

# CONSTRUCTION D'ÉVÉNEMENTS EQUIPROBABLES ET COEFFICIENTS MULTINOMIAUX MODULO $p^n$

PAR

JACQUES BERNARD ET GÉRARD LETAC

## Introduction

Soient  $(I, \mathfrak{C}, \pi)$  un espace de probabilité,  $(\Omega, \mathfrak{F}, P)$  l'espace formé en prenant le produit d'une infinité dénombrable de copies  $(I_t, \mathfrak{C}_t, \pi_t)$ ,  $t = 1, 2, \dots$ . On note  $a_t$  l'application canonique de  $\Omega$  dans  $I_t$  et  $\mathfrak{F}_t$  la tribu rendant mesurable les applications  $a_1 \cdots a_t$ .

En 1951, considérant le cas où  $I$  a 2 éléments, John Von Neumann [1] construisait un temps d'arrêt  $T$  par rapport aux  $(\mathfrak{F}_t)_{t \geq 1}$  et un ensemble  $\mathfrak{F}_T$  mesurable  $A$  tel que  $P(A) = \frac{1}{2}$  indépendamment de  $\pi$  (pourvu que  $\pi$  ne soit pas concentrée en un point de  $I$ ).

En 1970, W. Hoeffding et G. Simons [2] ont repris le problème, toujours dans le cas où  $I$  a 2 éléments, en fabriquant divers autres temps d'arrêt avec la même propriété et en cherchant à diminuer  $E(T)$ . L'une des procédures ( $Q_2$  dans [2]) consiste à considérer dans l'ensemble  $N^2$  des couples d'entiers l'ensemble  $H_2$  des points  $(x_1, x_2)$  tels que  $C_{x_1+x_2}^{x_1}$  soit pair, ainsi que la promenade aléatoire  $S_0 = (0, 0)$ ,  $S_t = y_1 + \cdots + y_t$  où  $y_1, \dots, y_t$  sont indépendants et de loi définie par  $P(y_t = (1, 0)) = \pi_1$  et  $P(y_t = (0, 1)) = \pi_2$ . Ils définissent ensuite  $T$  comme le temps de frappe de  $H_2$ , montrent que  $T$  répond à la question et calculent  $E(T)$ . C'est cette partie de [2] que nous généralisons ici, et cela suivant deux directions simultanément:

— en prenant  $I$  fini ou dénombrable;

— en construisant  $T$  de sorte qu'il existe une partition  $(A_1, \dots, A_m)$  de  $\Omega$  qui soit  $\mathfrak{F}_T$  mesurable et telle que  $P(A_1) = \cdots = P(A_m) = 1/m$ . Cette généralisation est facile et est faite au §2.

Des préliminaires nécessaires sont donnés en §1 et on calcule  $E(T)$  en §3 dans le cas où  $m$  est premier. Nous obtenons au passage l'interprétation combinatoire d'un théorème de Lucas sur le résidu des multinomiaux modulo  $p$ .

Bien que les tentatives pour calculer  $E(T)$ , dans le cas où  $m$  n'est pas premier, s'avèrent infructueuses, l'observation de tables des résidus modulo  $p^n$  des binomiaux (voir Tables 1 et 2) fait apparaître des faits nouveaux ou du moins peu connus, et c'est en réalité leurs démonstrations qui motivent cet article.

Ainsi on constate que si  $(x_1, x_2)$  est tel que  $C_{x_1+x_2}^{x_1} \equiv 0 \pmod{p^n}$  alors il en est de même pour les points  $(px_1 + a, px_2 + b)$  si  $|a| < p$ ,  $|b| < p$  et  $a + b \geq 0$ . Ceci est formalisé et généralisé au §4.

On observe ensuite que les bandes de la table des résidus modulo  $p^n$  qui sont parallèles aux axes et de longueur  $p^k$  possèdent une périodicité. Ce fait,

---

Received May 4, 1971.





connu dans le cas binomial [3], est démontré dans le cas multinomial en §5. On utilise pour cela une identité facile à établir, mais dont un corollaire donne une majoration du nombre de matrices à coefficients 0 ou 1 de marges données, dont la détermination reste une énigme [4].

Enfin une constatation curieuse est que les éléments du tableau des résidus modulo  $p^n$  sont peu différents si on change  $(x_1, x_2)$  en  $(px_1, px_2)$ . Cette observation conduit à la preuve de la convergence de  $C_{p^n(x_1+k_2)}^{p^n x_1}$  si  $n \rightarrow \infty$  dans l'anneau  $\mathbf{Z}_p$  des entiers  $p$  adiques. Il est à noter que le théorème est assez fin pour qu'il soit nécessaire de séparer  $p = 2$  et  $p > 2$ .

### 1. Le théorème de Kummer et ses conséquences

Désormais  $I$  note un ensemble fini ou dénombrable.  $\mathcal{G}$  est le groupe abélien libre engendré par  $I$ , identifié à l'ensemble des suites d'entiers  $x = (x_i)_{i \in I}$  telles que  $x_i \neq 0$  pour un nombre fini de  $i$  seulement;  $\mathcal{M}$  est le monoïde abélien libre engendré par  $I$ , identifié à l'ensemble des suites d'entiers non négatifs  $x = (x_i)_{i \in I}$  de  $\mathcal{G}$ . On définit en particulier  $\varepsilon^j$  dans  $\mathcal{M}$  avec  $j \in I$  par  $(\varepsilon^j)_i = 1$  si  $i = j$  et  $(\varepsilon^j)_i = 0$  si  $i \neq j$ . Si  $x \in \mathcal{G}$ , on pose  $|x| = \sum_i x_i$  et

$$c(x) = 0 \text{ si } x \notin \mathcal{M}, \quad c(x) = |x|! / \prod_i (x_i!) \text{ si } x \in \mathcal{M}.$$

Si  $(X_i)_{i \in I}$  est un ensemble de variables formelles, on pose  $X^x = \prod_i X_i^{x_i}$  si  $x \in \mathcal{M}$ .

On se fixe un nombre premier  $p$ . Dans les notations suivantes, qui s'y rapportent, on se dispense de faire figurer l'indice  $p$ .

