TRIANGLE DE PASCAL, COMPLEXITÉ ET AUTOMATES

J.-P. Allouche et V. Berthé

1 Introduction

À quoi reconnaît-on qu'une suite est plus ou moins "compliquée" ? Une des traductions mathématiques de ce terme vague consiste à compter les facteurs ou blocs qui apparaissent dans cette suite, (voir par exemple [2]). Il y a naturellement bien d'autres approches possibles, qui dépendent en particulier à la fois des applications qu'on a à l'esprit ... et des quantités que l'on sait calculer ou estimer pour une suite donnée. La même question peut aussi se poser pour une suite à deux (ou plusieurs) indices et nous nous proposons, à travers le choix de la suite double des coefficients binomiaux réduits modulo un entier, de décrire quelques approches possibles.

Plus précisément, si l'on représente la suite double $\left(\binom{m}{n} \bmod d\right)_{m,n}$ en noircissant ou non les carrés élémentaires du réseau $\mathbb{Z}^2$ suivant que $\binom{m}{n} \bmod d$ est non nul ou nul – ou bien si l'on représente les différentes valeurs de $\binom{m}{n} \bmod d$ par des carrés de différentes couleurs – on a l'impression que le dessin obtenu est "plus compliqué" lorsque d n'est pas une puissance d'un nombre premier que quand c'est une puissance d'un nombre premier (et un petit peu plus compliqué quand cette puissance est strictement supérieure à un que lorsqu'elle vaut un).

Dans cet article, nous nous proposons de rappeler quelques propriétés de la suite double $\left(\binom{m}{n} \bmod d\right)_{m,n}$ en termes d'engendrement par automate cellulaire, de propriétés de "renormalisation" et d'engendrement par automate fini, puis nous calculons la complexité par blocs rectangulaires de cette suite. Nous prouvons en particulier *une formule explicite pour la complexité lorsque d est un nombre premier p*, avec une expression particulièrement simple dans le cas $p = 2$: *le nombre de blocs rectangulaires différents de taille $u \times v$ qui apparaissent dans la suite double $\left(\binom{m}{n} \bmod 2\right)_{m,n}$ est $P(u,v) = u^2 + v^2 + 2uv - 3u - 3v + 4$.* Nous montrons aussi que *le nombre de blocs rectangulaires différents de taille $u \times v$ qui apparaissent dans la suite double $\left(\binom{m}{n} \bmod d\right)_{m,n}$ vérifie :*

$$\exists A > 0,\ \exists B > 0,\ \forall u, v \geq 1,\ A \sup(u,v)^{2\omega(d)} \leq P(u,v) \leq B \sup(u,v)^{2\omega(d)},$$

où $\omega(d)$ est le nombre de facteurs premiers distincts de l'entier d.

Notons qu'on pourrait aussi mesurer la "complication" du triangle de Pascal réduit modulo d en évaluant des fréquences de blocs. Par exemple, il a été prouvé dans [5] que *les coefficients binomiaux (en fait les coefficients multinomiaux) non congrus à 0 modulo un nombre premier p sont équirépartis dans les classes résiduelles modulo p.*

2 Automates cellulaires et coefficients binomiaux

Cette section, fort brève, est juste destinée à rappeler la règle du triangle de Pascal :

$$\binom{m+1}{n+1} = \binom{m}{n+1} + \binom{m}{n}.$$

Naturellement cette règle reste vraie si on remplace les nombres ci-dessus par leurs réductions modulo d. Ce rappel montre donc que la suite double des coefficients binomiaux modulo d peut être obtenue comme l'évolution temporelle de l'automate cellulaire linéaire et à une dimension sur $\mathbb{Z}/d\mathbb{Z}$ défini par la condition initiale où une seule cellule vaut 1 et toutes les autres 0, et la règle de transition

$$x(n+1, t+1) = x(n, t+1) + x(n, t).$$

Nous ne dirons rien de plus sur le sujet, renvoyant – par exemple – à [3] pour plus de détails, car cet aspect des choses ne dépend clairement pas des propriétés de l'entier d. En revanche cette approche permet d'obtenir d'autres propriétés de la suite double des coefficients binomiaux modulo d qui sont abordées au paragraphe suivant.

3 "Renormalisation" du triangle de Pascal réduit modulo d

Lorsque nous parlions dans l'introduction des dessins obtenus à partir du triangle de Pascal modulo d, nous sous-entendions comme chacun l'aura compris, qu'il ne s'agit pas d'étudier une partie de cette suite double mais *toute* cette suite. Comme nous ne prétendons pas faire des dessins infinis, c'est donc que nous sous-entendions aussi, soit que le réseau $\mathbb{Z}^2$ est dessiné avec des pas "infiniment petits", soit que le dessin obtenu est transformé – et plusieurs fois – par une homothétie "bien choisie" de rapport strictement inférieur à un.

En d'autres termes on dessine la suite $\left(\binom{m}{n} \bmod d\right)_{m,n\leq N_j}$, puis on applique aux carrés obtenus une homothétie de rapport λ_j, obtenant ainsi un dessin D_j

et on se demande si, pour un choix convenable de la suite $(N_j)_j$ et de la suite $(\lambda_j)_j$, la suite $(D_j)_j$ tend vers une limite au sens de la distance de Hausdorff. Nous renvoyons le lecteur à [8], [9] et [10] où il est prouvé que : *si $d = p^e$, avec p premier, en prenant $N_j = p^{je} - 1$ et $\lambda_j = \frac{1}{p^{je}}$, la limite des D_j existe et a pour dimension fractale (pour plusieurs définitions d'une dimension fractale)* $\frac{\log \frac{p(p+1)}{2}}{\log p}$*, indépendante de e; si $d = 6$, par exemple, on peut trouver, en utilisant un théorème diophantien, une suite λ_j à la fois proche des puissances de 2 et des puissances de 3, telle que la limite correspondante des D_j soit la réunion ensembliste des limites modulo 2 et modulo 3 ci-dessus.*

4 Engendrement par automate fini

Considérons le morphisme bidimensionnel défini sur l'alphabet $\{0, 1\}$ par :

$$0 \longrightarrow \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix},$$

$$1 \longrightarrow \begin{matrix} 1 & 0 \\ 1 & 1 \end{matrix}.$$

En itérant ce morphisme à partir de 1, (à partir de 0 cela n'a guère d'intérêt comme le lecteur s'en convaincra aisément), on obtient :

$$1 \longrightarrow \begin{matrix} 1 & 0 \\ 1 & 1 \end{matrix} \longrightarrow \begin{matrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{matrix} \longrightarrow \begin{matrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{matrix} \longrightarrow \cdots$$

On reconnaît la suite double des coefficients du binôme modulo 2, (le dessin engendré est aussi connu sous le nom de tamis de Sierpiński, voir par exemple le récent survol [16]); dans la littérature les dénominations "tamis" et "tapis" (en anglais "gasket" et "carpet") décrivent le plus souvent respectivement l'objet ci-dessus et l'objet "carré" égal au produit cartésien de deux copies de l'ensemble de Cantor (classique).

La question qui se pose alors est : pour quelles valeurs de d la suite double des binomiaux modulo d peut-elle être engendrée par un procédé de ce type?

Rappelons qu'une suite double $(z(m, n))_{m,n}$, à valeurs dans un alphabet fini A, est dite k-automatique s'il existe un alphabet fini B, un morphisme σ qui associe à chaque élément de B un "carré" de côté k d'éléments de B et une application (littérale) φ de B dans A, tels que :

- il existe une suite double infinie $(y(m,n))_{m,n}$ point fixe du morphisme σ prolongé aux suites doubles infinies,

- l'on ait, pour tout m, n, la relation $z(m,n) = \varphi(y(m,n))$.

Pour ces notions et des applications en théorie des nombres le lecteur pourra se reporter aux travaux de Salon ([14], [15]). Le lecteur pourra aussi consulter le beau survol [6].

On peut maintenant donner la réponse à la question posée plus haut : *la suite double* $\left(\binom{m}{n} \bmod d\right)_{m,n}$ *est k-automatique si et seulement si d est une puissance d'un nombre premier p. La suite est alors p-automatique.*

Ce résultat est prouvé dans [3] et donne une autre différence de comportement de la suite $\left(\binom{m}{n} \bmod d\right)_{m,n}$ suivant que d est ou n'est pas une puissance d'un nombre premier.

Ce curieux comportement d'une suite double $(z(m,n) \bmod d)_{m,n}$ (être ou ne pas être automatique suivant que d est ou n'est pas une puissance d'un nombre premier) est d'ailleurs vrai pour d'autres suites "issues de la combinatoire" (voir par exemple [11]) et l'on peut essayer de trouver une famille aussi grosse que possible de telles suites : c'est l'objet d'une étude en cours par M. Bousquet-Mélou, E. Roblet et le premier auteur.

