Indag. Mathem., N.S., 7 (2), 129–135 June 17, 1996

Distribution des coefficients multinomiaux et q-binomiaux modulo p

par Dominique Barbolosi* et Peter J. Grabner**

Université Aix-Marseille III, Faculté des Sciences et Technique de St. Jerôme, URA-CNRS 225 (équipe DSA), Case 322, Avenue Escadrille Normandie Niemen, 13013 Marseille, France
Institut für Mathematik A, Technische Universität Graz, Steyrergasse 30, 8010 Graz, Austria

Communicated by Prof. R. Tijdeman at the meeting of May 29, 1995

ABSTRACT

We study the distribution of binomial and multinomial coefficients in the residue classes modulo a prime. It is well known that 'most of the' binomial coefficients are in the 0 residue class; we consider the distribution of the remaining values in the non-0 residue classes. Finally, we use similar methods to study Gaussian binomial coefficients modulo an irreducible polynomial over a finite field.

1. INTRODUCTION

Dans toute la suite, p désignera un nombre premier. Il est bien connu que la densité asymptotique des coefficients multinomiaux divisibles par p est 1 (voir [Si]). Dans cet article, nous étudions la distribution des coefficients multinomiaux dont la classe résiduelle est a modulo p. Dans la première partie nous établissons que

$$(1)\qquad \left\{ \#\left\{ (n,k_1,\dots,k_r) \,\middle|\, 0 \le n < N, k_1+\cdots+k_r = n, \binom{n}{k_1,\dots,k_r} \not\equiv 0 \bmod p \right\} = N^{\alpha} F_{p,r}(\log_p N) \right.$$

* Partiellement subventionné par URA-CNRS 225.
** Auteur subventionné par la bourse Schrödinger No. J00936-PHY de la Fondation Autrichienne pour la Recherche.

où $F_{p,r}$ est une fonction continue, dérivable presque partout et $\alpha = \log_p \binom{p+r-1}{p-1}$. Cette formule a été établie pour $r = 2$ par Stein [St] où se trouve aussi que $\max_x F_{p,2}(x) = 1$ et un algorithme pour calculer $\min_x F_{p,2}(x)$ numériquement. Plus précisément, nous prouvons que, pour un $\varepsilon > 0$ bien déterminé,

$$(2) \qquad \begin{cases} \#\left\{(n,k_1,\ldots,k_r) \mid 0 \le n < N, k_1 + \cdots + k_r = n, \right. \\ \qquad \left. \binom{n}{k_1,\ldots,k_r} \equiv a \bmod p \right\} = \dfrac{1}{p-1} N^{\alpha} F_{p,r}(\log_p N) + O(N^{\alpha-\varepsilon}) \end{cases}$$

pour $a \not\equiv 0 \bmod p$. En d'autres termes, les coefficients multinomiaux non congrus à 0 sont équirépartis dans les classes résiduelles.

Dans la deuxième partie nous obtenons un résultat analogue pour les coefficients binomiaux gaussiens (cf. def. § 3) modulo un polynôme irréductible sur le corps fini $\mathbb{F}_p$. Plus précisément, on a:

$$(3) \qquad \begin{cases} \#\left\{(n,k) \mid 0 \le n < N, k \le n, \begin{bmatrix} n \\ k \end{bmatrix}_x \not\equiv 0 \bmod Q(x)\right\} \\ \quad = N^{\beta} G_{p,Q}(\log_p N) + o(N^{\beta}), \end{cases}$$

avec $\beta = \log_p \binom{p+1}{2}$ et $G_{p,Q}$ une fonction continue et dérivable presque partout. En plus nous établissons pour un polynôme a sur $\mathbb{F}_p$

$$(4) \qquad \begin{cases} \#\left\{(n,k) \mid n < N \begin{bmatrix} n \\ k \end{bmatrix}_x \equiv a(x) \bmod Q(x)\right\} \\ \quad = C(a) N^{\beta} G_{p,Q}(\log_p N) + o(N^{\beta}) \end{cases}$$

avec une expression explicite pour $C(a)$.