Si  $n$  est un entier  $\geq 0$ , on pose:

$$n = \sum_{\alpha \geq 0} h_\alpha(n) p^\alpha, \quad \text{avec } 0 \leq h_\alpha(n) < p \text{ et } h_\alpha(n) \text{ entier,}$$

$$v(n) = \inf \{ \alpha : h_\alpha(n) > 0 \}, \quad \text{avec } v(0) = +\infty$$

$$d(n) = \sup \{ \alpha : h_\alpha(n) > 0 \}, \quad \text{avec } d(0) = -\infty$$

et 
$$\|n\| = \sum_{\alpha \geq 0} h_\alpha(n).$$

Recensons, dans la proposition suivante, quelques faits importants:

- PROPOSITION 1. (a)  $\|pn\| = \|n\|$   
 (b)  $\|n\| \leq (d(n) - v(n) + 1)(p - 1)$  si  $n \neq 0$   
 (c)  $\|n - 1\| = (p - 1)v(n) + \|n - p^{v(n)}\|$   
 (d)  $(p - 1)v(n!) = n - \|n\|$   
 (e)  $\|n + m\| \leq \|n\| + \|m\|.$

(a), (b), et (c) sont immédiats. On trouvera une preuve de (d) dans [5]; nous allons montrer (e) dans un instant.

Si  $x \in \mathcal{M}$ , on définit  $h_\alpha(x)$  dans  $\mathcal{M}$  par  $(h_\alpha(x))_i = h_\alpha(x_i)$ ,

$$v(x) = \inf_i v(x_i), \quad d(x) = \sup_i d(x_i)$$

et  $\|x\| = \sum_i \|x_i\|$

D'après la proposition 1 (d) on a

(1) 
$$(p - 1)v(c(x)) = -\|x\| + \sum_i \|x_i\|$$

En appliquant cette formule à  $x = (m, n)$  et en utilisant le fait bien connu que  $c(x)$  est un entier, on a la preuve de (e).

Il est important de remarquer également que  $v(c(p^n x)) = v(c(x))$  pour tout  $n \geq 0$ . Introduisons les entiers  $q_0(x), \dots, q_\alpha(x), \dots$  définis par

$$pq_0(x) = |h_0(x)| - h_0(|x|),$$

$$pq_\alpha(x) = q_{\alpha-1}(x) + |h_\alpha(x)| - h_\alpha(|x|) \quad \text{si } \alpha \geq 1.$$

Un peu de réflexion montre que les  $q_\alpha(x)$  sont des entiers  $\geq 0$  et qu'ils constituent la "retenue" effectuée dans la colonne  $\alpha$  lorsqu'on effectue l'addition des  $x_i$  en base  $p$ . Le théorème suivant est dû essentiellement à Kummer [6].

**THÉORÈME 1.** *Si  $x \in \mathfrak{M}$ ,  $v(c(x)) = \sum_{\alpha \geq 0} q_\alpha(x)$ .*

*Preuve.* La preuve se fait en posant  $l_\alpha = |h_\alpha(x)| - h_\alpha(|x|)$ . Alors si  $\alpha \geq 0$ ,  $q_\alpha = l_\alpha/p + l_{\alpha-1}/p^2 + \dots + l_0/p^{\alpha+1}$ . Donc

$$\sum_{\alpha \geq 0} q_\alpha = (1/(p - 1)) \sum_{\alpha \geq 0} l_\alpha = v(c(x))$$

d'après (1). Le corollaire suivant du Théorème 1 est immédiat:

**COROLLAIRE.**  *$c(x) \not\equiv 0 \pmod p$  si et seulement si  $|h_\alpha(x)| < p$  pour tout  $\alpha \geq 0$ .*

Nous aurons besoin des conséquences suivantes du Théorème 1:

**THÉORÈME 2.** *Si  $x \in \mathfrak{M}$  et  $x \neq 0$ , alors*

- (a)  $v(|x|) - v(x) \leq v(c(x))$
- (b)  $d(|x|) - d(x) \leq v(c(x))$
- (c)  $v(c(x)) \leq (d(|x|) - v(x))(a(x) - 1)$

où  $a(x)$  est le nombre de  $i$  tels que  $x_i \neq 0$ .

*Preuve de (a).* Posons  $v(x) = \beta$  et  $v(|x|) = \gamma$ . On a donc

$$h_\alpha(|x|) = 0 \text{ si } \alpha < \gamma, \quad |h_\alpha(x)| = 0 \text{ si } \alpha < \beta, \quad h_\gamma(|x|) \neq 0 \quad \text{et} \quad |h_\beta(x)| \neq 0.$$

Donc si  $\beta < \gamma$ ,  $q_\beta > 0$ . De même si  $\beta \leq t < \gamma$  et  $q_{t-1} > 0$  alors  $q_t > 0$ . Donc  $q_\beta, \dots, q_{\gamma-1} > 0$  et d'après le Théorème 1,  $\sum_{\alpha \geq 0} q_\alpha \geq \gamma - \beta$ .

*Preuve de (b).* Posons  $d(x) = \beta$  et  $d(|x|) = \gamma$ . On a donc

$$h_\alpha(|x|) = 0 \text{ si } \alpha > \gamma, \quad |h_\alpha(x)| = 0 \text{ si } \alpha > \beta, \quad h_\gamma(|x|) \neq 0 \quad \text{et} \quad |h_\beta(x)| \neq 0.$$

Donc si  $\beta < \gamma$ ,  $q_\gamma \geq 0$  entraîne  $q_{\gamma-1} \geq h_\gamma(|x|) > 0$ . De même si  $\beta < t \leq \gamma$  et  $q_t > 0$  alors  $q_{t-1} > 0$  car  $|h_t(x)| = 0$ . Donc  $q_\beta, q_{\beta+1}, \dots, q_{\gamma-1}$  sont  $> 0$  et  $\sum_{\alpha \geq 0} q_\alpha \geq \gamma - \beta$ .

*Preuve de (c).* Posons  $v(x) = \beta$  et  $d(|x|) = \gamma$ . On a donc

$$h_\alpha(|x|) = 0 \text{ si } \alpha > \gamma, \quad |h_\alpha(x)| = 0 \text{ si } \alpha < \beta, \quad h_\gamma(|x|) \neq 0 \quad \text{et} \quad |h_\beta(x)| \neq 0.$$

Donc  $q_t$  est nul si  $t < \beta$  ou  $t \geq \gamma$ . D'autre part

$$pq_\beta = |h_\beta(x)| - h_\beta(|x|) \leq a(x)(p - 1).$$

Donc  $q_\beta \leq a(x) - a(x)/p$ .