5 Complexité par blocs de la suite double des binomiaux modulo un entier naturel

Nous nous proposons d'étudier la suite double $\left(\binom{m}{n} \bmod d\right)_{m,n\geq 0}$ sous l'angle de la complexité (par blocs). Cette suite peut être définie sur $\mathbb{N} \times \mathbb{N}$ tout entier en posant comme d'habitude $\binom{m}{n} = 0$ si $m < n$.

Définition 5.1 *On note $P_d(u,v)$ le nombre de blocs à u lignes et v colonnes qui apparaissent dans la suite double $\left(\binom{m}{n} \bmod d\right)_{m,n}$. On note aussi par abus d'écriture $P_d(v) = P_d(1,v)$, c'est le nombre de "mots" (en ligne) qui apparaissent dans la suite double $\left(\binom{m}{n} \bmod d\right)_{m,n}$. La fonction $(u,v) \to P_d(u,v)$ est appelée complexité (par blocs) de la suite double, la fonction $v \to P_d(v) = P_d(1,v)$ est appelée complexité en ligne de la suite double.*

Notre étude comprend alors quatre parties. Nous donnons d'abord quelques lemmes techniques, montrant en particulier que la suite $\left(\binom{m}{n} \bmod d\right)_{m,n}$ est récurrente, c'est-à-dire que tout bloc y apparaît une infinité de fois. Puis nous

montrons comment $P_d(u,v)$ peut être calculé en connaissant uniquement $P_d(1,v)$. Un dernier lemme montre que la complexité est "multiplicative" en d, autrement dit que la complexité de la suite modulo $d_1 d_2$ est le produit des complexités modulo d_1 et modulo d_2 dès que d_1 et d_2 sont premiers entre eux. Une deuxième partie étudie le cas où d est un nombre premier, nous donnons dans ce cas des formules explicites pour la complexité. La troisième partie traite le cas où d est une puissance d'un nombre premier. Enfin la quatrième et dernière partie donne le cas général. Dans ces deux dernières parties, nous n'avons pas de formule exacte, mais seulement les ordres de grandeur des complexités.

5.1 Quelques lemmes généraux

Lemme 5.2 *Soit $p \geq 2$ un nombre premier. Soient $\alpha \geq 1$, $\lambda \geq 1$ et $\beta \geq 1$ des entiers fixés. Soit a un entier tel que $a \geq 1 + \frac{\beta}{\alpha}$. Alors,*

$$(1+X)^{\lambda p^{a\alpha}} = 1 + c(p,\alpha,\lambda,\beta,a)X^{p^\beta} + \cdots + c(p,\alpha,\lambda,\beta,a)X^{\lambda p^{a\alpha}-p^\beta} + X^{\lambda p^{a\alpha}} \bmod p^\alpha.$$

En d'autres termes les coefficients de X^j pour $0 < j < p^\beta$ et $\lambda p^{a\alpha} - p^\beta < j < \lambda p^{a\alpha}$ sont nuls modulo p^α.

Preuve. Notons $v_p(n)$ la valuation p-adique de l'entier n, c'est-à-dire la plus grande puissance de p qui divise n et notons $s_p(n)$ la somme des chiffres de n en base p. Il est bien connu que l'on a, quel que soit l'entier n, l'égalité $(p-1)v_p(n!) = n - s_p(n)$, d'où l'on déduit sans mal :

$$\forall x, y \in \mathbb{N} \setminus \{0\},\ y \leq x,\ (p-1)v_p\binom{x}{y} = s_p(y) + s_p(x-y) - s_p(x).$$

Comme on a $\binom{\lambda p^{a\alpha}}{j} = \binom{\lambda p^{a\alpha}}{\lambda p^{a\alpha}-j}$ pour tout $j \in [0, \lambda p^{a\alpha}]$, il suffit de prouver que l'on a :

$$\forall j \in [1, p^{\beta-1}-1],\ \binom{\lambda p^{a\alpha}}{j} = 0 \bmod p^\alpha.$$

On calcule donc pour un tel j :

$$\begin{aligned}
(p-1)v_p\tbinom{\lambda p^{a\alpha}}{j} &= s_p(j) + s_p(\lambda p^{a\alpha} - j) - s_p(\lambda p^{a\alpha}) \\
&= s_p(j) + s_p(p^\beta(\lambda p^{a\alpha-\beta} - 1) + p^\beta - j) - s_p(\lambda) \\
&= s_p(j) + s_p(\lambda p^{a\alpha-\beta} - 1) + s_p(p^\beta - j) - s_p(\lambda) \\
&= s_p(j) + s_p((\lambda-1)p^{a\alpha-\beta} + p^{a\alpha-\beta} - 1) + s_p(p^\beta - j) - s_p(\lambda) \\
&= s_p(j) + s_p(\lambda - 1) + s_p(p^{a\alpha-\beta} - 1) + s_p(p^\beta - j) - s_p(\lambda) \\
&= s_p(j) + s_p(\lambda - 1) + (a\alpha - \beta)(p-1) + s_p(p^\beta - j) - s_p(\lambda) \\
&\geq (a\alpha - \beta)(p-1) - 1.
\end{aligned}$$

Nous avons utilisé la minoration $s_p(\lambda-1)-s_p(\lambda)\geq -1$ qui se prouve sans difficulté, (voir par exemple une preuve et une utilisation dans [1]).

On déduit donc du calcul ci-dessus la minoration

$$v_p\binom{\lambda p^{a\alpha}}{j}\geq a\alpha-\beta-\frac{1}{p-1},$$

qui implique, puisque le terme de gauche est un entier,

$$v_p\binom{\lambda p^{a\alpha}}{j}\geq a\alpha-\beta.$$

Ainsi, avec le choix de a, on a

$$v_p\binom{\lambda p^{a\alpha}}{j}\geq \alpha$$

et le lemme est démontré.

Lemme 5.3 *Soient $d\geq 2$ un entier et $d=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ sa décomposition en facteurs premiers. On se donne deux entiers fixés $\lambda\geq 1$ et $\beta\geq 1$. Soit $a\geq 1+\frac{\beta}{\inf\alpha_i}$. Alors,*

$$\forall j\in[1,(\inf p^i)^\beta-1],\ \binom{\lambda d^a}{j}=\binom{\lambda d^a}{\lambda d^a-j}=0 \bmod d^a.$$

On a donc :

$$(1+X)^{\lambda d^a}=1+\gamma(d,\lambda,\beta,a)X^{(\inf p_i)^\beta}+\cdots+\gamma(d,\lambda,\beta,a)X^{\lambda d^a-(\inf p_i)^\beta}+X^{\lambda d^a} \bmod d.$$

Preuve.

En effet, définissons, pour tout i, l'entier $d^{(i)}$ par $d=d^{(i)}p_i^{\alpha_i}$. Alors

$$\binom{\lambda d^a}{j}=\binom{(\lambda d^{(i)a})p_i^{a\alpha_i}}{j}=0 \bmod p_i^{\alpha_i}$$

pour $j\in[1,(\inf p_i)^\beta-1]$ d'après la preuve du lemme 5.2 ci-dessus. Le lemme chinois et la relation $\binom{\lambda d^a}{j}=\binom{\lambda d^a}{\lambda d^a-j}$ permettent de conclure.

Lemme 5.4

1) La suite double $\left(\binom{m}{n} \bmod d\right)_{m,n}$ est récurrente.

2) Quel que soit $d\geq 2$ et quels que soient les entiers u et v supérieurs ou égaux à 1, on a :

$$P_d(u,v)=P_d(1,u+v-1).$$

Preuve.

1) Montrons que tout bloc à u lignes et v colonnes qui apparaît dans la suite double y apparaît deux fois, ce qui impliquera la première assertion. Il suffit naturellement de se limiter aux blocs "initiaux", c'est-à-dire de la forme

$$\begin{array}{cccc} \binom{0}{0} & \binom{0}{1} & \cdots & \binom{0}{v-1} \\ \binom{1}{0} & \binom{1}{1} & \cdots & \binom{1}{v-1} \\ \vdots & & & \vdots \\ \binom{u-1}{0} & \binom{u-1}{1} & \cdots & \binom{u-1}{v-1} \end{array}$$

Un tel bloc est obtenu comme les coefficients des développements :

$$\begin{array}{rcccccc} (1+X)^0 & = & \binom{0}{0} & + & \binom{0}{1}X & + & \cdots \\ & \vdots & & & & & \\ (1+X)^{u-1} & = & \binom{u-1}{0} & + & \binom{u-1}{1}X & + & \cdots \end{array}$$

