Congruences modulo des polynômes cyclotomiques et indépendance algébrique

Travaux communs avec J. Bell, É. Delaygue et F. Jouhet

Boris Adamczewski

CNRS, Institut Camille Jordan, Lyon
Funded by the ERC consolidator grant Automata in Number Theory

Un théorème d'Édouard Lucas

Théorème (Lucas, 1878)

Pour tout couple d'entiers (n, k) et tout nombre premier p, on a :

$$\binom{n}{k} \equiv \prod_{i=1}^{r} \binom{n_i}{k_i} \bmod p\,,$$

où $n = \sum_{i=1}^{r} n_i p^i$ et $k = \sum_{i=1}^{r} k_i p^i$.

Preuve. On considère l'identité :

$$(1+x)^{pn+i} \equiv (1+x^p)^n (1+x)^i \bmod p\,.$$

En identifiant le coefficient de degré $pk+j$, on obtient la congruence de Lucas :

$$\binom{pn+i}{pk+j} \equiv \binom{n}{k}\binom{i}{j} \bmod p\,,$$

pour n, k, i, j entiers avec i, j dans $\{0, 1, \ldots, p-1\}$.

Il suffit ensuite d'itérer cette congruence. □

La propriété p-Lucas

Définition

Une suite $(a(\mathbf{n}))_{\mathbf{n}\in\mathbb{N}^d}$ à valeurs entières satisfait à la propriété p-Lucas si

$$a(p\mathbf{n}+\mathbf{i}) \equiv a(\mathbf{n})a(\mathbf{i}) \bmod p \qquad \forall p \text{ premier.}$$

Exemples. Les coefficients binomiaux $\binom{n}{k}$, les puissances de coefficients binomiaux centraux $\binom{2n}{n}^r$, les quotients de factorielles

$$\frac{(10n)!}{(5n)!(3n)!n!^2},$$

la suite hypergéométrique

$$\frac{(1/2)_n^2}{(2/3)_n n!}, \quad \text{où } (x)_n := x(x+1)\cdots(x+n-1).$$

Les suites d'Apéry $\sum_{k=0}^n \binom{n}{k}^2\binom{n+k}{k}^2$, de Franel $\sum_{k=0}^n \binom{n}{k}^3$, ou encore

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

Objectifs

Dans cette exposé, nous abordons les problèmes suivants.

- Chercher une explication conceptuelle à l'omniprésence de ces congruences.
- Obtenir un résultat général permettant de retrouver toutes ces congruences et de les généraliser aux cas de congruences modulo des polynômes cyclotomiques.
- Obtenir des résultats d'indépendance algébrique pour les séries génératrices associées à de telles suites.

Diagonales de fractions rationnelles

Définition

La diagonale d'une série formelle $f(\mathbf{x}) := \sum_{\mathbf{n}\in\mathbb{N}^d} a(\mathbf{n})\mathbf{x}^{\mathbf{n}}$ *est définie par*

$$\Delta(f)(x) := \sum_{n=0}^{\infty} a(n, n, \ldots, n)x^n.$$

Exemples. On a

$$\sum_{n=0}^{\infty} \binom{2n}{n}^2 x^n = \frac{2}{\pi}\int_0^{\pi/2} \frac{d\theta}{\sqrt{1-16x\sin^2\theta}} = \Delta\left(\frac{1}{1-(x_1+x_2)}\cdot\frac{1}{1-(x_3+x_4)}\right)$$

et

$$\sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\binom{n}{k}^2\binom{n+k}{k}^2\right)x^n = \Delta\left(\frac{1}{1-(x_1+x_2)(1-x_3-x_4)-x_1x_2x_3x_4}\right)$$

Conjecture (Christol)

Toute série dans $\mathbb{Z}[x]$*, différentiellement finie et ayant un rayon de convergence non nul est la diagonale d'une fraction rationnelle.*

Diagonales modulo p et propriété p-Lucas

Théorème (Furstenberg–Deligne)

La diagonale d'une série formelle algébrique $f(\mathbf{x}) := \sum_{\mathbf{n}\in\mathbb{N}^d} a(\mathbf{n})\mathbf{x}^{\mathbf{n}} \in \mathbb{Q}[[\mathbf{x}]]$ *est algébrique modulo* p *pour presque tout nombre premier* p.