$x \neq 0$  entraîne  $a(x) \neq 0$  et  $q_\beta$  étant entier satisfait à  $q_\beta \leq a(x) - 1$ .  
On montre ensuite que  $q_t \leq a(x) - 1$  entraîne  $q_{t+1} \leq a(x) - 1$ . En effet

$$pq_{t+1} = q_t + |h_t(x)| - h_t(|x|) \leq a(x) - 1 + a(x)(p - 1)$$

Donc  $q_{t+1} \leq a(x) - 1/p$

On en déduit que

$$\sum_{\alpha \geq 0} q_\alpha \leq (\gamma - \beta)(a(x) - 1)$$

ce qui achève la preuve du Théorème 2.

## 2. La construction d'évènements de probabilité $1/m$

L'espace de probabilité  $(I, \mathfrak{C}, \pi)$  de l'introduction est tel que  $I$  soit fini ou dénombrable, que  $\mathfrak{C}$  soit la tribu la plus fine, et que  $\pi$  satisfasse à la condition:

$$(2) \quad \pi_i < 1 \quad \text{pour tout } i \text{ de } I$$

en plus de  $\sum_i \pi_i = 1$  et  $\pi_i \geq 0$ .

Soit  $m$  un entier positif fixé. On désigne par  $\mathfrak{A}_m$  l'ensemble des temps d'arrêt  $T$  par rapport aux  $(\mathfrak{F}_t)_{t \geq 0}$  tels que  $T$  soit p. s. fini pour tout  $\pi$  et qu'il existe une partition  $(A_1, \dots, A_m)$  de  $\Omega$ ,  $\mathfrak{F}_T$  mesurable et telle que  $P(A_1) = \dots = P(A_m) = 1/m$  pour tout  $\pi$  satisfaisant à (2). Notre but est de construire un élément de  $\mathfrak{A}_m$ , si possible avec  $E(T)$  pas trop grand.

Considérons l'ensemble des v.a.  $(y_t)_{t \geq 1}$  à valeurs dans  $\mathfrak{M}$  définies pour  $\Omega$  par

$$y_t(\omega) = \varepsilon^i \quad \text{si } a_t(\omega) = i.$$

Les  $y_t$  sont indépendantes et de même loi par construction. On désigne par  $S_t = y_1 + \dots + y_t$  (avec  $S_0 = 0$ ) la promenade aléatoire dans  $\mathfrak{M}$  associée. Notant  $\pi^x$  pour  $\prod \pi_i^x$ , il est facile de voir que

$$P(S_t = x) = c(x)\pi^x \quad \text{si } |x| = t \\ = 0 \quad \text{si } |x| \neq t.$$

Il est clair que si  $E \subset \mathfrak{M}$ , le temps de frappe de  $E$ ,

$$T(E) = \inf \{t : S_t \in E\},$$

est un temps d'arrêt par rapport aux  $(\mathfrak{F}_t)_{t \geq 1}$ .

(C'est en fait à cette classe de temps d'arrêt que nous nous limiterons. La restriction est d'importance, beaucoup d'éléments de  $\mathfrak{A}_m$  ne sont pas des temps de frappe.)

Si  $(S'_t)_{t \geq 0}$  désigne le processus stoppé, c'est-à-dire

$$S'_t = S_t \text{ si } t < T(E) \quad S'_t = S_{T(E)} \text{ si } t \geq T(E),$$

on définit  $m_E(x)$  dans  $\mathfrak{M}$  par

$$P(S'_t = x) = m_E(x)\pi^x \quad \text{où } t = |x|.$$

Il est clair que  $m_E(x)$  ne dépend pas de  $\pi$  mais seulement de  $E$ . La quantité

$m_E(x)$  s'interprète comme le nombre de chemins dans  $\mathfrak{M}$  allant de 0 à  $x$  et ne passant par aucun point de  $E \setminus \{x\}$ . (On appelle chemin de  $x$  à  $y$  dans  $\mathfrak{M}$  une suite  $x^0 = x, x^1, \dots, x^a = y$  telle qu'il existe  $i_t$  tel que  $x^t = x^{t-1} + \varepsilon^{i_t}$  pour tout  $t = 1, 2, \dots, a = |y - x|$ .)

La grande habileté de [2] est de remarquer que si  $m_E(x) \equiv 0 \pmod m$  pour tout point de  $E$ , on peut partager en  $m$  ensembles de même cardinalité les chemins de 0 à  $x$  ne touchant pas  $E$  et donc  $T(E) \in \mathfrak{A}_m$  dès que  $T(E) < \infty$  p.s. La caractérisation complète de ces ensembles  $E$  est donnée par le théorème suivant, que est essentiellement le théorème fondamental de [2]:

**THÉORÈME 3.** *Soit  $E \subset M$ . Alors les trois affirmations suivantes sont équivalentes:*

- (a)  $m_E(x) \equiv 0 \pmod m$  si  $x \in E$
- (b)  $c(x) \equiv 0 \pmod m$  si  $x \in E$
- (c)  $m_E(x) \equiv c(x) \pmod m$  pour tout  $x$  de  $\mathfrak{M}$ .

Avant de donner la preuve du Théorème 3, il est nécessaire de préciser la dépendance entre  $m_E(x)$  et  $E$ . On définit  $\theta(E) = \bigcap_i (\varepsilon^i + E)$ , puis  $\theta^2(E)$ , etc. On pose ensuite

$$\mathfrak{Y}(E) = \bigcup_{n \geq 1} \theta^n(E), \mathfrak{S}(E) = E \setminus \mathfrak{Y}(E) \quad \text{et} \quad \mathfrak{C}(E) = \mathfrak{M} \setminus (\mathfrak{S}(E) \cup \mathfrak{Y}(E)).$$

$\mathfrak{Y}(E)$  représente l'ensemble des points inaccessibles par  $S'_i$ ;  $\mathfrak{S}(E)$  représente l'ensemble des points de  $E$  accessibles par  $S'_i$ ;  $\mathfrak{C}(E)$  représente l'ensemble des points de continuation de  $S'_i$ .