Nous notons ici que Fray, dans [Fr], considère des coefficients q-binomiaux mod p pour un q rationnel avec $\nu_p(q) = 0$ (ν_p étant la valuation p-adique).

2. LE CAS DES COEFFICIENTS MULTINOMIAUX

Proposition 1. *Soit n un entier naturel, $n = \sum_{l=0}^{L} \varepsilon_l p^l$; notons $s_i(n)$, pour chaque entier i entre 1 et $p-1$, le nombre des chiffres i dans la décomposition p-adique de n. On a alors:*

$$(5) \qquad \begin{cases} \#\left\{(h_1,\ldots,h_r) \mid \binom{n}{h_1,\ldots,h_r} \equiv a \bmod p\right\} \\ \quad = \dfrac{1}{p-1} \sum_{\chi} \bar{\chi}(a) \left(\sum_{\delta_1 + \cdots + \delta_r = 1} \chi\binom{1}{\delta_1,\ldots,\delta_r} \right)^{s_1(n)} \\ \qquad \cdots \left(\sum_{\delta_1 + \cdots + \delta_r = p-1} \chi\binom{p-1}{\delta_1,\ldots,\delta_r} \right) \end{cases}$$

où la somme est étendue sur tous les caractères χ de $\mathbb{F}_p^*$. Les formules (1) *et* (2) *résultent aisément de* (4).

Remarque. Pour $p = 2$ ou 3 et $r = 2$ la Proposition 1 permet de retrouver les résultats

$$\#\left\{k \mid \binom{n}{k} \equiv 1 \bmod 2\right\} = 2^{s_1(n)} \quad \text{(classique)}$$

$$\#\left\{k \mid \binom{n}{k} \equiv 1 \bmod 3\right\} = \frac{1}{2} 2^{s_1(n)} \quad (3^{s_2(n)} + 1)$$

$$\#\left\{k \mid \binom{n}{k} \equiv 2 \bmod 3\right\} = \frac{1}{2} 2^{s_1(n)} \quad (3^{s_2(n)} - 1).$$

Notons que Wolfram, dans [Wo], donne une formule fausse pour

$$\#\left\{k \mid \binom{n}{k} \not\equiv 0 \bmod 3\right\}$$

qui est en fait égal à $2^{s_1(n)} 3^{s_2(n)}$.
En plus, mentionnons que Stein [St] donne la formule

$$\#\left\{k \mid \binom{n}{k} \not\equiv 0 \bmod p\right\} = \prod_{\ell=1}^{p-1} (\ell + 1)^{s_\ell(n)}$$

et trouve (1) pour $r = 2$, en utilisant une méthode différente. Dans [Ho1], Howard montre

$$\#\left\{(k_1, \ldots, k_r) \mid \binom{n}{k_1, \ldots, k_r} \not\equiv 0 \bmod p\right\} = \prod_{\ell=1}^{p-1} \binom{\ell + r - 1}{\ell}^{s_\ell(n)}$$

et dans [Ho2], il trouve une formule plus compliquée pour (5).

Démonstration. Posons pour chaque i entre 1 et r, $h_i = \sum_{\ell=0}^{L} \varepsilon_\ell^{(i)} p^\ell$. On a, pour la valuation p-adique,

$$\nu_p\binom{n}{h_1, \ldots, h_r} = 0 \Longleftrightarrow \forall \ell : \varepsilon_\ell^{(1)} + \cdots + \varepsilon_\ell^{(r)} = \varepsilon_\ell,$$

cela étant une conséquence immédiate de la formule de Legendre $\nu_p(n!) = \sum_{\ell=1}^{\infty} [n/p^\ell]$. Un calcul analogue à celui de Lucas [Di] montre que

$$\binom{n}{h_1, \ldots, h_r} \equiv \prod_{\ell=0}^{L} \binom{\varepsilon_\ell}{\varepsilon_\ell^{(1)}, \ldots, \varepsilon_\ell^{(r)}} \bmod p.$$