Regardons alors les développements

$$\begin{array}{rcccccc} (1+X)^{d^a} & = & \binom{d^a}{0} & + & \binom{d^a}{1}X & + & \cdots \\ & \vdots & & & & & \\ (1+X)^{d^a+u-1} & = & \binom{d^a+u-1}{0} & + & \binom{d^a+u-1}{1}X & + & \cdots \end{array}$$

où β est choisi de sorte que $u-1 < (\inf p_i)^\beta$ et $a \geq 1 + \frac{\beta}{\inf \alpha_i}$, (on note toujours $d = \prod p_i^{\alpha_i}$ la décomposition en nombres premiers de l'entier d). Il résulte du lemme 5.3 et du choix de β qu'il n'y a pas "chevauchement" des puissances de X : pour i compris entre 0 et $u-1$, on a

$$\begin{array}{rl} (1+X)^{d^a+i} = & (1+X)^i + \gamma(d,1,\beta,a)X^{(\inf p_i)^\beta}(1+X)^i + ... \\ & +\gamma(d,1,\beta,a)X^{\lambda d^a-(\inf p_i)^\beta}(1+X)^i + X^{\lambda d^a}(1+X)^i \mod d, \end{array}$$

en particulier le bloc de coefficients

$$\begin{matrix} \binom{d^a}{d^a} & \binom{d^a}{d^a+1} & \cdots & \binom{d^a}{d^a+v-1} \\ \binom{d^a+1}{d^a} & \binom{d^a+1}{d^a+1} & \cdots & \binom{d^a+1}{d^a+v-1} \\ \vdots & & & \vdots \\ \binom{d^a+u-1}{d^a} & \binom{d^a+u-1}{d^a+1} & \cdots & \binom{d^a+u-1}{d^a+v-1} \end{matrix}$$

est égal au bloc

$$\begin{matrix} \binom{0}{0} & \binom{0}{1} & \cdots & \binom{0}{v-1} \\ \binom{1}{0} & \binom{1}{1} & \cdots & \binom{1}{v-1} \\ \vdots & & & \vdots \\ \binom{u-1}{0} & \binom{u-1}{1} & \cdots & \binom{u-1}{v-1} \end{matrix}$$

ce qui prouve le résultat.

2) Montrons que l'on a : $\forall u \geq 2,\ \forall v \geq 1,\ P_d(u,v) = P_d(u-1,v+1)$. Le résultat s'en déduit facilement par récurrence finie. Pour cela, considérons l'application Φ qui associe à une matrice à u lignes et v colonnes la matrice à $u-1$ lignes et $v+1$ colonnes définie par

$$\Phi \begin{pmatrix} a_{1,1} & \cdots & a_{1,v} \\ \vdots & & \vdots \\ a_{u,1} & \cdots & a_{u,v} \end{pmatrix} = \begin{pmatrix} b_{1,1} & \cdots & b_{1,v+1} \\ \vdots & & \vdots \\ b_{u-1,1} & \cdots & b_{u-1,v+1} \end{pmatrix}$$

avec :

$$\begin{array}{rcl} b_{i,j} & = & a_{i,j-1} \quad \forall i \in [1,u-1],\ \forall j \in [2,v+1] \\ b_{1,1} & = & a_{2,1} - a_{1,1} \\ \vdots & & \\ b_{u-2,1} & = & a_{u-1,1} - a_{u-2,1} \\ b_{u-1,1} & = & a_{u,1} - a_{u-1,1}. \end{array}$$

Si l'on note alors Ψ l'application qui associe à une matrice à $u-1$ lignes et $v+1$ colonnes la matrice à u lignes et v colonnes définie par

$$\Psi \begin{pmatrix} b_{1,1} & \cdots & b_{1,v+1} \\ \vdots & & \vdots \\ b_{u-1,1} & \cdots & b_{u-1,v+1} \end{pmatrix} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,v} \\ \vdots & & \vdots \\ a_{u,1} & \cdots & a_{u,v} \end{pmatrix}$$

avec :

$$\begin{array}{rcll} a_{i,j} & = & b_{i,j+1} & \forall i \in [1, u-1],\ \forall j \in [1, v] \\ a_{u,1} & = & b_{u-1,1} + b_{u-1,2} & \\ a_{u,2} & = & b_{u-1,2} + b_{u-1,3} & \\ \vdots & & & \\ a_{u,v} & = & b_{u-1,v} + b_{u-1,v+1}. & \end{array}$$

il est clair que :

- d'une part

$$\Phi \circ \Psi \begin{pmatrix} b_{1,1} & \cdots & b_{1,v+1} \\ \vdots & & \vdots \\ b_{u-1,1} & \cdots & b_{u-1,v+1} \end{pmatrix} = \begin{pmatrix} b_{1,1} & \cdots & b_{1,v+1} \\ \vdots & & \vdots \\ b_{u-1,1} & \cdots & b_{u-1,v+1} \end{pmatrix}$$

  si et seulement si :

$$\forall i \in [1, u-2],\ b_{i,1} = b_{i+1,2} - b_{i,2},$$

- d'autre part

$$\Psi \circ \Phi \begin{pmatrix} a_{1,1} & \cdots & a_{1,v} \\ \vdots & & \vdots \\ a_{u,1} & \cdots & a_{u,v} \end{pmatrix} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,v} \\ \vdots & & \vdots \\ a_{u,1} & \cdots & a_{u,v} \end{pmatrix}$$

  si et seulement si :

$$\forall j \in [2, v],\ a_{u,j} = a_{u-1,j-1} + a_{u-1,j},$$

- quels que soient $m \geq 0$ et $n \geq 1$, si on note A et B les blocs

$$A = \begin{pmatrix} \binom{m}{n} & \binom{m}{n+1} & \cdots & \binom{m}{n+v-1} \\ \binom{m+1}{n} & \binom{m+1}{n+1} & \cdots & \binom{m+1}{n+v-1} \\ \vdots & & & \vdots \\ \binom{m+u-1}{n} & \binom{m+u-1}{n+1} & \cdots & \binom{m+u-1}{n+v-1} \end{pmatrix}$$

$$B = \begin{pmatrix} \binom{m}{n-1} & \binom{m}{n} & \binom{m}{n+1} & \cdots & \binom{m}{n+v-1} \\ \binom{m+1}{n-1} & \binom{m+1}{n} & \binom{m+1}{n+1} & \cdots & \binom{m+1}{n+v-1} \\ \vdots & & & & \vdots \\ \binom{m+u-2}{n-1} & \binom{m+u-2}{n} & \binom{m+u-2}{n+1} & \cdots & \binom{m+u-2}{n+v-1} \end{pmatrix}$$

alors

$$\Phi(A) = B, \quad \Psi(B) = A.$$

Ces observations, jointes au fait que tout bloc qui apparaît dans le triangle de Pascal modulo d apparaît aussi ailleurs qu'"au bord", (première partie de ce lemme 5.4), montrent que les restrictions de Φ et Ψ aux ensembles des blocs de tailles respectives $u \times v$ et $(u-1) \times (v+1)$ qui apparaissent dans le triangle de Pascal sont des bijections inverses l'une de l'autre, et la seconde partie de notre lemme est prouvée.

Lemme 5.5 *Si d_1 et d_2 sont premiers entre eux, alors :*

$$P_{d_1 d_2}(u, v) = P_{d_1}(u, v) P_{d_2}(u, v), \ \forall u, v \geq 1.$$

Preuve.

D'après la seconde partie du lemme 5.4 ci-dessus, il suffit de prouver le résultat pour $u = 1$, c'est-à-dire :

$$P_{d_1 d_2}(1, v) = P_{d_1}(1, v) P_{d_2}(1, v), \ \forall v \geq 1.$$

En re-réduisant modulo d_1 (resp. d_2) un mot réduit modulo $d_1 d_2$, on a la majoration triviale :

$$P_{d_1 d_2}(1, v) \leq P_{d_1}(1, v) P_{d_2}(1, v), \ \forall v \geq 1.$$

Pour montrer l'égalité on a besoin d'une sorte d'indépendance : il suffit en fait de montrer que si $a_1 \cdots a_r$ est un facteur (en ligne) de la suite double des coefficients du binôme modulo d_1 et $b_1 \cdots b_r$ un facteur de la suite des coefficients du binôme modulo d_2, alors il existe un *même* couple d'indices (m, n) tel que :

$$\binom{m}{n} \cdots \binom{m}{n+r-1} = a_1 \cdots a_r \bmod d_1$$

et

$$\binom{m}{n} \cdots \binom{m}{n+r-1} = b_1 \cdots b_r \bmod d_2$$

Le lemme chinois montre alors en effet que le mot $c_1 \cdots c_r$ (modulo $d_1 d_2$), dont les réductions modulo d_1 et d_2 sont respectivement $a_1 \cdots a_r$ et $b_1 \cdots b_r$, apparaît (en particulier) en position (m, n) dans la suite des coefficients du binôme modulo $d_1 d_2$. Nous aurons bien alors l'autre inégalité :

$$P_{d_1 d_2}(1, v) \geq P_{d_1}(1, v) P_{d_2}(1, v), \ \forall v \geq 1.$$

Nous allons, étant donnés (m, n) et (m', n') tels que

$$\binom{m}{n} \cdots \binom{m}{n+r-1} = a_1 \cdots a_r \bmod d_1$$

et

$$\binom{m'}{n'} \cdots \binom{m'}{n'+r-1} = b_1 \cdots b_r \bmod d_2,$$

procéder en trois étapes :

- rendre m supérieur ou égal à $n+r-1$ et m' supérieur ou égal à $n'+r-1$, (pour être sûr que les lettres des mots étudiés apparaissent comme des coefficients des polynômes $(1+X)^m$ et $(1+X)^{m'}$);
- montrer qu'on peut supposer $n' = n$, (c'est-à-dire trouver une autre occurrence de $a_1 \cdots a_r$ et une autre occurrence de $b_1 \cdots b_r$ dans leurs triangles de Pascal respectifs, qui commencent en des colonnes de même indice);
- montrer qu'on peut aussi supposer $m' = m$.