Il est évident que les objets  $\mathfrak{Y}(E), \mathfrak{S}(E), \mathfrak{C}(E)$  et  $m_E(x)$  sont invariants si on remplace  $E$  par  $F$ , avec  $\mathfrak{S}(E) \subset F \subset \mathfrak{S}(E) \cup \mathfrak{Y}(E)$ . Convenons  $m_E(x) = 0$  si  $x \notin \mathfrak{M}$ . Alors  $m_E$  satisfait à l'identité dans  $\mathfrak{G}$ :

$$(3) \quad m_E(x) = \sum_i m_E(x - \varepsilon^i) \mathbf{1}_{\mathfrak{C}(E)}(x - \varepsilon^i) + \delta(x)$$

où  $\mathbf{1}_{\mathfrak{C}(E)}$  est l'indicatrice de  $\mathfrak{C}(E)$  dans  $\mathfrak{G}$  et  $\delta$  est l'indicatrice de 0. De plus à l'aide de l'identité dans  $\mathfrak{G}$ ,

$$(4) \quad c(x) = \sum_i c(x - \varepsilon^i) + \delta(x),$$

on établit facilement que

$$c(x) \equiv 0 \pmod m \quad \text{si } x \in E \text{ entraîne}$$

$$c(x) \equiv 0 \pmod m \quad \text{si } x \in F \text{ avec } \mathfrak{S}(E) \subset F \subset \mathfrak{S}(E) \cup \mathfrak{Y}(E).$$

*Preuve du Théorème 3.* Supposons (a) ou (b) et montrons par récurrence sur  $|x|$  que  $c(x) \equiv m_E(x) \pmod m$ . C'est vrai pour  $x = 0$ . Supposons le vrai pour tout  $x$  tel que  $|x| = n - 1$  et montrons le pour  $|x| = n$ . Puisque

$$c(x - \varepsilon_i) \equiv m_E(x - \varepsilon^i) \pmod m, \quad \forall i,$$

au vu de (3) et (4) on a

$$c(x) - m_E(x) \equiv \sum_i m_E(x - \varepsilon^i) \mathbf{1}_{\mathfrak{S}(E) \cup \mathfrak{Y}(E)}(x - \varepsilon^i) \equiv \sum_i c(x - \varepsilon^i) \mathbf{1}_{\mathfrak{S}(E) \cup \mathfrak{Y}(E)}(x - \varepsilon^i) \pmod m.$$

Si (a) est vrai, les termes du second membre sont congrus à zéro. Si (b) est vrai, il en est de même pour le 3ème membre.

Supposons (c). Montrons que (a) est vrai. Sinon il existe  $x$  tel que  $m_E(x) \not\equiv 0 \pmod{m}$  si  $x \in E$ . En particulier,  $i$  étant fixé dans  $I$  de façon quelconque, on peut trouver  $x \in \mathfrak{S}(E)$  tel que

$$m_E(x) \not\equiv 0 \pmod{m} \quad \text{et} \quad m_E(x + \varepsilon^i - \varepsilon^j) \equiv 0 \pmod{m} \quad \text{pour tout } j \neq 1.$$

Alors en utilisant (3) et (4),

$$\begin{aligned} m_E(x + \varepsilon^i) &\equiv c(x + \varepsilon^i) = \sum_j c(x + \varepsilon^i - \varepsilon^j) \\ &\equiv m_E(x) + \sum_{j \neq i} m_E(x + \varepsilon^i - \varepsilon^j) \equiv m_E(x) \pmod{m}. \end{aligned}$$

D'autre part

$$\begin{aligned} m_E(x + \varepsilon^i) &\equiv \sum_j m_E(x + \varepsilon^i - \varepsilon^j) \mathbf{1}_{\mathfrak{S}(E)}(x + \varepsilon^i - \varepsilon^j) \\ &\equiv m_E(x) \mathbf{1}_{\mathfrak{S}(E)}(x) \equiv 0 \pmod{m}. \end{aligned}$$

D'où la contradiction. Il est clair enfin que (c) et (a) entraînent (b).

**THÉORÈME 4.** *Si  $H_m = \{x \in \mathfrak{M}; c(x) \equiv 0 \pmod{m}\}$  alors  $T(H_m) \in \mathfrak{A}_m$ .*

*Preuve.* D'après le Théorème 3,  $m_{H_m}(x) \equiv 0 \pmod{m}$ . Nous avons seulement à démontrer que  $T(H_m) < \infty$  p. s., quel que soit  $\pi$  satisfaisant à (2). Soit donc  $i$  et  $j$  distincts tels que  $\pi_i > 0$  et  $\pi_j > 0$ . Posons

$$F_{i,j} = \{x; x_i \equiv 1 \text{ et } x_j \equiv -1 \pmod{m}\}$$

Soit  $\Gamma$  le groupe  $(Z/mZ)^2$ . On définit l'homomorphisme  $a$  de  $\mathfrak{G}$  dans  $\Gamma$  par

$$a(x) = (x_i \pmod{m}, x_j \pmod{m}).$$

Alors  $a(S_t) = a(y_1) + \dots + a(y_t)$  où

$$P(a(y_t) = (1, 0)) = \pi_i, \quad P(a(y_t) = (0, 1)) = \pi_j,$$

$$P(a(y_t) = (0, 0)) = 1 - \pi_i - \pi_j$$

et

$$T(F_{ij}) = \inf \{t : a(S_t) = (1, -1)\}.$$

Puisque  $\pi_i$  et  $\pi_j \neq 0$ , la promenade aléatoire  $a(S_t)$  sur le groupe fini  $\Gamma$  n'a qu'une seule classe et est donc récurrente [7].

Donc  $T(F_{ij}) < \infty$  p. s. et est d'espérance finie.

Reste à montrer que  $F_{ij} \subset H_m$ . Si  $x \in F_{ij}$ , le coefficient

$$c(x) = |x|! / \prod_{k \neq i, k \neq j} x_k! x_i! x_j!$$

est toujours un multiple de  $c(x_i, x_j) = (x_i + x_j)! / x_i! x_j!$ . Prenons  $x \in F_{ij}$ ; posons  $x_i = am + 1$  et  $x_j = bm - 1$  (avec  $a \geq 0$  et  $b > 0$ ). Soit  $p$  un nombre premier quelconque divisant  $m$ . Il faut montrer que

$$v(c(am + 1, bm - 1)) \geq v(m).$$

Posant  $m = hp^k$ , avec  $k = v(m) > 0$ , on a à l'aide de la formule (1):

$$(p - 1)v(am + 1, bm - 1) = \|ahp^k + 1\| + \|bhp^k - 1\| - \|ah + bh\|.$$

Mais il est facile de constater, d'après la proposition 1, que

$$\begin{aligned} \|ahp^k + 1\| &= 1 + \|ah\| \quad \text{et} \quad \|bhp^k - 1\| = (p - 1)k + \|bh - 1\|. \\ v(c(am + 1, bm - 1)) &= k + (1/(p - 1))(\|ah\| + 1 + \|bh - 1\| - \|ah + bh\|). \end{aligned}$$

D'après la Proposition 1(e),

$$\|ah + bh\| \leq \|ah\| + \|bh - 1\| + \|1\|$$

ce qui achève la preuve du Théorème 4.

