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.
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 $n \geq 0, r \geq 1$. 
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.**

\[
\binom{2(pn + m)}{pn + m} \equiv \binom{2m}{m} \binom{2n}{n} \mod p,
\]

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

**Definition**

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

\[
a(pn + m) \equiv a(m) a(n) \mod p \quad \text{for all} \quad m \in \{0, \ldots, p - 1\}^d.
\]
Other examples

Binomial coefficients \( \binom{n}{k}, \binom{2n}{n} \).
Other examples

Binomial coefficients \( \binom{n}{k}, \binom{2n}{n} \)

Factorial ratios \( \frac{(10n)!}{(5n)!(3n)!n!^2} \)
Other examples

Binomial coefficients \( \binom{n}{k}, \binom{2n}{n} \)

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

Apéry sequences \( \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 \)
Other examples

Binomial coefficients \( \binom{n}{k}, \binom{2n}{n} \)

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

Apéry sequences \( \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 \)

Franel numbers \( \sum_{k=0}^{n} \binom{n}{k}^3 \)
Other examples

Binomial coefficients \( \binom{n}{k}, \binom{2n}{n} \)

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

Apéry sequences \( \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 \)

Franel numbers \( \sum_{k=0}^{n} \binom{n}{k}^3 \)

Or \( \sum_{k=0}^{\lfloor n/3 \rfloor} 2^k 3^{\frac{n-3k}{2}} \binom{n}{k} \binom{n-k}{\frac{n-k}{2}} \binom{\frac{n-k}{2}}{k} \).
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.
Define \( g_r(x) := \sum_{n=0}^{\infty} \binom{2n}{n}^r x^n \). Then we have

\[
g_r(x) \equiv \sum_{m=0}^{p-1} \sum_{n=0}^{\infty} \binom{2m}{m}^r \binom{2n}{n}^r x^{pn+m} \mod p\mathbb{Z}[[x]]
\]

\[
\equiv \left( \sum_{m=0}^{p-1} \binom{2m}{m}^r x^m \right) g_r(x^p) \mod p\mathbb{Z}[[x]].
\]
A generating series approach

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

$$g_r(x) \equiv \sum_{m=0}^{p-1} \sum_{n=0}^{\infty} \binom{2m}{m} \binom{2n}{n} x^{pn+m} \mod p\mathbb{Z}[[x]]$$

$$\equiv \left(\sum_{m=0}^{p-1} \binom{2m}{m} x^m\right) g_r(x^p) \mod p\mathbb{Z}[[x]].$$

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 $p - 1$. 
A generating series approach

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

\[
g_r(x) \equiv p^{r-1} \sum_{m=0}^{p-1} \sum_{n=0}^{\infty} \binom{2m}{m}^r \binom{2n}{n}^r x^{pn+m} \mod p\mathbb{Z}[[x]]
\]

\[
\equiv \left( \sum_{m=0}^{p-1} \binom{2m}{m}^r x^m \right) g_r(x^p) \mod p\mathbb{Z}[[x]].
\]

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 \( p \).
Furstenberg (1967) and Deligne (1983) proved that the diagonal of a multivariate algebraic power series $f(x) \in \mathbb{Q}[[x]]$ is algebraic modulo $p$ for almost all prime numbers $p$. Adamczewski–Bell (2013) proved that when $f(x) \in \mathbb{Z}[[x]]$ the reductions modulo $p$ of such diagonals satisfy an Ore equation of an order $r$ independent of $p$: there exist $A_i(x) \in \mathbb{F}_p[x]$ such that

$$A_0(x) \Delta(f) |_p(x) + A_1(x) \Delta(f) |_p(x) + \cdots + A_r(x) \Delta(f) |_p(x)^p = 0.$$ 

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 $p$. Jouhet (ICJ, Lyon 1) Congruences modulo cyclotomic polynomials and algebraic independence for $q$-series Séminaire Flajolet, 2018 6 / 23
Motivations

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

Adamczewski–Bell (2013) proved that when $f(x) \in \mathbb{Z}[[x]]$ 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

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

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

Adamczewski–Bell (2013) proved that when \( f(x) \in \mathbb{Z}[[x]] \) 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.
Motivations

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

Adamczewski–Bell (2013) proved that when $f(x) \in \mathbb{Z}[[x]]$ 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

$$A_0(x)\Delta(f)(x) + A_1(x)\Delta(f)(x) + \cdots + A_r(x)\Delta(f)(x) = 0.$$ 

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 $p$. 
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

$$\left[ \begin{array}{c} n \\ k \end{array} \right]_q := \frac{[n]_q!}{[n-k]_q! [k]_q!} \in \mathbb{N}[q].$$
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

$$\binom{n}{k}_q := \frac{[n]_q!}{[n-k]_q![k]_q!} \in \mathbb{N}[q].$$

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

$$\phi_b(q) := \prod_{0 \leq k < b-1 \atop (k,b) = 1} \left( q - e^{2ik\pi/b} \right).$$
Extension of the $p$-Lucas property

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

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

**Definition**

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

$$a_q(bn + m) \equiv a_q(m) a_1(n) \mod \phi_b(q)\mathbb{Z}[q]$$

for all $m \in \{0, \ldots, b - 1\}$.