Ce dernier résultat et un calcul standard sur les caractères (cf. [LN]) donnent alors la formule (5).
D'autre part, le terme de la formule (5) correspondant au caractère trivial est:

$$\frac{1}{p-1} \prod_{k=1}^{p-1} \binom{k + r - 1}{k}^{s_k(n)}.$$

Considérons alors

$$\sum_{n<N} \#\left\{(h_1, \ldots, h_r) \mid \binom{n}{h_1, \ldots, h_r} \equiv a \bmod p\right\}.$$

L'application du résultat sur les formules sommatoires obtenu dans [Gr] donne (2) pourvu que l'on ait prouvé que, pour $\chi \neq \chi_0$, l'inégalité

$$(6) \qquad \left| \sum_{k=0}^{p-1} \sum_{\delta_1 + \cdots + \delta_r = k} \chi\binom{k}{\delta_1, \ldots, \delta_r} \right| < \binom{p+r-1}{p-1}.$$

Supposons maintenant que

$$\left| \sum_{k=0}^{p-1} \sum_{\delta_1 + \cdots + \delta_r = k} \chi\binom{k}{\delta_1, \ldots, \delta_r} \right| = \binom{p+r-1}{p-1}.$$

Alors, toutes les évaluations du caractère doivent être égales à 1 parce que $\chi(1) = 1$ et que 1 est une des valeurs possibles du coefficient multinomial. Mais $\binom{k}{k-1,1,0,\ldots,0} = k$, d'où nécessairement $\chi = \chi_0$; l'inégalité (6) s'en déduit.

Le calcul précedent permet aussi de déduire une expression pour le terme d'erreur dans (2). Il résulte de la formule sommatoire donnée dans [Gr] que chaque caractère $\chi \neq \chi_0$ contribue pour $O(N^{\log_p M_\chi})$ dans la formule sommatoire avec

$$M_\chi = \max\left(\max_{k=0,\ldots,p-1} \left| \sum_{\delta_1 + \cdots + \delta_r = k} \chi\binom{k}{\delta_1, \ldots, \delta_r} \right|, \left| \sum_{k=0}^{p-1} \sum_{\delta_1 + \cdots + \delta_r = k} \chi\binom{k}{\delta_1, \ldots, \delta_r} \right| \right).$$

Pour $p = 3$ un calcul direct donne

$$M_\chi = \begin{cases} 4 & \text{pour } r \leq 3 \\ r & \text{pour } 4 \leq r \leq 5 \\ \dfrac{r}{2}(r-3) & \text{pour } r > 5 \end{cases}$$

et pour tous les nombres premiers $p \geq 5$ on a

$$M_\chi \leq \binom{p+r-1}{p-1} - r(p-1).$$

Ces majorations conduisent à une valeur explicite pour ε dans (2). □

3. LE CAS DES COEFFICIENTS BINOMIAUX GAUSSIENS

Dans ce qui suit, $\begin{bmatrix} n \\ k \end{bmatrix}_q$ est défini par

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{[n]_q!}{[k]_q![n-k]_q!} = \frac{[1]_q[2]_q \cdots [n]_q}{[1]_q[2]_q \cdots [k]_q \cdot [1]_q[2]_q \cdots [n-k]_q},$$

où $[n]_q$ vaut $1 + q + \cdots + q^{n-1}$.

Proposition 2. *Soit Q un polynôme de degré s, irreductible sur $\mathbb{F}_p$ et ζ une racine de Q d'ordre R dans $\mathbb{F}_{p^s}^*$. Soient n' et n'' respectivement le quotient et le reste de la division euclidienne de n par R, où n est un entier naturel non nul. Alors,*

$$
(7)\qquad \begin{cases} \#\left\{k \mid \begin{bmatrix} n \\ k \end{bmatrix}_x \equiv a(x) \bmod Q(x)\right\} \\ \quad = \dfrac{1}{p^s-1} \displaystyle\sum_{\chi} \bar{\chi}(a(\zeta)) \sum_{\ell=0}^{n''} \prod_{d=1}^{\min(\ell, n''-\ell)} \chi([d]_\zeta^{-1}[n''+1-d]_\zeta) \\ \qquad \times \displaystyle\prod_{r=0}^{p-1} \left(\sum_{\delta=0}^{r} \chi\binom{r}{\delta} \right)^{s_r(n')}, \end{cases}
$$

où la sommation est étendue sur tous les caractères χ de $\mathbb{F}_{p^s}^*$.