### 3. La loi de $T(H_m)$ si $m$ est premier

Dans tout ce paragraphe, on suppose que  $m$  est un nombre premier  $p$ . Pour simplifier, on posera  $m_{\pi_m}(x) = m(x)$ ,  $\mathfrak{C}(H_m) = \mathfrak{C}$  etc. Il est évident que

$$(5) \quad P(T(H_p) > t) = \sum_{x:|x|=t} m(x)\mathbf{1}_{\mathfrak{C}}(x)\pi^x.$$

Pour connaître la loi de  $T(H_p)$ , il est nécessaire de connaître  $m(x)\mathbf{1}_{\mathfrak{C}}(x)$ : c'est le théorème suivant.

**THÉORÈME 5.** *Si  $x \in \mathfrak{C}$ , alors  $m(x) = \prod_{\alpha \geq 0} c(h_\alpha(x))$ .*

Le lemme suivant est essentiel.

**LEMME 1.** *Soit  $x \in \mathfrak{M}$  tel que  $|x| = qp^n$  avec  $q < p$ , et  $n \geq 0$ . Alors  $x \in \mathfrak{C}$  si et seulement si il existe  $y \in \mathfrak{M}$  tel que  $x = yp^n$ .*

Remarquons qu'ici  $d(|x|) = v(|x|) = n$ .

En utilisant la partie (a) du Théorème 2, on voit que  $x \in \mathfrak{C}$  entraîne  $v(x) = n$ , ce qui est le résultat demandé. En utilisant la partie (c) du Théorème 2, on voit que  $v(x) = n$  entraîne  $v(c(x)) = 0$ , ce qui démontre le lemme.

On va d'abord démontrer le théorème dans le cas où  $|x| = qp^n$ , avec  $q < p$ . D'après le Lemme 1,  $x = yp^n$  avec  $|y| < p$ . Remarquons que si  $n \in \mathfrak{M}$  et  $|u| < p - 1$ , alors

$$up^n + t\varepsilon^i \in \mathfrak{C} \quad \text{si } 0 \leq t < p^n \text{ et } i \in I.$$

En effet

$$(p - 1)v(c(up^n + t\varepsilon^i)) = \|u_i p^n + t\| + \sum_{j \neq i} \|u_j\| - \| |u| p^n + t \|.$$

D'après la Proposition 1,

$$\|u_i p^n + t\| = \|u_i\| + \|t\|, \quad \| |u| p^n + t \| = \|u\| + \|t\|.$$

Donc  $v(c(up^n + t\varepsilon^i)) = v(c(u))$ , c'est-à-dire zéro d'après le Lemme 1. II

y a donc un et un seul chemin entièrement situé dans  $\mathbb{C}$  entre  $up^n$  et  $(u + \varepsilon^i)p^n$  si  $|u| < p - 1$ . Comme d'après le Lemme 1 tous les points de la forme  $up^n$  appartiennent à  $\mathbb{C}$  avec  $|u| < p$ , le nombre de chemins dans  $\mathbb{C}$  de 0 à  $yp^n$  est  $c(y)$ , ce qui établit le théorème dans ce cas particulier.

Montrons ensuite que si  $x \in \mathbb{C}$ , donc si  $|h_\alpha(x)| < p$  pour tout  $\alpha \geq 0$ , (d'après le corollaire du Théorème 1) alors

$$(6) \quad m(x) = m(h_n(x)p^n)m(x - h_n(x)p^n) \quad \text{si } n = d(|x|).$$

En effet, tout chemin de 0 à  $x$  entièrement dans  $\mathbb{C}$  passe par le point  $h_n(x)p^n$ . Car si  $|h_n(x)| = q$ , le  $qp^n$  ième point du chemin est, d'après le Lemme 1, de la forme  $yp^n$ . Si  $y \neq h_n(x)$ , puisque  $|y| = q$  il existe  $i$  tel que  $y_i > h_n(x_i)$ . Comme  $n \geq d(x_i)$  il est impossible qu'un chemin passant par  $yp^n$  passe par  $x$ . Donc  $y = h_n(x)$ .

Reste à montrer que le nombre de chemins de  $h_n(x)p^n$  à  $x$  dans  $\mathbb{C}$  est  $m(x - h_n(x)p^n)$ . Il suffit d'observer que  $v(c(h_n(x)p^n + y)) = v(c(y))$  si  $|y| < p^n$ . Ceci démontre (6).

Comme  $m(h_n(x)p^n) = c(h_n(x))$  on déduit facilement le théorème par une récurrence sur  $n$ .

**COROLLAIRE 1** (Lucas [6]).  $c(x) \equiv \prod_{\alpha \geq 0} c(h_\alpha(x)) \pmod p$ .

Si  $x \in \mathfrak{S} \cup \mathfrak{J}$ , c'est le corollaire du Théorème 1. Si  $x \in \mathbb{C}$  il suffit de comparer les Théorèmes 3(c) et 5.

**COROLLAIRE 2.** Posant  $U_n(X) = \sum_i X_i^{p^n}$ ,

$$\sum_x m(x) \mathbf{1}_{\mathbb{C}}(x) X^x = \prod_{n=0}^{\infty} \frac{1 - (U_n(X))^p}{1 - U_n(X)}.$$

Le calcul est standard à partir du Théorème 5.

**COROLLAIRE 3.**

$$\sum_x m(x) X^x = 1 + U_0(X) \prod_{n=0}^{\infty} \frac{1 - (U_n(X))^p}{1 - U_n(X)}.$$

Ceci est la conséquence immédiate du Corollaire 2 et de la formule 4. Remarquons qu'on n'a pas d'autre expression explicite de  $m(x)$  si  $x \in \mathfrak{S}$ .

A partir du Corollaire 2, on peut avoir une expression des moments de  $T(H_p)$ , en particulier pour le premier.

**COROLLAIRE 4.**

$$E(T(H_p)) = p \prod_{n=1}^{\infty} \frac{1 - (U_n(\pi))^p}{1 - U_n(\pi)}.$$

*Preuve.*  $E(T(H_p)) = \sum_{t \geq 0} P(T(H_p) > t)$  et on utilise la relation (5) et le Corollaire 2.