Première étape

On peut supposer $m \geq n+r-1$ et $m' \geq n'+r-1$: en effet, d'après le lemme 5.3, si $d_1 = \prod p_i^{\alpha_i}$, si β est choisi tel que $\sup\{m, n+r-1\} < (\inf p_i)^\beta$ et a tel que $a \geq 1 + \frac{\beta}{\inf \alpha_i}$, alors,

$$\begin{aligned}(1+X)^{m+\lambda d_1^a} &= (1+X)^m + \gamma(d_1,\lambda,\beta,a)X^{(\inf p_i)^\beta}(1+X)^m + \cdots \\ &\quad + \gamma(d_1,\lambda,\beta,a)X^{\lambda d_1^a-(\inf p_i)^\beta}(1+X)^m + X^{\lambda d_1^a}(1+X)^m \\ &\quad \bmod d\end{aligned}$$

et donc le mot formé par les coefficients du développement de $(1+X)^{m+\lambda d_1^a}$ contient le facteur $a_1 \cdots a_r$ (dans les coefficients des termes de degré $< (\inf p_i)^\beta$) et l'on a $m + \lambda d_1^a \geq n+r-1$, à condition de prendre $\lambda \geq n+r-1$. Le raisonnement est le même pour m'.

Deuxième étape

Soient donc (m,n) et (m',n') tels que

$$\binom{m}{n} \cdots \binom{m}{n+r-1} = a_1 \cdots a_r \bmod d_1$$

et

$$\binom{m'}{n'} \cdots \binom{m'}{n'+r-1} = b_1 \cdots b_r \bmod d_2,$$

avec m supérieur ou égal à $n+r-1$ et m' supérieur ou égal à $n'+r-1$. Montrons qu'on peut supposer $n' = n$.

Soit β tel que $(\inf p_i)^\beta > m \geq n+r-1$, où $d_1 = \prod p_i^{\alpha_i}$. Alors toujours d'après le lemme 5.3, quels que soient $\lambda \geq 1$ et $a \geq 1 + \frac{\beta}{\inf \alpha_i}$, on a

$$(1+X)^{m+\lambda d_1^a} = (1+X)^m + \cdots + \gamma(d_1,\lambda,\beta,a)X^{\lambda d_1^a-(\inf p_i)^\beta}(1+X)^m + X^{\lambda d_1^a}(1+X)^m.$$

Le choix des paramètres implique que le facteur $a_1 \cdots a_r$ qui apparaît dans le mot formé par les coefficients de $(1+X)^m$ apparaît aussi dans le mot de ceux des coefficients de $(1+X)^{m+\lambda d_1^a}$ qui viennent de $X^{\lambda d_1^a}(1+X)^m$; plus précisément :

$$\binom{m}{n} \cdots \binom{m}{n+r-1} = \binom{m+\lambda d_1^a}{n+\lambda d_1^a} \cdots \binom{m+\lambda d_1^a}{n+\lambda d_1^a+r-1}.$$

De même, pour tout $\mu \geq 1$, en choisissant convenablement a (éventuellement différent de celui choisi ci-dessus, mais on appellera encore a le plus grand des deux) :

$$\binom{m'}{n'} \cdots \binom{m'}{n'+r-1} = \binom{m'+\mu d_2^a}{n'+\mu d_2^a} \cdots \binom{m'+\mu d_2^a}{n'+\mu d_2^a+r-1}.$$

Supposons par exemple $n' \geq n$, alors, comme d_1 et d_2 sont premiers entre eux, il existe deux entiers strictement positifs λ et μ tels que :

$$\lambda d_1^a - \mu d_2^a = n' - n,$$

d'où

$$n' + \mu d_2^a = n + \lambda d_1^a.$$

Ainsi, en remplaçant m par $m + \lambda d_1^a$, n par $n + \lambda d_1^a$, m' par $m' + \mu d_2^a$ et n' par $n' + \mu d_2^a$, obtient-on le résultat annoncé, (sans perdre le fait que les nouvelles valeurs de m et m' sont supérieures respectivement à $n + r - 1$ et $n' + r - 1$).

Troisième étape

Nous sommes donc maintenant dans la situation :

$$\binom{m}{n} \cdots \binom{m}{n+r-1} = a_1 \cdots a_r$$

et

$$\binom{m'}{n} \cdots \binom{m'}{n+r-1} = b_1 \cdots b_r,$$

avec $m \geq n + r - 1$ et $m' \geq n' + r - 1$. Montrons qu'on peut maintenant, tout en gardant n, remplacer m et m' par un même indice.

Pour cela, on choisit un β' tel que le plus petit nombre premier p qui divise l'un des nombres d_1 ou d_2 vérifie : $p^{\beta'} > \sup(m, m')$. On choisit aussi a' tel que $a' \geq 1 + \frac{\beta'}{\alpha}$ pour tous les α qui apparaissent comme exposants dans les décompositions en facteurs premiers de d_1 et de d_2. On écrit alors, pour tout $\lambda' \geq 1$,

$$(1+X)^{m+\lambda' d_1^{a'}} = (1+X)^m + \gamma(d_1, \lambda', \beta', a') X^{p^{\beta'}} (1+X)^m + \cdots$$

et le choix des paramètres montre que les puissances de X qui apparaissent dans le premier terme du second membre ($(1+X)^m$) ne réapparaissent pas dans les termes suivants, donc :

$$\binom{m+\lambda' d_1^{a'}}{n} \cdots \binom{m+\lambda' d_1^{a'}}{n+r-1} = \binom{m}{n} \cdots \binom{m}{n+r-1} = a_1 \cdots a_r.$$

De la même façon, et quitte à remplacer a' par un entier plus grand, pour tout $\mu' \geq 1$,

$$\binom{m'+\mu' d_2^{a'}}{n} \cdots \binom{m'+\mu' d_2^{a'}}{n+r-1} = \binom{m'}{n} \cdots \binom{m'}{n+r-1} = b_1 \cdots b_r.$$

Supposons $m' \geq m$, il existe comme précédemment deux entiers strictement positifs λ' et μ' tel que

$$\lambda' d_1^{a'} - \mu' d_2^{a'} = m' - m,$$

c'est-à-dire

$$m + \lambda' d_1^{a'} = m' + \mu' d_2^{a'},$$

ce qui achève la preuve de ce lemme.

Remarque 5.6 La "multiplicativité" de la complexité est à rapprocher intuitivement d'une propriété que nous avons rappelée au paragraphe 3 : on peut obtenir un dessin limite modulo 6 qui est la réunion des dessins limites modulo 2 et modulo 3.

5.2 Complexité du triangle de Pascal réduit modulo un nombre premier

Dans ce paragraphe, nous noterons $a = a(i,j)_{i,j\in\mathbf{N}}$ la suite double correspondant au triangle de Pascal réduit modulo p premier, c'est-à-dire la suite double définie sur l'alphabet $\mathcal{A} = \{\overline{0}, \cdots, \overline{p-1}\}$ (on note $\overline{j}$ la classe de j modulo p) par :

$$a(i,j) = \overline{\binom{i}{j}},$$

(pour simplifier les notations nous écrirons 0 au lieu de $\overline{0}$).

Nous nous proposons d'abord de compter les facteurs en ligne apparaissant dans cette suite double, c'est-à-dire d'évaluer la fonction de complexité en ligne $P_p(v) = P_p(1,v)$.

Le lemme suivant est une conséquence directe de la loi d'évolution de l'automate cellulaire.

Lemme 5.7 *Fixons l'entier n. Soit $a_i = a(n,i)$, pour $0 \leq i \leq n$. Les lignes d'indices pn à $pn+p-1$ sont données dans le schéma suivant où nous avons ajouté des signes "|" pour délimiter les blocs de longueur p :*

$$\begin{array}{cccccc|c|cccccc|cc}
a_0 & 0 & 0 & \dots & 0 & 0 & \dots & a_n & 0 & 0 & \dots & 0 & 0 & 0 & \dots \\
a_0 & a_0 & 0 & \dots & 0 & 0 & \dots & a_n & a_n & 0 & \dots & 0 & 0 & 0 & \dots \\
 & & & & & & \dots & & & & & & & & \\
a_0 & -a_0 & a_0 & \dots & -a_0 & a_0 & \dots & a_n & -a_n & a_n & \dots & -a_n & a_n & 0 & \dots
\end{array}$$

Preuve.