**Remark.** If $(a_q(n))_{n \in \mathbb{N}}$ is $\phi_b(q)$-Lucas for all $b$, then $(a_1(n))_{n \in \mathbb{N}}$ is $p$-Lucas for all primes $p$. This comes from $\phi_p(1) = p$. 
Extension of the $p$-Lucas property

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

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

Definition

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

$$a_q(bn + m) \equiv a_q(m) a_1(n) \mod \phi_b(q)\mathbb{Z}[q] \quad \text{for all} \quad m \in \{0, \ldots, b - 1\}^d.$$
Extension of the $p$-Lucas property

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

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

**Definition**

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

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

**Remark.** If $(a_q(n))_{n \in \mathbb{N}^d}$ is $\phi_b$-Lucas for all $b$, then $(a_1(n))_{n \in \mathbb{N}^d}$ 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):

\[
\begin{bmatrix} 2(m + nb) \end{bmatrix}_{q}^{r} \equiv \begin{bmatrix} 2m \end{bmatrix}_{q}^{r} \begin{bmatrix} 2n \end{bmatrix}_{q}^{r} \mod \phi_{b}(q)\mathbb{Z}[q],
\]

where \( n, m, b, r \) are nonnegative integers with \( b, r \geq 1 \) and \( 0 \leq m \leq b - 1 \).
Another example

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

\[
\left[ \frac{2(m + nb)}{m + nb} \right]_q^r = \left[ \frac{2m}{m} \right]_q^r \left( \frac{2n}{n} \right)^r \mod \phi_b(q) \mathbb{Z}[q],
\]

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

\[
f_r(q; x) := \sum_{n=0}^{\infty} \left[ \frac{2n}{n} \right]_q^r x^n, \quad g_r(x) = f_r(1; x).
\]
Given \(d\)-tuples of positive integers \(e_1, \ldots, e_u\) and \(f_1, \ldots, f_v\), set:

\[
Q(q; n) = Q_{e,f}(q; n) := \frac{[e_1 \cdot n]_q! \cdots [e_u \cdot n]_q!}{[f_1 \cdot n]_q! \cdots [f_v \cdot n]_q!}
\]

for \(n \in \mathbb{N}^d\).

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

\[
\Delta(x) = \Delta_{e,f}(x) := \sum_{i=1}^{u} [e_i \cdot x] - \sum_{j=1}^{v} [f_j \cdot x].
\]

We assume that \(\sum_{i=1}^{u} e_i = \sum_{j=1}^{v} f_j\), denoted \(|e| = |f|\). Therefore \(\Delta\) is \(1\)-periodic in all directions.
Define

\[ D := \{ x \in [0, 1)^d : \text{there exists } i \text{ such that } e_i \cdot x \geq 1 \text{ or } f_i \cdot x \geq 1 \} . \]

Proposition (ABDJ, 2017)

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

\[ Q(q; bn + m) \equiv Q(q; m) Q(1; n) \mod \phi_b(q)\mathbb{Z}[q]. \]
Tools for the proof

We have

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

and so

\[
Q(q; n) = \prod_{b=2}^\infty \phi_b(q)^{\Delta(n/b)}.
\]
Tools for the proof

We have

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

and so

\[ Q(q; n) = \prod_{b=2}^{\infty} \phi_b(q)^{\Delta(n/b)}. \]

Thus

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

\[ Q(q; n) \equiv 0 \mod \phi_b(q)\mathbb{Z}[q] \iff \Delta(n/b) \geq 1. \]
Tools for the proof

We have

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

and so

\[
Q(q; n) = \prod_{b=2}^{\infty} \phi_b(q)^{\Delta(n/b)}.
\]

Thus

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

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

\[
A(q) \equiv B(q) \mod \phi_b(q)\mathbb{Z}[q] \iff A(\xi) = B(\xi) \ \forall \ \xi \ \text{primitive} \ b\text{-th root of } 1.
\]
Example

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

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

We have

$$Q(q; n) = \frac{[2n]_q!^r}{[n]_q!^2}$$

and

$$\Delta(x) = r([2x] - 2[x]).$$

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

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

mod $\phi_b(q) \mathbb{Z}[q]$. 
Functional approach

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

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

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

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

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

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

**Proposition (specialization, ABDJ, 2017)**

Let $t \in \mathbb{N}^d$ and $m \in \mathbb{N}^d$ be such that if $x$ in $[0, 1]^d$ satisfies $m \cdot x \geq 1$, then $\Delta(x) \geq 1$. 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 $\phi_b$-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 $e_1, e_2 = (2; 1); f_1, \ldots, f_4 = (1; 0); f_5, f_6 = (0; 1)$, and