Démonstration. Notons ν_Q la valuation dans l'anneau $\mathbb{F}_p[x]$ associée au polynôme Q. De manière évidente

$$
\nu_Q([\ell R + d]_x) = 0 \quad \text{pour } 0 < d < R \text{ et}
$$
$$
\nu_Q([\ell R]_x) = p^{\nu_p(\ell)}.
$$

Un calcul, analogue à celui qui permet d'obtenir la formule de Legendre donnant $\nu_p(n!)$, donne:

$$
\nu_Q([n]_x!) = n' + \left(1 - \frac{1}{p}\right) \sum_{k=1}^{\infty} p^k \left[\frac{n'}{p^k}\right].
$$

On écrit $k = k'R + k''$ avec $0 \le k'' < R$ et remarquons que $\begin{bmatrix} n \\ k \end{bmatrix}_x \not\equiv 0 \bmod Q(x)$ si et seulement si $n' = [(n-k)/R] + [k/R]$ (qui est équivalent à $k'' \le n''$) et si l'addition $[(n-k)/R] + [k/R]$ s'effectue sans retenue en base p. Dans ce cas, on utilise la formule

$$
[\ell R + d]_x \equiv [d]_x \bmod Q(x) \quad \text{pour } 0 < d < R \text{ et}
$$
$$
[\ell R]_x = \frac{\ell}{p^{\nu_p(\ell)}} (x-1)^{-1} \left(\frac{x^R - 1}{Q(x)}\right)^{p^{\nu_p(\ell)}} Q(x)^{p^{\nu_p(\ell)}}
$$

pour obtenir

$$
\begin{bmatrix} n \\ k \end{bmatrix}_x \equiv \prod_{d=1}^{R-1} [d]_x^{[(n''-d)/R] - [(k''-d)/R] - [(n''-k''-d)/R] - 1} \binom{n'}{k'} \bmod Q(x).
$$

Remarquons que $[(n''-d)/R] - [(k''-d)/R] - [(n''-k''-d)/R] - 1$ ne prend que les valeurs $-1, 0, 1$. Plus précisément

$$
\left[\frac{n''-d}{R}\right] - \left[\frac{k''-d}{R}\right] - \left[\frac{n''-k''-d}{R}\right] - 1
$$
$$
= \begin{cases} -1 & \text{pour } 1 \le d \le \min(k'', n''-k'') \\ 0 & \text{pour } \min(k'', n''-k'') < d \le \max(k'', n''-k'') \text{ ou} \\ & \quad n'' < d < R \\ 1 & \text{pour } \max(k'', n''-k'') < d \le n''. \end{cases}
$$

Enfin un calcul de caractères donne l'équation (7). □

Pour déduire le résultat (3), il suffit sommer la famille d'équations (7) sur tous les $n < N$ et tous les polynômes $a \neq 0$, ce qui donne

$$\begin{cases} \#\left\{(n,k) \mid n < N \begin{bmatrix} n \\ k \end{bmatrix}_x \not\equiv 0 \bmod Q(x)\right\} \\ \quad = \sum\limits_{n<N} (n''+1) \prod\limits_{r=0}^{p-1} (r+1)^{s_r(n')}, \end{cases}$$

d'où l'on déduit avec une application de la formule sommatoire pour les fonctions q-multiplicatives de [Gr]:

$$(8) \qquad \begin{cases} \#\left\{(n,k) \mid n < N \begin{bmatrix} n \\ k \end{bmatrix}_x \not\equiv 0 \bmod Q(x)\right\} \\ \quad = \dfrac{R(R+1)}{2} \left(\dfrac{N}{R}\right)^{\beta} F_{p,2}\left(\log_p \dfrac{N}{R}\right)(1+o(1)). \end{cases}$$