En effet, en utilisant la règle du triangle de Pascal, il suffit de connaître la ligne d'indice pn pour en déduire les lignes suivantes. Or les lignes d'indice n et pn se déduisent l'une de l'autre dans $\mathbb{Z}/p\mathbb{Z}$, de la manière suivante :

$$(1+X)^{pn} = (1+X^p)^n = \sum_{0 \leq i \leq n} a_i X^{pi} = \sum a(pn,j) X^j.$$

On a, plus précisément, la propriété de "rythme" suivante concernant la suite double a.

Lemme 5.8 *Un facteur en ligne de la suite $(a(i,j))_{i,j \in \mathbb{N}}$ de longueur supérieure ou égale à 3, différent de $x0\cdots0$ ou de $0\cdots0x$, où x est une lettre, apparaît à une unique congruence de ligne modulo p : en d'autres termes, il existe un (unique) entier k de $\{0,\cdots,p-1\}$ tel que, si i est l'indice d'une ligne à laquelle ce facteur apparaît, alors i est congru à k modulo p. De plus, si k est différent de $p-1$, B apparaît à une unique congruence de colonne modulo p. En revanche, si k est égal à $p-1$, B apparaît à une unique congruence de colonne si et seulement si B n'est pas de la forme $x\ \ (p-1)x\ \ x\ \ (p-1)x\ \ \cdots$, où x est une lettre.*

Preuve.

Nous allons, dans un premier temps, démontrer ce résultat pour des mots de longueur 3. On considère donc un facteur en ligne B de longueur 3, qui n'est pas de la forme $x00$ ou de $00x$, où x est une lettre. Soit (i,j) un indice d'apparition de ce facteur dans la suite double a. Soient $x = a(i,j)$, $y = a(i,j+1)$ et $z = a(i,j+2)$. On a donc $B = xyz$. Écrivons, de plus, $i = pi' + r$ et $j = pj' + s$, avec $0 \leq r, s \leq p-1$.

Nous allons distinguer deux cas selon que B contient ou non une lettre non nulle.

- Supposons que les lettres de B soient toutes non nulles. Supposons, de plus, que $s+2 \geq p$. On a donc $a(i, pj'+p-1) \neq 0$. Or, d'après le

théorème de Lucas [12], on a :

$$a(i, pj' + p - 1) = a(pi' + r, pj' + p - 1) = a(i', j')\overline{\binom{r}{p-1}}.$$

On en déduit, en particulier, que $\overline{\binom{r}{p-1}} \neq 0$, ce qui implique que $r = p - 1$. En effet, si u et v sont deux entiers tels que : $0 \leq u, v \leq p - 1$, on vérifie que l'on a $\overline{\binom{u}{v}} = 0$ si et seulement si $u < v$. On vérifie que, si $s = p - 2$, alors $z = (\overline{p-1})y$, et si $s = p - 1$, alors $x = (\overline{p-1})y$, ce qui s'écrit encore $y = (\overline{p-1})x$, puisque $(p-1)^2 \equiv 1$.

Montrons que pour toute autre occurrence de B, l'indice de ligne est encore congru à $p - 1$. Supposons donc qu'il existe une occurrence de B d'indice (m, n), avec $m \equiv r' \bmod p$, $n \equiv s' \bmod p$, $0 \leq r' \leq p-1$ et $0 \leq s' \leq p-3$, pour $p \neq 2$. Il existe alors un entier t', avec $0 \leq t' \leq p - 2$, tel que $\frac{\binom{r'}{t'+1}}{\binom{r'}{t'}} \equiv p - 1$. En effet, si $z = (\overline{p-1})y$, on a $t' = s' + 2$ et si $x = (\overline{p-1})y$, on a $t' = s' + 1$. Or cette égalité implique que $r' - t' \equiv (p-1)(t'+1)$, c'est-à-dire $r' = p - 1$.

Supposons, de plus, que B n'est pas de la forme $x\ (p-1)x\ x$. Soit t l'indice de la première lettre de B différente de x et de $(p-1)x$. La classe de s est alors déterminée par $s \equiv p - t + 1$.

Supposons maintenant que l'on ait $s+2 \leq p-1$. On a, d'après le théorème de Lucas :

$$a(i, j + l) = \overline{\binom{r}{s+l}}a(i', j'),$$

pour $l = 0,\ 1$ ou 2. Par conséquent, les rapports modulo p : $\frac{\binom{r}{s+l}}{\binom{r}{s+l+1}}$, pour $l = 0$ ou 1, ne dépendent que du bloc B. Or on vérifie que si l'on a les égalités suivantes modulo p, pour $l \in \{0, 1\}$ et pour $s+l$, r, $s'+l$ et r' dans l'intervalle $[0, p-2]$:

$$\frac{\binom{r}{s+l}}{\binom{r}{s+l+1}} \equiv \frac{\binom{r'}{s'+l}}{\binom{r'}{s'+l+1}}, \tag{1}$$

alors $r = r'$. En effet, en simplifiant l'égalité (1) on obtient

$$(r - (s + l))(s' + l + 1) = (r' - (s' + l))(s + l + 1),$$

c'est-à-dire

$$rs' + rl + r - s = r's + r'l + r' - s'.$$

En soustrayant les deux équations obtenues respectivement pour $l = 0$ et $l = 1$, on obtient bien $r = r'$. Par conséquent, la classe de r est uniquement déterminée par la valeur de ces quotients. Notons, de plus, que l'on a $s = s'$ si $r \neq p - 1$.

- Supposons que B contienne un 0. Le facteur B est alors de l'une des formes suivantes :

$$xy0,\ x0z,\ 0y0,\ 0yz,$$

avec $x, y, z \neq 0$. En effet, on a supposé que B ne s'écrit pas sous la forme $x00$ ou $00x$.

Supposons que $B = xy0$. Montrons que l'on a alors nécessairement $r = s+1$. En effet, supposons que $s+2 \leq p-1$. On a $y \neq 0$, et donc d'après le théorème de Lucas, on a $\overline{\binom{r}{s+1}} \neq 0$. On a, de plus, $a(i, j+2) = 0$, ce qui implique que $\overline{\binom{r}{s+2}} = 0$. On a donc bien $r = s+1$. Supposons maintenant que $s = p-2$. Comme $a(i, pj'+p-1) = y \neq 0$, on a alors $r = p-1 = s+1$. Enfin, on vérifie que l'on ne peut pas avoir $s = p-1$. En effet, on aurait alors $a(i, p(j'+1)) = y \neq 0$ et $a(i, p(j'+1)+1) = 0$, ce qui impliquerait que $r = 0$ et donc que $a(i, p(j'+1)-1) = x = 0$. Or on a supposé que $x \neq 0$.

On a donc bien $r = s+1$. On a alors, d'après le théorème de Lucas :

$$x = a(i,j) = a(pi'+r, pj'+s) = \overline{\binom{r}{r-1}} a(i',j') = \overline{r} a(i',j'),$$

et

$$y = a(i, j+1) = a(i', j').$$

L'entier r est donc uniquement déterminé par la relation : $x = \overline{r}y$.

Supposons que $B = x0z$. On ne peut avoir $s < p-2$, puisqu'il est impossible de satisfaire simultanément les égalités $z = a(i, j+2) = \overline{\binom{r}{s+2}} a(i', j') \neq 0$ et $0 = a(i, j+1) = \overline{\binom{r}{s+1}} a(i', j')$, car $\overline{\binom{r}{s+2}} \neq 0$ implique $\overline{\binom{r}{s+1}} \neq 0$. De même, $s \neq p-1$, puisque l'on aurait dans le cas contraire $a(i', j'+1) = 0$, ce qui contredit la non-nullité de z. On a donc $s = p-2$. On a alors $\binom{r}{p-2} \not\equiv 0$ et $\binom{r}{p-1} \equiv 0$, ce qui implique que $r = p-2$.

Supposons $B = 0y0$. On ne peut de même avoir $s \leq p-2$, puisque $a(i,j) = 0$ et $a(i, j+1) \neq 0$. On a donc $s = p-1$. On a alors $\binom{r}{0} \not\equiv 0$ et $\binom{r}{1} \equiv 0$, ce qui implique que $r = 0$.