*Remarques.* 1° Le facteur  $p$  est en évidence: il est facile de constater que  $T(H_p) \equiv 0 \pmod p$ , c'est-à-dire que  $x \in \mathfrak{S}$  entraîne  $|x| = 0 \pmod p$ . En effet

$x \in \mathfrak{C}$  entraîne qu'il existe  $i$  tel que  $x - \varepsilon^i \in \mathfrak{C}$ . Donc  $c(x - \varepsilon^i) \not\equiv 0$  et  $c(x) \equiv 0 \pmod p$ . Or  $x_i c(x) = |x| c(x - x_i)$ , ce qui entraîne le résultat.

2° Si  $J \subset I$ , il est clair que  $\sum_{i \in J} \pi_i^{p^n} \leq (\sum_{i \in J} \pi_i)^{p^n}$ . On obtiendrait donc un  $E(T)$  plus grand en prenant sur  $I$  une tribu moins fine, ce qui justifie, à posteriori, que nous passions de  $I$  à 2 éléments à un  $I$  plus grand.

3° On constate aisément que  $E(T(H_p))/p \rightarrow 1$  si  $p \rightarrow \infty$ . Ceci montre tout l'intérêt qu'on a à travailler avec  $H_p$ . En effet, il est clair qu'on peut fabriquer un élément de  $\mathfrak{A}_p^k$  en répétant  $k$  fois une procédure de  $\mathfrak{A}_p$ . D'autre part, il est facile de constater, à l'aide du Théorème 2(c), que si  $I$  a 2 éléments,  $T(H_{p^k}) \geq p^k$ , et donc que  $E(T(H_{p^k})) \geq p^k$  ce qui, si  $p$  est grand, est largement supérieur à  $kE(T(H_p))$  qui est équivalent à  $kp$ . La relation entre  $E(T(H_{p^k}))$  et  $E(T(H_p))$  reste un mystère. On aimerait toujours avoir  $E(T(H_{p^k})) \geq kE(T(H_p))$ . C'est malheureusement faux; pour  $k = 2$ ,  $p = 2$  et  $\pi = (\frac{1}{2}, \frac{1}{2})$ , ces deux nombres sont alors égaux approximativement à 6,2 et 6,8.

#### 4. Un théorème sur $H_{p^n}$

On peut faire diverses constatations sur examen du Tableau 1. Beaucoup dérivent de la simple identité

$$v(c(x + y)) = v(c(x)) + v(c(y)) \quad \text{si } v(x) > d(|y|)$$

que nous généraliserons au Théorème 6. La constatation la plus intéressante est que si  $x \in H_{p^n}$  alors non seulement  $p^k x \in H_{p^n}$ , mais aussi tout le "triangle" des  $p^k x + y$ , avec  $y \in \mathfrak{G}$ ,  $|y| \geq 0$  et  $|y_i| < p^k$  est contenu dans  $H_{p^n}$ . Nous le démontrons au Théorème 7, en conséquence du théorème 6.

**THÉORÈME 6.** Soit  $\eta = (\eta_i)_{i \in I}$  tel que  $\eta_i = \pm 1$ . Si  $y \in \mathfrak{M}$  on note  $\eta y$  l'élément de  $\mathfrak{G}$  défini par  $(\eta y)_i = \eta_i y_i$ . Alors, si  $v(x_i) > d(y_i)$  pour tout  $i$  et si  $|y| \geq 0$ , on a

$$\begin{aligned} & (p - 1)(v(c(x + \eta y)) - v(x)) \\ &= (p - 1) \sum_i \frac{1}{2} (1 - \eta_i) (v(x_i) - v(y_i) + \sum_i \eta_i \|y_i\| + \|x\| - \|x + \eta y\|). \end{aligned}$$

Les conditions  $v(x_i) > d(y_i)$  et  $|y| \geq 0$  garantissent évidemment  $x + \eta y \in \mathfrak{M}$ . Si  $\eta_i = 1$ ,  $d(y_i) < v(x_i)$  entraîne  $\|x_i + \eta_i y_i\| = \|x_i\| + \|y_i\|$ . Si  $\eta_i = -1$ , alors

$$x_i - y_i = (x_i - p^{v(x_i)}) + (p^{v(x_i)} - y_i),$$

d'où

$$\|x_i + \eta_i y_i\| = \|x_i - p^{v(x_i)}\| + \|p^{v(x_i)} - y_i\|.$$

Or il est facile de voir que  $h_\alpha(p^{v(x_i)} - y_i) + h_\alpha(y_i)$  est nul si  $\alpha < v(y_i)$  ou  $\alpha \geq v(x_i)$ , égal à  $p$  si  $\alpha = v(y_i)$  et égal à  $p - 1$  si  $v(y_i) < \alpha < v(x_i)$ . Donc

$$\|p^{v(x_i)} - y_i\| = (v(x_i) - v(y_i))(p - 1) - \|y_i\| + 1.$$

On en déduit que si  $\eta_i = -1$ ,

$$\|x_i + \eta_i y_i\| = (v(x_i) - v(y_i))(p - 1) + \|x_i\| - \|y_i\|,$$

ce qui, compte tenu de l'identité (1), achève la preuve du Théorème 6.

**THÉORÈME 7.** *Sans les hypothèses du Théorème 6, on a*

$$v(c(x + \eta y)) \geq v(c(x)).$$

On commence par l'établir pour  $|\eta y| = 0$ . Dans ce cas

$$\begin{aligned} & v(c(x + \eta y)) - v(c(x)) \\ &= \sum_i \frac{1}{2}(1 - \eta_i) \|y_i\| + \sum_i \frac{1}{2}(1 - \eta_i)(v(x_i) - v(y_i) - \|y_i\|/(p - 1)) \end{aligned}$$

Or d'après la Proposition 1(b), on a

$$\|y_i\| \leq (d(y_i) + 1 - v(y_i))(p - 1) \leq (v(x_i) - v(y_i))(p - 1).$$

Chaque terme du second membre de l'égalité précédente est donc positif ou nul. Si  $|\eta y| > 0$ , on procède par récurrence à l'aide de la formule (4):

$$\begin{aligned} c(x + \eta y) &= \sum_i c(x + \eta y - \varepsilon^i), \\ v(c(x + \eta y)) &\geq \inf_i v(c(x + \eta y - \varepsilon^i)). \end{aligned}$$

Or  $|\eta y| > 0$  entraîne  $|\eta y - \varepsilon^i| \geq 0$  et  $d(y_i - 1) \leq d(y_i) < v(x_i)$ . Donc par hypothèse de récurrence  $v(c(x + \eta y - \varepsilon^i)) \geq v(c(x))$ .