Nous remarquons que $G_{p,Q}(t) = ((R(R+1))/2R^{\beta})F_{p,2}(t - \log_p R)$.
Enfin, nous étudions le cas où la quantité

$$\#\left\{(n,k) \mid n < N \begin{bmatrix} n \\ k \end{bmatrix}_x \equiv a(x) \bmod Q(x)\right\}$$

est d'ordre de grandeur N^{β}, pour un polynôme $a \in \mathbb{F}_p[x]$. Nous remarquons que le terme principal d'ordre de grandeur N^{β} existe si et seulement si la somme,

$$\sum_{\chi}{}' \bar{\chi}(a(\zeta)) \sum_{\ell=0}^{n''} \prod_{d=1}^{\min(\ell, n''-\ell)} \chi([d]_{\zeta}^{-1}[n''+1-d]_{\zeta}) \prod_{r=0}^{p-1} \left(\sum_{\delta=0}^{r} \chi\binom{r}{\delta}\right)^{s_r(n')}$$

étendue sur tous les caractères χ de $\mathbb{F}_{p^s}^*$ dont la restriction à $\mathbb{F}_p^*$ est le caractère trivial, n'est pas nulle.
En utilisant la formule classique

$$\sum_{\chi}{}' \chi(x) = \begin{cases} 0 & \text{pour } x \in \mathbb{F}_{p^s}^* \setminus \mathbb{F}_p^* \\ \dfrac{p^s - 1}{p-1} & \text{pour } x \in \mathbb{F}_p^*, \end{cases}$$

nous obtenons:

$$(9) \qquad \begin{cases} \#\left\{(n,k) \mid n < N \begin{bmatrix} n \\ k \end{bmatrix}_x \equiv a(x) \bmod Q(x)\right\} \\ \quad = \#\left\{(m,\ell) \mid 0 \leq m \leq R-1, \right. \\ \qquad\qquad \left. 0 \leq \ell \leq m, \prod\limits_{d=1}^{\min(\ell, m-\ell)} [d]_{\zeta}^{-1}(m+1-d]_{\zeta} \in a(\zeta)\mathbb{F}_p^*\right\} \\ \quad \times \dfrac{1}{p-1} \left(\dfrac{N}{R}\right)^{\beta} F_{p,2}\left(\log_p \dfrac{N}{R}\right) + o(N^{\beta}). \end{cases}$$

REMERCIEMENT

Ce travail a été réalisé pendant la visite du deuxième auteur à Marseille dans l'équipe DSA. Les auteurs remercient Pierre Liardet pour ses remarques concernant la présentation du papier.

REFERENCES

[Di] Dickson, L.E. – History of the theory of numbers, Vol. 1. Chelsea, New York (1952).

[Fi] Fine, N.J. – Binomial coefficients modulo a prime. Amer. Math. Monthly **54**, 589–592 (1947).

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

[Gr] Grabner, P.J. – Completely q-Multiplicative Functions: the Mellin-Transform Approach. Acta Arith. **65**, 85–96 (1993).

[Ho1] Howard, F.T. – The number of multinomial coefficients divisible by a fixed power of a prime. Pacific J. Math. **50**, 99–107 (1974).

[Ho2] Howard, F.T. – Multinomial and Q-binomial coefficients modulo 4 and modulo P. Fibonacci Q. **31**, 53–64 (1993).

[LN] Lidl, R. and H. Niederreiter – Introduction to finite fields and their application. Cambridge University Press (1986).

[Si] Singmaster, D. – Notes on binomial coefficients, I - A generalization of Lucas congruence, II - The least n such that p^e divides an r-nomial coefficient of rank n, III - Any integer divides almost all binomial coefficients. J. London Math. Soc. (2) **8**, 545–548, 549–554, 555–560 (1974).

[St] Stein, A.H. – Binomial coefficients not divisible by a prime. Number Theory, New York (1985/88), Lecture Notes in Mathematics **1383**, 170–177, Springer (1989).

[Wo] Wolfram, S. – Geometry of binomial coefficients. Amer. Math. Monthly **91**, 566–571 (1984).

NOTE ADDED IN PROOF

An alternative approach to formula (5) in the binomial case is contained in R. Garfield and H.S. Wilf, The Distribution of the Binomial Coefficients Modulo p, J. Number Th. **41**, 1–5 (1992). Their approach uses generating functions instead of character sum computations.