Supposons $B = 0yz$. On a, de même, $s = p-1$. L'entier r est alors uniquement déterminé par

$$z = \overline{r}y.$$

On a donc montré le lemme 5.8 pour tout mot de longueur 3. Considérons maintenant un facteur en ligne B de longueur supérieure ou égale à 3, différent de $x0\cdots0$ ou de $0\cdots0x$, où x est une lettre. Un tel facteur contient nécessairement un mot de longueur 3 ne s'écrivant pas $00x$ ou $x00$, sauf s'il est de la forme

$x0\cdots0y$. On a alors $a(i, j + |B| - 2) = 0$ et $a(i, j + |B| - 1) = y \neq 0$. On en déduit que $j + |B| - 1 \equiv 0 \bmod p$, c'est-à-dire $s \equiv p + 1 - |B| \bmod p$. On vérifie, de plus, que $r = s$, car $a(i, j) \neq 0$ et $a(i, j + 1) = 0$. Par conséquent, r est uniquement déterminé par :

$$r \equiv p + 1 - |B|.$$

Enfin, un bloc ne s'écrivant pas sous la forme $x\ (p-1)x\ x\ldots$ contient nécessairement un mot de longueur 3 ne s'écrivant pas sous cette même forme.

Remarque 5.9

- Les facteurs $x0\cdots0$ et $0\cdots0x$, où x est une lettre apparaissent à toutes les congruences de lignes.

On déduit de cette propriété de "synchronisation" le résultat suivant concernant la "complexité en ligne".

Théorème 5.10 *On a, pour $0 \leq k \leq p-1$ et $v \geq 0$ tels que $pv + k \geq 3$:*

$$P_p(pv+k+1) - P_p(pv+k) = (p-k)(P_p(v+1) - P_p(v)) + k(P_p(v+2) - P_p(v+1)),$$

en posant $P_p(0) = 1$. On a, de plus, $P_p(1) = p$, $P_p(2) = p^2$ et

$$P_p(3) = \frac{p^3 + 4p^2 - 5p + 2}{2}.$$

Preuve.

L'idée de la preuve de ce théorème revient à compter les extensions des facteurs expansifs. On appelle facteur *expansif* un facteur en ligne ayant plusieurs extensions à droite. Notons qu'on entend généralement par extension d'un facteur B un facteur Bx, où x est une lettre qui suit le bloc B dans la suite. Nous appelons ici extension, par abus de langage, la lettre x elle-même. La différence première $P_p(v+1) - P_p(v)$ s'exprime de la manière suivante en fonction des extensions des facteurs expansifs. On note $\varphi(B)$ le nombre d'extensions à droite d'un bloc B de longueur n. On a alors

$$P_p(v+1) - P_p(v) = \sum_{|B|=v} (\varphi(B) - 1).$$

Nous allons démontrer dans un premier temps que $P_p(1) = p$, que $P_p(2) = p^2$ et que $P_p(3) = \frac{p^3+4p^2-5p+2}{2}$. Dans un second temps, nous allons considérer les prolongements des facteurs de la forme $0\cdots0x$, où x est une lettre. Enfin, nous démontrerons le théorème 5.10.

Lemme 5.11 *On a $P_p(1) = p$ et $P_p(2) = p^2$.*

Preuve.

Toutes les lettres de $\{\overline{0}, \cdots, \overline{p-1}\}$ apparaissent dans la suite a. En effet, on a $a(r,1) = \overline{\binom{r}{1}} = \overline{r}$, pour $0 \leq r \leq p-1$. On en déduit que $P_p(1) = p$.

Montrons que tous les blocs de longueur 2 sur $\{\overline{0}, \overline{1}, \cdots, \overline{p-1}\}$ apparaissent. Soit xy un tel bloc de première lettre x non nulle. Soit r l'unique entier de $\{0, 1, \cdots, p-1\}$ tel que $y = \overline{r}x$. Soit (i,j) un indice d'apparition de la lettre x. On vérifie, d'après le théorème de Lucas, que le facteur en ligne xy apparaît à l'indice $(pi + r, pj)$. On vérifie, de plus, que le bloc $0\overline{r}$, avec $0 \leq r \leq p-1$, apparaît à l'indice $(pr, p-1)$. On a donc $P_p(2) = p^2$.

Lemme 5.12 *On a* $P_p(3) = \frac{p^3+4p^2-5p+2}{2}$.

Preuve.

D'après le lemme 5.8, un facteur de longueur 3 ne s'écrivant pas $x00$ ou $00x$, apparaît à une unique congruence de ligne. On va donc compter les facteurs de longueur 3 selon la congruence des indices des lignes auxquelles ils apparaissent.

On vérifie qu'il y a $(r+1)(p-1)$ facteurs différents de $x00$ ou de $00x$ apparaissant à un indice de ligne congru à r modulo p, pour $0 \leq r \leq p-3$. En effet, les blocs de p lettres de la forme $a(i,pj')a(i,pj'+1)\cdots a(i,pj'+p-1)$, où i est congru à r, finissent par au moins $p-1-r$ zéros, d'après le lemme 5.7. Les facteurs différents de $x00$ ou de $00x$ apparaissant à un indice de ligne congru à un entier $r \leq p-3$ sont donc de la forme

$$\overline{\binom{r}{l}}y \ \ \overline{\binom{r}{l+1}}y \ \ \overline{\binom{r}{l+2}}y,$$

avec $0 \leq l \leq r-1$, ou de la forme

$$0 \ y \ \overline{r}y,$$

où y est une lettre non nulle. On vérifie alors que ces mots sont tous distincts et qu'ils sont au nombre de $(r+1)(p-1)$. On a vu, en effet, dans la preuve du lemme 5.8 qu'une égalité du type (1) implique, quand $r \neq p-1$, l'unicité de l.

Les facteurs différents de $x00$ ou de $00x$ apparaissant à un indice de ligne congru à $p-2$ modulo p sont de l'une des formes

$$\overline{\binom{p-2}{l}}y \ \ \overline{\binom{p-2}{l+1}}y \ \ \overline{\binom{p-2}{l+2}}y, \qquad y \ 0 \ z, \qquad \text{ou} \quad 0 \ \ y \ \ \overline{(p-2)}y,$$

où y et z sont des lettres non nulles et où $0 \leq l \leq p-3$. On vérifie que ces mots sont tous distincts et qu'ils sont au nombre de $2(p-1)^2$.

Enfin, les facteurs différents de $x00$ ou de $00x$ apparaissant à un indice de ligne congru à $p-1$ modulo p sont de l'une des formes suivantes

$$0 \ y \ (p-1)y, \quad (p-1)y \ y \ z, \quad y \ z \ (p-1)z, \quad y \ (p-1)y \ 0,$$

où y et z sont des lettres non nulles. On vérifie qu'il y a alors $2(p-1)$ facteurs de la forme $0\ y\ (p-1)y$ ou de la forme $y\ (p-1)y\ 0$, et $2(p-1)^2-(p-1)$ facteurs de la forme $(p-1)y\ y\ z$ ou de la forme $y\ z\ (p-1)z$, soit en tout $p-1+2(p-1)^2$ tels facteurs.

En adjoignant à ces divers facteurs les $2p-1$ facteurs de la forme $x00$ et de la forme $00x$, on obtient bien le résultat annoncé, à savoir :

$$P_p(3) = (p-1)(1+2+\cdots+p-2) + 4(p-1)^2 + (p-1) + 2p - 1,$$

c'est-à-dire

$$P_p(3) = \frac{p^3+4p^2-5p+2}{2}.$$

Lemme 5.13 *Un bloc de la forme $0\cdots0x$, où x est une lettre, a p prolongements.*

Preuve.

Il suffit de montrer que tout bloc de la forme $0\cdots0x$, de longueur p^t+1, où x est une lettre non nulle de $\{\overline{1},\cdots,\overline{p-1}\}$ et t un entier supérieur ou égal à 1, apparaît dans le triangle de Pascal et admet p prolongements. Soit donc y une lettre de $\{\overline{0},\overline{1},\cdots,\overline{p-1}\}$ et soit r l'unique entier de $\{0,1,\cdots,p-1\}$ tel que $y=\overline{r}x$. Soit (i,j) un indice d'apparition du bloc $0x$. On a, d'après le théorème de Lucas :

$$a(p^ti+r,p^t(j+1)) = a(i,j+1) = x,$$
$$a(p^ti+r,p^t(j+1)+1) = \overline{r}a(i,j+1) = \overline{r}x = y,$$
$$a(p^ti+r,p^tj+l) = 0, \text{ pour } 0\le l\le p^t-1.$$

On a donc montré que le bloc $0\cdots0xy$ apparaît à l'indice (p^ti+r,p^tj). Ce bloc est donc un facteur de la suite double a, ce qui achève la preuve du lemme 5.13.

Preuve du théorème 5.10.