Plus précisément, on peut montrer que

Théorème (AB)

La réduction $\Delta(f)_{|p}$ *satisfait à une équation d'Ore d'ordre* r *:*

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

avec $A_i(x) \in \mathbb{F}_p[x]$ *et où* r *ne dépend pas de* p.

Point de vue fonctionnel. La suite $a(\mathbf{n})$ satisfait à la propriété p-Lucas si, et seulement si, la série génératrice $f(\mathbf{x}) = \sum a(\mathbf{n})\mathbf{x}^{\mathbf{n}}$ vérifie l'équation :

$$f(\mathbf{x}) \equiv A(\mathbf{x})f(\mathbf{x})^p \bmod p\ ,$$

où $A(\mathbf{x})$ est un polynôme de degré au plus $p-1$ en chaque variable.

Une généralisation de la propriété p-Lucas

Soit q un nombre complexe. On définit classiquement le q-analogue d'un entier n par

$$[n]_q := \frac{1-q^n}{1-q} \quad \text{de sorte que} \quad [n!]_q := \prod_{i=1}^{n} \frac{1-q^i}{1-q} \quad \text{et} \quad \begin{bmatrix} n \\ k \end{bmatrix}_q := \frac{[n!]_q}{[(n-k)!]_q [k!]_q}.$$

En 1967, Fray a montré que la suite $\begin{bmatrix} n \\ k \end{bmatrix}_q$ satisfait à la congruence suivante :

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

où $b \geq 1$, ϕ_b désigne le b-ième polynôme cyclotomique et $0 \leq i, j \leq b-1$.

Remarque. En spécialisant en $b = p$ et $q = 1$, on retrouve la congruence de Lucas.

Définition

Une suite $(a(q;\mathbf{n}))_{\mathbf{n}\in\mathbb{N}^d}$ à valeurs dans $\mathbb{Z}[q]$ satisfait à la propriété ϕ_b-Lucas si

$$a(q; b\mathbf{n}+\mathbf{i}) \equiv a(1;\mathbf{n})a(q;\mathbf{i}) \bmod \phi_b(q)\mathbb{Z}[q]$$

q-Analogues et quotients de factorielles

Étant donnés des d-uplets d'entiers positifs $\mathbf{e}_1, \ldots, \mathbf{e}_u$ et $\mathbf{f}_1, \ldots, \mathbf{f}_v$, on pose :

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

On définit alors la fonction de Landau $\Delta_{e,f}$ par :

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

On ne considère dans la suite que le cas où $\sum_{i=1}^{u} \mathbf{e}_i = \sum_{j=1}^{v} \mathbf{f}_j$, que l'on notera simplement $|e| = |f|$. La fonction $\Delta_{e,f}$ est donc 1-périodique dans toutes les directions.

On pose :

$$\mathcal{D}_{e,f} := \left\{ \mathbf{x} \in [0,1)^d \ : \text{ il existe } i \text{ tel que } \mathbf{e}_i \cdot \mathbf{x} \geq 1 \text{ ou } \mathbf{f}_i \cdot \mathbf{x} \geq 1 \right\} .$$

Proposition (ABDJ)

Si $\Delta_{e,f} \geq 0$, alors $\mathcal{Q}_{e,f}(q; \mathbf{n}) \in \mathbb{Z}[q]$.

Si $\Delta_{e,f} \geq 1$ sur l'ensemble $\mathcal{D}_{e,f}$, alors $\mathcal{Q}_{e,f}(q; n)$ a la propriété ϕ_b-Lucas.

Lien avec la fonction de Landau. On a

$$\frac{1-q^n}{1-q} = \prod_{b\geq 2,\, b|n} \phi_b(q)\,,$$

de sorte que

$$[n!]_q = \prod_{b=2}^{n} \phi_b(q)^{\lfloor n/b \rfloor}$$

et donc

$$\mathcal{Q}_{e,f}(q;\mathbf{n}) = \prod_{b=2}^{\infty} \phi_b(q)^{\Delta_{e,f}(\mathbf{n}/b)}\,.$$

Ainsi

$$\mathcal{Q}_{e,f}(q;\mathbf{n}) \in \mathbb{Z}[q] \iff \Delta_{e,f} \geq 0$$

et

$$\mathcal{Q}_{e,f}(q;\mathbf{n}) \equiv 0 \bmod \phi_b(q) \iff \Delta_{e,f}(\mathbf{n}/b) \geq 1\,.$$

Remarques préliminaires

Étant donnés deux polynômes $A(q)$ et $B(q)$, montrer la congruence

$$A(q) \equiv B(q) \bmod \phi_b(q)\mathbb{Z}[q]\,,$$

revient à prouver l'égalité

$$A(\xi) = B(\xi)$$

pour toute une racine primitive b-ième de l'unité ξ.