Le Théorème 7 est donc établi.

### 5. La limite $p$ -adique de $c(x + p^n \varepsilon^i)$ est $c(x)$

Si on considère le Tableau 2, on constate que les nombres du rectangle  $x_1 < 4$  et  $x_2 < 16$  se reproduisent si on fait glisser ce rectangle le long de l'axe  $x_2$ . Nous allons le prouver au Théorème 8, qui nécessite la proposition suivante.

**PROPOSITION 2.** *Si  $I$  et  $J$  sont deux ensembles quelconques,  $\mathfrak{M}_I$ ,  $\mathfrak{M}_J$  et  $\mathfrak{M}_{I \times J}$  sont les monoïdes libres engendrés par  $I$ ,  $J$  et  $I \times J$ . Si  $x \in \mathfrak{M}_I$  et  $y \in \mathfrak{M}_J$ , avec  $|x| = |y|$ , alors  $c(x)c(y) = \sum c(z)$ , où la somme est prise pour tous les  $z = (z_{ij})$  de  $\mathfrak{M}_{I \times J}$  de marges  $x$  et  $y$ , c'est-à-dire tels que  $\sum_j z_{ij} = x_i$  et  $\sum_i z_{ij} = y_j$ .*

*Preuve.* Posons  $N = |x| = |y|$ . Si  $(X_i)_{i \in I}$  et  $(Y_j)_{j \in J}$  sont des variables formelles on a  $\sum_x c(x)X^x = (\sum X_i)^N$  si la somme est prise pour tous les  $x \in \mathfrak{M}_I$  tels que  $|x| = N$ . De même  $\sum_y c(y)Y^y = (\sum Y_j)^N$ . Donc

$$(\sum_x c(x)X^x)(\sum_y c(y)Y^y) = (\sum_{i,j} X_i Y_j)^N = \sum_z c(z) \prod_{ij} (X_i Y_j)^{z_{ij}},$$

la dernière somme étant prise pour tous les  $z$  de  $\mathfrak{M}_{I \times J}$  tels que  $|z| = N$ .

Cette identité achève la preuve de la Proposition 2.

Mentionnons ici un résultat intéressant.

**COROLLAIRE.** *Soit  $m(x, y)$  le nombre de matrices à coefficients 0 ou 1 de*

marges  $x$  et  $y$ ,  $M(x, y)$  le nombre de matrices à coefficients entiers non négatifs de marges  $x$  et  $y$ . Alors si  $N = |x| = |y|$ ,

$$m(x, y) \leq c(x)c(y)/N! \leq M(x, y).$$

Le preuve de la première égalité est immédiate en remarquant que si  $z \in \mathfrak{M}_{I \times J}$  correspond à une matrice à coefficients 0 ou 1 telle que  $|z| = N$  alors  $c(z)/N! = 1$ .

Pour la deuxième inégalité, on utilise  $c(z)/N! \leq 1$  si  $|z| = N$ .

**THÉORÈME 8.** Soit  $i$  fixé dans  $I$  et  $x \in \mathfrak{M}$  tel que  $x_i = 0$ . Alors

$$v(c(x + t\varepsilon^i) - c(x + (t + p^n)\varepsilon^i)) \geq n - d(x) \text{ pour tout } t \geq 0.$$

*Preuve.* Si  $a$  et  $b$  sont des entiers, posons

$$\begin{aligned} c(a, b) &= (a + b)!/a!b! \text{ si } a \geq 0 \text{ et } b \geq 0 \\ &= 0 \text{ sinon.} \end{aligned}$$

On a alors  $c(x + t\varepsilon^i) = c(x)c(|x|, t)$ . Par application de la proposition précédente,

$$\begin{aligned} (7) \quad c(x + (t + p^n)\varepsilon^i) - c(x + t\varepsilon^i) & \\ &= c(x)(c(|x|, t + p^n) - c(|x|, t)) \\ &= \sum_{k>0} c(|x| - k, |t| + k) \cdot c(x) \cdot c(k, p^n - k). \end{aligned}$$

Les termes de cette somme sont nuls si  $k > \min(p^n, |x|)$ . Si  $0 < k \leq p^n$ ,

$$\min(v(k), v(p^n - k)) = v(k)$$

et, par application du Théorème 2(a)

$$v(c(k, p^n - k)) \geq n - v(k).$$

Si  $0 < k \leq |x|$ ,  $v(k) \leq d(|x|)$  et d'après le Théorème 2(b)

$$v(c(x)) \geq d(|x|) - d(x).$$

Donc si  $0 < k \leq \min(p^n, |x|)$

$$v(c(x)c(k, p^n - k)) \geq n - d(x) + d(|x|) - v(k) \geq n - d(x).$$

En utilisant (7), on a le théorème.

**COROLLAIRE.** Si  $x \in \mathfrak{M}$  et  $i \in I$ , la limite  $p$ -adique de  $c(x + \varepsilon^i p^n)$  si  $n \rightarrow +\infty$  existe et est égale à  $c(x)$ .

### 6. La limite $p$ -adique de $c(p^n x)$ existe

**THÉORÈME 9.** Soit  $x \in \mathfrak{M}$ ,  $x \neq 0$  et  $n \geq 0$ . Alors

$$v(c(p^n x) - c(p^{n-1} x)) \geq n + v(x) + v(c(x)).$$

LEMME 2. Soit  $a$  un entier positif. Alors  $((pa)!/a!)p^{-a}$  est égal au produit des entiers positifs inférieurs à  $pa$  et non divisibles par  $p$ .

*Preuve.* Immédiate par récurrence sur  $a$ .

On définit ensuite pour tout  $k$  premier avec  $p$  le nombre

$$r_n(k) = (p^n k)! p^{-v((p^n k)!)}$$

LEMME 3. Si  $p > 2$  et  $n > 0$  on a

$$r_n(k) \equiv (-1)^k r_{n-1}(k) \pmod{p^n}$$

Si  $p^n = 4$  on a

$$r_2(k) \equiv -r_1(k) \pmod{4}$$

Si  $p = 2$  et  $n \neq 2$  on a

$$r_n(k) \equiv r_{n-1}(k) \pmod{2^n}.$$

*Preuve.* D'après le Lemme 2 et la Proposition 1(d);  $r_n(k)/r_{n-1}(k) = A(p^n k)$ , où  $A(p^n k)$  est le produit des entiers compris entre 1 et  $p^n k$  et premiers avec  $p$ . De plus il est facile de constater que

$$A(p^n k) \equiv (A(p^n))^k \pmod{p^n}.$$

Or, d'après le théorème de Wilson généralisé [6], on sait que

$$A(p^n) \equiv -1 \pmod{p^n} \quad \text{si } p > 2 \text{ ou si } p^n = 4,$$

et

$$A(2^n) \equiv +1 \pmod{2^n} \quad \text{si } n \neq 2.$$

Compte tenu du fait que  $k$  est impair si  $p = 2$ , on a le Lemme 3.