Notons qu'un facteur de la forme $x0\cdots0$, où x est une lettre non nulle, et de longueur $pv+k$, où $0\le k\le p-1$, peut apparaître à plusieurs congruences de lignes, mais on vérifie qu'il n'aura une extension autre que 0 qu'à une ligne d'indice congru à $p-k$ modulo p (lemme 5.7). Par conséquent, on déduit de cette remarque et du lemme 5.8 qu'un facteur expansif qui n'est pas de la forme $0\cdots0x$, où x est une lettre, apparaît à une unique congruence en ligne. Nous allons comptabiliser dans $P_p(v)$ les facteurs selon la congruence en ligne à laquelle ils apparaissent. On note donc, pour $0\le r\le p-1$, $P^{(r)}(v)$ le nombre de facteurs en ligne de longueur v qui ne sont pas de la forme $0\cdots0x$ et qui apparaissent à un indice de ligne congru à r modulo p. On a donc :

$$P_p(v+1)-P_p(v) = \sum_{r=0}^{p-1}(P^{(r)}(v+1)-P^{(r)}(v)) + \sum_{x\in\{0,1,\cdots,p-1\}}(\varphi(0\cdots0x)-1),$$

c'est-à-dire, d'après le lemme 5.13 :

$$P_p(v+1) - P_p(v) = \sum_{r=0}^{p-1} (P^{(r)}(v+1) - P^{(r)}(v)) + p(p-1). \tag{2}$$

Soient $k \in [0, p-1]$ et $v \geq 0$ tels que $pv + k \geq 3$. Soit B un facteur en ligne expansif de longueur $pv + k$, différent de $0 \cdots 0x$, où x est une lettre. Soit $\overline{r}$ la classe modulo p des indices des lignes dans lesquelles B apparaît.

Soit (i, j) un indice d'apparition du bloc B. Écrivons $i = pi' + r$ et $j = pj' + s$, avec $0 \leq r, s \leq p-1$. On a

$$B = a(i, j) \cdots a(i, j + pv + k - 1).$$

Pour toute occurrence de B telle que $j + pv + k - 1 \not\equiv p - 1$, c'est-à-dire $s \not\equiv p - k$, B admet une unique extension, déterminée par les lettres de B. En effet, considérons une telle occurrence. D'après le lemme de Lucas, B est suivi de la lettre

$$a(i, j + pv + k - 1)\overline{\frac{\binom{r}{s+k}}{\binom{r}{s+k-1}}},$$

si $1 \leq s + k \leq p - 1$ ou de la lettre

$$a(i, j + pv + k - 1)\overline{\frac{\binom{r}{s+k-p}}{\binom{r}{s+k-1-p}}},$$

si $s + k \geq p + 1$. Or, d'après le lemme 5.8, l'entier s est entièrement déterminé, si B n'est pas de la forme $x\ (p-1)x\ x \cdots$, où x est une lettre; enfin, tout bloc de la forme $x\ (p-1)x\ x \cdots$ est suivi de son avant-dernière lettre, pour une telle occurrence.

Supposons donc $s \equiv p - k$. Nous allons distinguer deux cas selon la position de r par rapport à $p - k - 1$.

- Supposons $0 \leq r \leq p - k - 1$. Chaque bloc de p termes compris entre deux indices de colonnes divisibles par p finit par au moins k zéros (lemme 5.7). Notons qu'on a alors $v \geq 1$, car on a supposé que B n'est pas le facteur nul. Les entiers r, k et j étant fixés, le bloc B est alors uniquement déterminé par les lettres du bloc B' défini ci-dessous et apparaissant à l'indice $(i', j' + 1)$:

  $$B' = a(i', j' + 1) \cdots a(i', j' + v) = a(i, pj' + p) \cdots a(i, pj' + pv).$$

  Le bloc B a, de plus, les mêmes extensions à droite que le bloc B'. Réciproquement, on vérifie qu'on peut associer à chaque facteur expansif B' différent de $0 \cdots 0$ et de longueur v, un facteur expansif B de longueur

$pv+k$, ne s'écrivant pas sous la forme $0\cdots 0x$, apparaissant à un indice de ligne congru à un entier r inférieur ou égal à $p-k-1$ et ayant, enfin, les mêmes extensions que B'.

On obtient donc :

$$P^{(r)}(pv+k+1) - P^{(r)}(pv+k) = P_p(v+1) - P_p(v) - (p-1).$$

Le terme $p-1$ provient du fait que l'on a soustrait l'apport en extensions du facteur $0\cdots 0$.

- Supposons $p-k \leq r \leq p-1$. Le raisonnement est alors le même en considérant, dans ce cas, le bloc B', de longueur $v+1$, suivant :

  $$B' = a(i',j')\cdots a(i',j'+v) = a(i,pj'+p-k)a(i,pj'+p)\cdots a(i,pj'+pv).$$

  En effet, on a besoin de connaître, dans ce cas, la lettre $a(i',j')$, qui détermine les valeurs, non forcément toutes nulles ici, des k premières lettres du bloc B. On a donc

  $$P^{(r)}(pv+k+1) - P^{(r)}(pv+k) = P_p(v+2) - P_p(v+1) - (p-1).$$

On déduit alors de (2) la relation suivante, en posant $P_p(0)=1$:

$$\begin{aligned} P_p(pv+k+1) - P_p(pv+k) &= (p-k)(P_p(v+1) - P_p(v) - (p-1)) \\ &\quad + k(P_p(v+2) - P_p(v+1) - (p-1)), \\ &\quad + p(p-1) \end{aligned}$$

c'est-à-dire

$$P_p(pv+k+1) - P_p(pv+k) = (p-k)(P_p(v+1) - P_p(v)) + k(P_p(v+2) - P_p(v+1)).$$

Remarque 5.14

- On vérifie que l'on a, pour $p=2$ et pour tout v : $P_2(v) = v^2 - v + 2$. En revanche, pour des valeurs de $p \neq 2$, l'expression de la complexité n'est pas polynomiale. En effet, les premières valeurs de la différence seconde de la complexité $x(v) = P_p(v+2) - 2P_p(v+1) + P_p(v)$ satisfont, d'après le théorème 5.10, $x(2) = \frac{-p^3+6p^2-9p+4}{2}$ et $x(1) = \frac{p^3-3p+2}{2}$, pour $p \neq 2$, ce qui implique que $x(2) \neq x(1)$. Si la complexité était polynomiale, ce serait un polynôme de degré au plus égal à deux d'après la troisième partie de cette remarque. Or la différence seconde d'une expression polynomiale de degré au plus deux est constante.

- Néanmoins, on déduit du théorème 5.10 la propriété suivante : les suites $(P_p(v))_{v\in\mathbb{N}}$ et $(P_p(v+1) - P_p(v))_{v\in\mathbb{N}}$ sont p-régulières au sens de [4].

- On déduit du théorème 5.10 que la différence seconde de la complexité $x(v) = P_p(v+2) - 2P_p(v+1) + P_p(v)$ vérifie :

$$x(pv+k) = x(v),$$

pour $k \in [0, p-1]$ et pour $pv+k \geq 3$. Il suffit, en effet, d'évaluer la différence $x(pv+k) = (P_p(pv+k+2) - P_p(pv+k+1)) - (P_p(pv+k+1) - P_p(pv+k))$. Cette suite ne prend donc qu'un nombre fini de valeurs ($x(0)$, $x(1)$, $x(2)$). Le calcul de ces valeurs montre que $x(0) = (p-1)^2 > 0$ et que, pour $p \neq 2$ et 3, $0 < -x(2) < x(1)$. On a enfin, pour $p = 2$ ou 3, $x(2) > 0$. On en déduit, d'une part, que cette suite est p-automatique au sens de [7], et d'autre part, le lemme suivant.

Lemme 5.15 *Soit $P_p(v)$ la complexité en ligne du triangle de Pascal réduit modulo un nombre premier p. Il exite alors deux constantes C_1 et C_2 telles que l'on ait, pour tout entier v :*

$$C_1 v^2 \leq P_p(v) \leq C_2 v^2.$$

Plus généralement, on déduit de la deuxième assertion du lemme 5.4 et de la première des remarques 5.14 ci-dessus le théorème suivant.

Théorème 5.16 *Soit $P_p(u,v)$ la complexité par blocs du triangle de Pascal réduit modulo un nombre premier p.*
Si $p = 2$, alors

$$P_2(u,v) = u^2 + v^2 + 2uv - 3u - 3v + 4.$$

Pour tout nombre premier p, il existe deux constantes C_1 et C_2 (qui dépendent de p) telles que l'on ait, pour tout entier $u \geq 1$ et tout entier $v \geq 1$:

$$C_1 sup(u,v)^2 \leq P_p(u,v) \leq C_2 sup(u,v)^2.$$

Notons que la suite double des coefficients binomiaux modulo p est p-automatique, voir [3]. Cette propriété implique aussi la majoration quadratique ci-dessus d'après [13].

5.3 Complexité du triangle de Pascal réduit modulo une puissance d'un nombre premier

Nous pouvons maintenant obtenir facilement des bornes pour la complexité du triangle de Pascal réduit modulo une puissance d'un nombre premier.

Théorème 5.17 *Si $d = p^e$ où p est un nombre premier, alors il existe deux constantes C_3 et C_4 (qui dépendent de p^e) telles que :*

$$C_3 sup(u,v)^2 \leq P_{p^e}(u,v) \leq C_4 sup(u,v)^2.$$

Preuve.

