^{k_i} - 1$. We set $k := \operatorname{lcm}(d_\mathfrak{p}, k_1, \dots, k_n)$. Then iterating the above relation, for all i in $\{1, \dots, n\}$ and all $\mathfrak{p}$ in $\mathcal{S}$, there exists $B_i(\mathbf{x})$ in $\mathbb{Z}[\mathbf{x}]$ satisfying

$$g_i(\mathbf{x}) \equiv B_i(\mathbf{x}) g_i\big(\mathbf{x}^{p^k}\big) \mod \mathfrak{p}[[\mathbf{x}]], \tag{4.1}$$

with $\deg_{x_j}(B_i) \leq p^k - 1$.

Now let us assume by contradiction that $f_1, \dots, f_n$ are algebraically dependent over $\mathbb{C}(\mathbf{x})$ and thus over $K(\mathbf{x})$ for the coefficients of the formal power series f_i belong to K (see for instance [2]). Let $Q(\mathbf{x}, y_1, \dots, y_n)$ be a nonzero polynomial in $R[\mathbf{x}][y_1, \dots, y_n]$ of total degree at most κ in $y_1, \dots, y_n$ such that $Q\big(\mathbf{x}, f_1(q;\mathbf{x}), \dots, f_n(q;\mathbf{x})\big) = 0$. Since $f_i \in \mathcal{D}(q; g_i)$, for every i in $\{1, \dots, n\}$, Proposition 4.2 implies that $f_i(q;\mathbf{x}) \equiv A_i(q;\mathbf{x}) g_i(\mathbf{x}^b)$ mod $\mathfrak{p}R_\mathfrak{p}[[\mathbf{x}]]$, for some prime b. Since Q and the series f_i are all nonzero and R is a Dedekind domain, there thus exists an infinite subset $\mathcal{S}'$ of $\mathcal{S}$ such that, for every $\mathfrak{p}$ in S', the relation

$$Q\big(\mathbf{x}, A_1(q;\mathbf{x}) g_1(\mathbf{x}^b), \dots, A_n(q;\mathbf{x}) g_n(\mathbf{x}^b)\big) \equiv 0 \mod \mathfrak{p}R_\mathfrak{p}[[\mathbf{x}]]$$

provides a nontrivial algebraic relation over $R_\mathfrak{p}/\mathfrak{p} = R/\mathfrak{p}$ between the series $g_{i|\mathfrak{p}}(\mathbf{x}^b)$. By (4.1), one has $g_i(\mathbf{x}^b) \equiv B_i(\mathbf{x}^b) g_i\big(\mathbf{x}^{bp^k}\big)$ mod $\mathfrak{p}[[\mathbf{x}]]$ and Proposition 4.1 then applies to $g_{1|\mathfrak{p}}(\mathbf{x}^b), \dots, g_{n|\mathfrak{p}}(\mathbf{x}^b)$ by taking $F = R/\mathfrak{p}$. There thus exist integers $m_1, \dots, m_n$, not all zero, and a nonzero rational fraction $r(\mathbf{x})$ in $F(\mathbf{x})$ such that

$$B_{1|\mathfrak{p}}(\mathbf{x}^b)^{m_1} \cdots B_{n|\mathfrak{p}}(\mathbf{x}^b)^{m_n} = r(\mathbf{x})^{p^k - 1}. \tag{4.2}$$

As g_i belongs to $\mathcal{L}_d$, the constant coefficient in the left-hand side of (4.2) is equal to 1. By Lemma 4.4, as $p^k - 1 \neq 0 \bmod p$, there exists a rational fraction $u(\mathbf{x})$ in $F(\mathbf{x})$ such that $r(\mathbf{x}) = u(\mathbf{x}^b)$ and we obtain that $B_{1|\mathfrak{p}}(\mathbf{x})^{m_1} \cdots B_{n|\mathfrak{p}}(\mathbf{x})^{m_n} = u(\mathbf{x})^{p^k-1}$. Furthermore, we have $|m_1 + \cdots + m_n| \leq \kappa$ and $|m_i| \leq \kappa$ for $1 \leq i \leq n$. Note that the rational fractions B_i, u and the integers m_i all depend on $\mathfrak{p}$. However, since all the integers m_i belong to a finite set, the pigeonhole principle implies the existence of an infinite subset $\mathcal{S}''$ of $\mathcal{S}'$ and of integers $t_1, \ldots, t_n$ such that, for all $\mathfrak{p}$ in $\mathcal{S}''$, we have $m_i = t_i$ for $1 \leq i \leq n$. We can thus assume that $\mathfrak{p}$ belongs to $\mathcal{S}''$ and write $u(\mathbf{x}) = s(\mathbf{x})/t(\mathbf{x})$ with $s(\mathbf{x})$ and $t(\mathbf{x})$ in $F[\mathbf{x}]$ and coprime. Since $\deg B_i \leq p^k - 1$, the degrees of $s(\mathbf{x})$ and $t(\mathbf{x})$ are bounded by $|t_1| + \cdots + |t_n| \leq n\kappa$. Set $h(\mathbf{x}) := g_1(\mathbf{x})^{-t_1} \cdots g_n(\mathbf{x})^{-t_n} \in \mathbb{Z}[[\mathbf{x}]] \subset R[[\mathbf{x}]]$. Then we obtain that