*Preuve du Théorème 9.* Rappelons que  $v(c(p^n x)) = v(c(x))$  pour tout  $n$ . On a donc

$$(8) \quad c(p^n x) p^{-v(c(x))} = \frac{r_{n+v(|x|)}(|x| p^{-v(|x|)})}{\prod_i r_{n+v(x_i)}(x_i p^{-v(x_i)})}$$

Nous distinguons ensuite les trois cas du Lemme 3.

$p > 2$ . Compte tenu du fait qu'une congruence valable modulo  $p^{n+v(x_i)}$  ou  $p^{n+v(|x|)}$  est valable modulo  $p^{n+v(x)}$ , on a

$$c(p^n x) \equiv c(p^{n-1} x) (-1)^\alpha \pmod{p^\beta}$$

où

$$\beta = n + v(x) + v(|x|) \quad \text{et} \quad \alpha = |x| p^{-v(|x|)} - \sum_i x_i p^{-v(x_i)}$$

d'après (8) et le Lemme 3. Mais  $p$  étant impair, il est clair que  $x_i p^{-v(x_i)}$  et  $x_i$  ont même parité; comme  $\sum_i x_i = |x|$ , on a donc  $\alpha \equiv 0 \pmod{2}$ , ce qui achève la preuve.

$p^{n+v(x)} = 4$ . Dans ce cas

$$r_{n+v(x_i)}(x_i p^{-v(x_i)}) \equiv \varepsilon r_{n+v(x_i)-1}(x_i p^{-v(x_i)}) \pmod{4}$$

où  $\varepsilon = -1$  si  $v(x_i) = v(x)$ , et  $\varepsilon = 1$  si  $v(x_i) > v(x)$ ; autrement dit  $\varepsilon = (-1)^{x_i 2^{-v(x)}}$ . Donc

$$c(2^n x) \equiv c(2^{n-1} x) (-1)^\alpha \pmod{2^\beta}$$

où

$$\beta = 2 + v(c(x)) + v(x) \quad \text{et} \quad \alpha = |x| 2^{-v(x)} - \sum_i x_i 2^{-v(x)}.$$

Cet  $\alpha$  étant nul, la preuve est faite.

$p = 2, n + v(x) \neq 2$ . Le Lemme 3 et (8) donnent directement la preuve du théorème.

**COROLLAIRE.** *Si  $x \in \mathfrak{M}$ , la limite  $p$ -adique de  $c(p^n x)$  si  $n \rightarrow +\infty$  existe.*

Si  $x \in \mathfrak{M}$ , désignons par  $L(x)$  l'entier  $p$ -adique égal à la limite de  $c(p^n x)$  si  $n \rightarrow +\infty$ .

Voici pour terminer une propriété de cette limite qui complète la Proposition 2. (Les notations sont celles de cette Proposition 2.)

**THÉORÈME 10.** *Soient  $x \in \mathfrak{M}_I, y \in \mathfrak{M}_J$  tels que  $|x| = |y|$  et*

$$\inf(v(x), v(y)) = 0.$$

*Alors  $L(x)L(y) = \sum_z L(z)$ , où la somme est prise pour tous les  $z$  de  $\mathfrak{M}_{I \times J}$  de marges  $p^k x$  et  $p^k y$  pour un certain  $k \geq 0$ , et tels que  $v(z) = 0$ .*

*Remarque.* La restriction  $\inf(v(x), v(y)) = 0$  n'est là que pour simplifier l'énoncé, puisque  $L(px) = L(x)$ .

*Preuve du théorème.* Soit  $A_k$  l'ensemble des  $z$  de  $\mathfrak{M}_{I \times J}$  de marges  $p^k x$  et  $p^k y$  et tels que  $v(z) = 0$ . Alors, d'après la Proposition 2,

$$(9) \quad c(p^n x)c(p^n y) = \sum_{k=0}^n \sum_{z \in A_k} c(p^{n-k} z).$$

D'après le Théorème 2(a),  $z \in A_k$  entraîne

$$(10) \quad v(c(z)) \geq k + v(|x|).$$

Donc si  $n < k$  et  $z \in A_k$  on a  $L(z) \equiv 0 \pmod{p^n}$ , ce qui garantit la convergence de la série de terme général  $\sum_{z \in A_k} L(z)$ .

Si  $n \geq k$  et  $z \in A_k$ , d'après le Théorème 9,

$$L(z) \equiv c(p^{n-k} z) \pmod{p^\alpha}$$

où  $\alpha = n - k + 1 + v(c(z))$ .

D'après (10) on a  $\alpha > n$  et donc

$$\sum_{k=0}^n \sum_{z \in A_k} c(p^{n-k} z) \equiv \sum_{k=0}^\infty \sum_{z \in A_k} L(z) \pmod{p^n}.$$

Cette égalité, jointe à (9), démontre le théorème.

**BIBLIOGRAPHIE**

1. J. VON NEUMANN, *Various techniques used in connection with random digits, Monte-Carlo Method*, Applied Mathematics Series N°12.36-38. U.S. National Bureau of Standards, 1951.

2. W. Hoeffding and G. Simons, *Unbiased coin tossing with a biased coin*, Ann. Math. Statist., vol. 41 (1970), pp. 341–352.
3. R. D. Fray, *Congruences properties of ordinary and  $q$ . binomial coefficients*. Duke Math. J., vol. 34 (1967), pp. 469–480.
4. H. J. Ryser, *Combinatorial mathematics*, Wiley, New York, 1963.
5. G. Bachman, *Introduction to  $p$ -adic numbers and valuation theory*, Academic Press, New York, 1964.
6. L. E. Dickson, *History of the theory of numbers*, vol. 1., G. E. Stechert, New York, 1934.
7. W. Feller, *An introduction to probability theory and its applications*, 2<sup>d</sup> edition, vol. 1, Wiley, 1957.

UNIVERSITÉ DE CLERMONT  
CLERMONT-FERRAND, FRANCE