La majoration se déduit de l'automaticité de la suite des coefficients binomiaux modulo p^e prouvée dans [3] et du résultat de [13] sur la complexité des suites doubles automatiques.

Pour la minoration, il suffit de remarquer que, pour $u, v \geq 1$:

$$P_{p^e}(u, v) \geq P_p(u, v).$$

Cette inégalité s'obtient sans difficulté en re-réduisant modulo p le triangle de Pascal modulo p^e.

5.4 Complexité du triangle de Pascal réduit modulo un entier $d \geq 1$

Dans ce paragraphe nous allons rassembler les résultats de complexité déjà donnés pour établir un résultat général sur la complexité du triangle de Pascal modulo un entier d.

Théorème 5.18 *Soit $d \geq 1$. On note $\omega(d)$ le nombre de facteurs premiers distincts de la décomposition de d. Alors il existe deux constantes A et B (qui dépendent de d) telles que, quels que soient $u, v \geq 1$, on ait*

$$A \sup(u, v)^{2\omega(d)} \leq P_d(u, v) \leq B \sup(u, v)^{2\omega(d)}.$$

Preuve.

La preuve est aisée : on utilise la multiplicativité de la complexité donnée dans le lemme 5.5 et le théorème 5.17 ci-dessus.

Remarque 5.19

- Le théorème 5.18 ci-dessus non seulement montre une différence qualitative entre le cas où d est une puissance d'un nombre premier et le cas, disons, $d = 6$, mais il fournit aussi une sorte de mesure quantitative indiquant que la "complication" du triangle de Pascal modulo d croît avec le nombre de diviseurs premiers (distincts) de d.

- Nous avons établi le théorème 5.18 ci-dessus en utilisant (via le théorème 5.17) la propriété que la suite double des binomiaux modulo une puissance d'un nombre premier est automatique [3]. Mais à son tour ce théorème 5.18 implique que *la suite des binomiaux modulo d n'est k-automatique pour aucun $k \geq 2$ quand d n'est pas une puissance d'un nombre premier*, puisque la complexité croît alors trop vite et ne satisfait pas la majoration quadratique donnée dans [13]. Nous obtenons ainsi une nouvelle preuve de ce résultat déjà démontré dans [3].

- Peut-on obtenir l'ordre de grandeur de la complexité dans le cas d'un automate cellulaire linéaire quelconque? Le premier cas que l'on peut considérer est celui de l'automate cellulaire donné par $r(X)(1+X)^k$, c'est-à-dire le triangle de Pascal avec une condition initiale $r(X)$ non nécessairement égale à 1. Écrivons $r(X) = r_0 + r_1X + \cdots + r_tX^t$, avec r_t différent de zéro modulo d. Considérons l'application de l'ensemble $\mathcal{P}^{(1)}(v+t)$ des facteurs (en ligne) de longueur $v+t$ du triangle de Pascal avec condition initiale 1 dans l'ensemble $\mathcal{P}^{(r)}(v)$ des facteurs (en ligne) de longueur v du triangle de Pascal avec condition initiale $r(X)$, qui à un bloc $B = b_1 \cdots b_{v+t}$ associe le bloc $B' = b'_1 \cdots b'_v$, où $b'_i = r_0b_i + \cdots + r_tb_{t+i}$. On vérifie que cette application est surjective et que chaque bloc admet au plus d^t antécédents, si d désigne l'entier selon lequel on réduit. Ceci donne une estimation du cardinal de $\mathcal{P}^{(r)}(v)$, d'où l'on déduit que la complexité du triangle de Pascal avec la condition initiale $r(X)$ admet le même ordre de croissance que la complexité du triangle de Pascal avec condition initiale 1, c'est-à-dire

$$\exists A > 0,\ \exists B > 0,\ \forall u, v \geq 1,\ A \sup(u,v)^{2\omega(d)} \leq P(u,v) \leq B \sup(u,v)^{2\omega(d)}.$$

Pour un automate cellulaire linéaire général, en utilisant l'automaticité dans le cas où l'on réduit modulo une puissance d'un nombre premier [3], puis la majoration quadratique dans ce cas [13] et enfin la partie facile du lemme 5.5, (c'est-à-dire la majoration

$$P_{d_1d_2}(u,v) \leq P_{d_1}(u,v)P_{d_2}(u,v),\ \forall u, v \geq 1$$

pour d_1 et d_2 premiers entre eux), on prouve facilement :
la complexité de la suite double engendrée par un automate cellulaire linéaire modulo d vérifie :

$$P(u,v) \leq C \sup(u,v)^{2\omega(d)}.$$

Nous n'avons pas encore pu obtenir de minoration.

6 Triangle de Pascal et musique

On peut penser naïvement que la musique se trouve entre le désordre (qui présente une grande complexité) et un ordre ennuyeux (avec une faible complexité). Pour développer cette idée, le compositeur Tom Johnson a proposé une illustration musicale du triangle de Pascal réduit respectivement modulo 7 et modulo 8. Cette expérience a donné lieu à une émission radiophonique, (France Culture, Atelier de Création Radiophonique, Le triangle de Pascal, par Tom Johnson et René Farabet, avec le premier auteur et Bernadette Le Saché, le 12 février 1995).

Remerciements

Nous remercions chaleureusement G. Skordev qui nous a suggéré cette étude de la complexité du triangle de Pascal, M. Keane et M. Dekking qui nous ont indiqué indépendamment qu'il devait y avoir une propriété d'"indépendance" pour ces triangles réduits modulo deux nombres premiers entre eux, ainsi que M. Koskas qui a adapté pour nous son programme efficace de calcul de complexités de suites doubles. Nous remercions enfin l'arbitre de ce papier pour ses commentaires précis et utiles.

Références

[1] J.-P. Allouche, Sur la transcendance de la série formelle Π, *Séminaire de Théorie des Nombres de Bordeaux, Deuxième Série* **2** (1990), 103–117.

[2] J.-P. Allouche, Sur la complexité des suites infinies, *Bull. Belg. Math. Soc.* **1** (1994), 133–143.

[3] J.-P. Allouche, F. von Haeseler, H.-O. Peitgen, G. Skordev, Linear cellular automata, finite automata and Pascal's triangle, *Discrete Applied Math.* (1995), à paraître.

[4] J.-P. Allouche, J. Shallit, The ring of k-regular sequences, *Theoret. Comput. Sci.* **98** (1992), 163–187.

[5] D. Barbolosi, P. J. Grabner, Distribution des coefficients multinomiaux et q-binomiaux modulo p, *Indag. Math.* (1996), à paraître.

[6] V. Bruyère, G. Hansel, C. Michaux, R. Villemaire, Logic and p-recognizable sets of integers, *Bull. Belg. Math. Soc.* **1** (1994), 191–238; 577.

[7] G. Christol, T. Kamae, M. Mendès France, G. Rauzy, Suites algébriques, automates et substitutions, *Bull. Soc. math. France* **108** (1980), 401–419.

[8] F. von Haeseler, H.-O. Peitgen, G. Skordev, Pascal's triangle, dynamical systems and attractors, *Ergod. Th. & Dynam. Sys.* **12** (1992), 479–486.

[9] F. von Haeseler, H.-O. Peitgen, G. Skordev, On the fractal structure of rescaled evolution sets of cellular automata and attractors of dynamical systems, Report 278 (1992), Inst. Dyn. Syst., University of Bremen,

[10] F. von Haeseler, H.-O. Peitgen, G. Skordev, Global analysis of self-similarity features of cellular automata: selected examples, *Physica D* **86** (1995), 64–80.

[11] E. Lange, H.-O. Peitgen, G. Skordev, Fractal patterns in Gaussian and Stirling number tables, *Ars Combinatoria* (1997), à paraître.

[12] E. Lucas, Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, *Bull. Soc. math. France* **6** (1878), 49–54.

[13] D. Razafy Andriamampianina, Nombre de facteurs d'une suite infinie, prépublication (1994).

[14] O. Salon, Suites automatiques à multi-indices et algébricité, *C. R. Acad. Sci. Paris, Série I* **305** (1987), 501–504.

[15] O. Salon, Suites automatiques à multi-indices, *Séminaire de Théorie des Nombres de Bordeaux*, Exposé 4, (1986-1987), 4-01–4-27; suivi par un Appendice de J. Shallit, 4-29A–4-36A.

[16] I. Stewart, Four encounters with Sierpiński's gasket, *Mathematical Intelligencer* **17** (1995), 52–64.

Jean-Paul Allouche
C. N. R. S.,
LRI, Bâtiment 490
F-91405 Orsay Cedex
France
allouche@lri.lri.fr

Valérie Berthé
C. N. R. S.,
LMD, Luminy, Case 930
F-13288 Marseille Cedex 9
France
berthe@lmd.univ-mrs.fr