$$\begin{aligned} h_{|\mathfrak{p}}\left(\mathbf{x}^{p^k}\right) &= g_{1|\mathfrak{p}}\left(\mathbf{x}^{p^k}\right)^{-t_1} \cdots g_{n|\mathfrak{p}}\left(\mathbf{x}^{p^k}\right)^{-t_n} \\ &= g_{1|\mathfrak{p}}(\mathbf{x})^{-t_1} \cdots g_{n|\mathfrak{p}}(\mathbf{x})^{-t_n} B_{1|\mathfrak{p}}(\mathbf{x})^{t_1} \cdots B_{n|\mathfrak{p}}(\mathbf{x})^{t_n} \\ &= h_{|\mathfrak{p}}(\mathbf{x}) u(\mathbf{x})^{p^k-1}. \end{aligned}$$

Since $h_{|\mathfrak{p}}$ is nonzero, we obtain that $h|_{\mathfrak{p}}(\mathbf{x})^{p^k-1} = u(\mathbf{x})^{p^k-1}$ and there exists a in a suitable algebraic extension of F such that $h_{|\mathfrak{p}}(\mathbf{x}) = a u(\mathbf{x})$. As the coefficients of $h_{|\mathfrak{p}}$ and u belong to $R/\mathfrak{p}$, we get $a \in R/\mathfrak{p}$. Thus for infinitely many maximal ideals $\mathfrak{p}$, the reduction modulo $\mathfrak{p}$ of the power series $x_i^m h(\mathbf{x})$ and x_i^m, $1 \leq i \leq n$, $0 \leq m \leq n\kappa$, are linearly dependent over $R/\mathfrak{p}$. Since R is a Dedekind domain, Lemma 4.3 implies that these power series are linearly dependent over K, which means that $h(\mathbf{x})$ belongs to $K(\mathbf{x})$. This is a contradiction as $g_1, \ldots, g_n$ are algebraically independent over $\mathbb{C}(\mathbf{x})$. □

Acknowledgements

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 648132.

References

[1] B. Adamczewski and J. P. Bell. "Diagonalization and rationalization of algebraic Laurent series". *Ann. Sci. Éc. Norm. Supér.* **46** (2013), pp. 963–1004. DOI.

[2] B. Adamczewski, J. P. Bell, and E. Delaygue. "Algebraic independence of G-functions and congruences "à la Lucas"". 2016. arXiv:1603.04187.

[3] F. Beukers and G. Heckman. "Monodromy for the hypergeometric functions ${}_nF_{n-1}$". *Invent. Math.* **95** (1989), pp. 325–354. DOI.

[4] M. Bousquet-Mélou. “Rational and algebraic series in combinatorial enumeration”. *International Congress of Mathematicians, Vol. 3*. Eur. Math. Soc., 2006, pp. 789–826.

[5] E. Delaygue. “Arithmetic properties of Apéry-like numbers”. 2013. arXiv:1310.4131.

[6] P. Flajolet. “Analytic models and ambiguity of context-free languages”. *Theor. Comput. Sci* **49** (1987), pp. 283–309. DOI.

[7] R. D. Fray. “Congruence properties of ordinary and q-binomial coefficients”. *Duke Math. J.* **34** (1967), pp. 467–480. DOI.

[8] V. J. W. Guo and J. Zeng. “Some congruences involving central q-binomial coefficients”. *Adv. Appl. Math.* **45** (2010), pp. 303–316. DOI.

[9] E. Lucas. “Sur les congruences des nombres eulériens et les coefficients différentiels des fonctions trigonométriques, suivant un module premier”. *Bull. Soc. Math. France* **6** (1877–1878), pp. 49–54. DOI.

[10] H. Pan. “A Lucas-type congruence for q-Delannoy numbers”. 2015. arXiv:1508.02046.

[11] B. E. Sagan. “Congruence properties of q-analogs”. *Adv. Math.* **95** (1992), pp. 127–143. DOI.

[12] H. Sharif and C. F. Woodcock. “On the transcendence of certain series”. *J. Algebra* **121** (1989), pp. 364–369. DOI.

[13] R. P. Stanley. “Differentiably finite power series”. *European J. Combin.* **1** (1980), pp. 175–188. DOI.

[14] V. Strehl. “Zum q-Analogon der Kongruenz von Lucas”. *Séminaire Lotharingien de Combinatoire, 5-iéme Session*. Institut de Recherche Mathématique Avancée, 1982, pp. 102–104.

[15] S. O. Warnaar and W. Zudilin. “A q-rious positivity”. *Aeq. Math.* **81** (2011), pp. 177–183. DOI.