Comme $[n!]_q = \prod_{i=1}^{n} \frac{1-q^i}{1-q}$, nous allons nous ramener à l'étude de quotients de la forme

$$\frac{1-\xi^{ib+\ell}}{1-\xi^{jb+\ell}}\,.$$

La démonstration repose alors sur l'observation suivante. Pour tout entier $1 \leq \ell < b$, on a :

$$\frac{1-\xi^{ib+\ell}}{1-\xi^{jb+\ell}} = 1\,,$$

tandis qu'il découle de la règle de l'Hôpital que

$$\lim_{q\to\xi} \frac{1-q^{ib}}{1-q^{jb}} = \frac{i}{j}\,.$$

Démonstration

On écrira $\mathcal{Q}$ pour $\mathcal{Q}_{e,f}$, Δ pour $\Delta_{e,f}$ et $\mathcal{D}$ pour $\mathcal{D}_{e,f}$.

Comme $|e| = |f|$, on obtient

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

On distingue alors deux cas.

1. Si $\mathbf{a}/b \notin \mathcal{D}$, alors par définition aucun élément de $\{1, \ldots, \mathbf{e_i} \cdot \mathbf{a}\}$ ou $\{1, \ldots, \mathbf{f_j} \cdot \mathbf{a}\}$ n'est divisible par b.

Ainsi

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

pour toute racine primitive de b-ième de l'unité ξ, de sorte que

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

2. Si $\mathbf{a}/b \in \mathcal{D}$, on a par hypothèse que $\Delta(\mathbf{a}/b) \geq 1$.
Comme

$$\mathcal{Q}_{e,f}(q;\mathbf{n}) \equiv 0 \bmod \phi_b(q) \iff \Delta_{e,f}(\mathbf{n}/b) \geq 1$$

et que $\Delta(\frac{\mathbf{a}}{b} + \mathbf{n}) = \Delta(\mathbf{a}/b) \geq 1$, on obtient que les deux polynômes $\mathcal{Q}(q;\mathbf{a})$ et $\mathcal{Q}(q;\mathbf{a}+\mathbf{n}b)$ sont divibles par $\phi_b(q)$.

Ainsi, la congruence

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

est triviale.

Démonstration

Il reste à montrer que

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

On a

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

et comme par hypothèse $|e| = |f|$:

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

En utilisant à nouveau que $|e| = |f|$, il vient :

$$\mathcal{Q}(\xi;\mathbf{n}b) = \frac{\prod_{i=1}^{u}\prod_{k=1}^{\mathbf{e}_i\cdot\mathbf{n}}\left(\lim_{q\to\xi}\frac{1-q^{kb}}{1-q^{b}}\right)}{\prod_{j=1}^{v}\prod_{k=1}^{\mathbf{f}_j\cdot\mathbf{n}}\left(\lim_{q\to\xi}\frac{1-q^{kb}}{1-q^{b}}\right)} = \mathcal{Q}(1;\mathbf{n})\,.$$

□

Posons

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

La propriété ϕ_b-Lucas est alors équivalente à :

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

pour tout entier b, où $A(q;\mathbf{x})$ est un polynôme de degré $\leq b-1$ en chaque variable.

On obtient alors le résultat suivant.

Proposition (ABDJ)

Si $\Delta_{e,f} \geq 1$ sur l'ensemble $\mathcal{D}_{e,f}$, alors la série $F_{e,f}(q;x,x,\ldots,x)$ a également la propriété ϕ_b-Lucas.

Un exemple

Considérons la série

$$F_{e,f}(q; x_1, x_2) := \sum_{n_1, n_2 \geq 0} \frac{[2n_1 + n_2]_q^2!}{[n_1]_q!^4 [n_2]_q!^2} x_1^{n_1} x_2^{n_2} .$$

On a trivialement que $\Delta_{e,f} \geq 1$ sur $\mathcal{D}_{e,f}$.