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

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

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

\( \Delta(x, y) = 2[2x + y] \geq 1 \) 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

\[ F(q; x, x) = \sum_{n=0}^{\infty} \left( \sum_{k=0}^{n} \binom{n}{k}_q \binom{n+k}{k}_q \right) x^n, \]

we derive that \( \sum_{k=0}^{n} \binom{n}{k}_q \binom{n+k}{k}_q \) is \( \phi_b \)-Lucas.
Recall that the multivariate power series \( f_1(x), \ldots, f_n(x) \) are algebraically dependent over \( \mathbb{C}(x) \) if there exists a non-zero polynomial \( P(Y_1, \ldots, Y_n) \) in \( \mathbb{C}[x][Y_1, \ldots, Y_n] \) such that \( P(f_1, \ldots, f_n) = 0 \). Otherwise they are algebraically independent over \( \mathbb{C}(x) \).
An algebraic independence result

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

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

Jouhet (ICJ, Lyon 1)

Congruences modulo cyclotomic polynomials  

Séminaire Flajolet, 2018 16 / 23
Recall that the multivariate power series $f_1(x), \ldots, f_n(x)$ are algebraically dependent over $\mathbb{C}(x)$ if there exists a non-zero polynomial $P(Y_1, \ldots, Y_n)$ in $\mathbb{C}[x][Y_1, \ldots, Y_n]$ such that $P(f_1, \ldots, f_n) = 0$. Otherwise they are algebraically independent over $\mathbb{C}(x)$.

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

$$f_1(x)^{a_1} \cdots f_r(x)^{a_r} \in \mathbb{Q}(x).$$
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 \( \mathbb{C}(x) \).
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.
Theorem (ABDJ, 2017)

Let \( q \neq 0 \) be a complex number. Assume that for \( 1 \leq i \leq n \), the coefficients of the series \( f_i(q; x) \in \mathbb{Z}[q][[x]] \) are \( \phi_b \)-Lucas for all positive integers \( b \). If the series \( f_1(1; x), \ldots, f_n(1; x) \) are algebraically independent over \( \mathbb{C}(x) \), then their \( q \)-analogues \( f_1(q; x), \ldots, f_n(q; x) \) are also algebraically independent over \( \mathbb{C}(x) \).
Theorem (ABDJ, 2017)

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

Corollary (ABDJ, 2017)

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


Corollary 2 (ABDJ, 2017)

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

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

and

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

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 $f_1, \ldots, f_n$ whose coefficients belong to a finite extension of $\mathbb{F}_p$ of degree $d_p$ and which satisfy $f_i(x) = A_i(x)f_i(x^{p^k})$ for some $A_i \in F[x]$, where $k \mid d_p$ is a fixed positive integer.

- A property extending the linear dependence over $R/p$ of the series $f_1|_p, \ldots, f_n|_p$ to the linear dependence of the series $f_1, \ldots, f_n$ over the field of fractions of $R$, where $R$ is a domain and $p$ belongs to a set $S$ 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.
Proposition (ABDJ, 2017)

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

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

and such that, for all $p$ in $S$, we have $\phi_{b_p}(q)\mathbb{Z}[q] \subset p$ for some number $b_p$ (depending on $p$).
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 $S$ of maximal ideals of $R = \mathbb{Z}[q]$ of finite index satisfying

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

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

**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 $p_n = (p_n, \phi_{b_n}(x))$, where $(p_n)_n$ and $(b_n)_n$ are both increasing sequences of prime numbers.
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 $S$ of maximal ideals of $R$ of finite index satisfying (1) and such that, for all $p \in S$, we have $\mathbb{Z}[q] \subset R_p$ and $\phi_{b_p}(q)\mathbb{Z}[q] \subset pR_p$ for some number $b_p$ (depending on $p$).
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 $S$ of maximal ideals of $R$ of finite index satisfying (1) and such that, for all $p \in S$, we have $\mathbb{Z}[q] \subset R_p$ and $\phi_{b_p}(q)\mathbb{Z}[q] \subset pR_p$ for some number $b_p$ (depending on $p$).

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

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

We thus only need to prove the existence of an infinite set $S$ 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

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

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

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 $\phi_n(x^p)$. As $\phi_n(x)$ only has simple roots:

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

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

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 $\phi_n(x^p)$. As $\phi_n(x)$ only has simple roots:

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

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

\[
\phi_{np}(x) = \frac{\phi_n(x^p)}{\phi_n(x)}.
\]

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 \( \phi_n(x^p) \). As \( \phi_n(x) \) only has simple roots:

\[
\phi_{np}(q) = \frac{pq^{p-1}\phi'_n(q^p)}{\phi'_n(q)} = p.
\]

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

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