Comme

$$F_{e,f}(q; x, x) = \sum_{n=1}^{\infty} \left(\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q^2 \begin{bmatrix} n+k \\ k \end{bmatrix}_q^2 \right) x^n ,$$

on en déduit que la suite

$$\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q^2 \begin{bmatrix} n+k \\ k \end{bmatrix}_q^2$$

a la propriété ϕ_b-Lucas et, en choisissant $q = 1$ et $b = p$, que la suite d'Apéry

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

a la propriété p-Lucas.

Transcendance de séries génératrices : un exemple classique

Pour tout entier $r \geq 1$, on pose

$$\mathfrak{f}_r(x) := \sum_{n=0}^{\infty} \binom{2n}{n}^r x^n .$$

En 1980, Stanley a conjecturé que les séries $\mathfrak{f}_r$ sont toutes transcendantes sur $\mathbb{C}(x)$ sauf si $r = 1$, auquel cas $\mathfrak{f}_1(x) = 1/\sqrt{1-4x}$.

Stanley a aussi démontré le cas où r est pair en utilisant le comportement asymptotique de $\binom{2n}{n}^r$ (via la formule de Stirling).

Une réponse positive a finalement été apportée de façon indépendante par :

- Flajolet (1987) en utilisant plus finement cet asymptotique (et la transcendance de π).
- Sharif et Woodcock (1989) en utilisant la propriété p-Lucas.

Théorème (ABD)

Soient $f_1(x), \ldots, f_r(x)$ des séries dans $\mathbb{Q}[[x]]$ satifaisant à la propriété p-Lucas (pour une infinité de nombres premiers).
Ces séries sont algébriquement dépendantes sur $\mathbb{C}(x)$ si, et seulement si, il existe des entiers relatifs $a_1, \ldots, a_r$, non tous nuls, tels que

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

Corollaire

Les séries

$$\mathfrak{f}_r(x) := \sum_{n=0}^{\infty} \binom{2n}{n}^r x^n\,, \qquad r \geq 2$$

sont algébriquement indépendantes sur $\mathbb{C}(x)$.

Démonstration

Supposons par l'absurde que $\mathfrak{f}_2, \mathfrak{f}_3, \ldots, \mathfrak{f}_n$ sont algébriquement dépendantes. D'après le théorème, il existe $a_2, \ldots, a_n \in \mathbb{Z}$, non tous nuls, tels que

$$\mathfrak{f}_2(x)^{a_2} \cdots \mathfrak{f}_n(x)^{a_n} = r(x)\,,$$

avec $r(x) \in \mathbb{Q}(x)$.

Soit r le plus grand indice tel que $a_r \neq 0$. On obtient

$$\mathfrak{f}_r(z)^{a_r} = r(z)\mathfrak{f}_2(z)^{-a_2} \cdots \mathfrak{f}_{r-1}(z)^{-a_{r-1}}\,. \tag{1}$$

On peut supposer sans perte de généralité que $a_r > 1$.

La formule de Stirling implique que

$$\binom{2n}{n}^r \underset{n\to\infty}{\sim} \frac{2^{(2n+1/2)r}}{(2\pi n)^{r/2}}\,.$$

et donc le rayon de convergence de $\mathfrak{f}_i$ est égal à 2^{-2i}, de sorte que le membre de droite est méromorphe dans un voisinage de $z_0 := 2^{-2r}$.

D'autre part, $\mathfrak{f}_r^{a_r}$ a nécessairement une singularité en z_0, mais l'asymptotique implique que ce ne peut pas être un pôle. □

Un phénomène de propagation

Théorème (ABDJ)

Soit $q \neq 0$ dans $\mathbb{C}$. Soient $f_1(q;x), \ldots, f_r(q;x)$ des séries satisfaisant à la propriété ϕ_b-Lucas. Si les séries

$$f_1(1;x), \ldots, f_r(1;x)$$

sont algébriquement indépendantes sur $\mathbb{C}(x)$, alors les séries

$$f_1(q;x), \ldots, f_r(q;x)$$

le sont également.

Corollaire

Soit $q \neq 0$ dans $\mathbb{C}$. Les séries

$$\mathfrak{f}_r(q;x) := \sum_{n=0}^{\infty} \begin{bmatrix} 2n \\ n \end{bmatrix}_q^r x^n, \qquad r \geq 2$$

sont algébriquement indépendantes sur $\mathbb{C}(x)$.