Monatsh. Math. 131, 263–277 (2000)

Monatshefte für
Mathematik
© Springer-Verlag 2000
Printed in Austria

On the Distribution of the Sums of Binomial Coefficients Modulo a Prime

By

Henri Faure

CNRS, Marseille, France

(Received 21 June 1999; in revised form 13 July 2000)

Abstract. Let $\binom{c}{l}$ be the binomial coefficient modulo b (b prime), with $\binom{c}{l} = 0$ if l is greater than c, and let σ_c^l be the sum of binomial coefficients modulo b, that is $\sigma_c^l = \sum_{h=0}^{l} \binom{c}{h}$ (mod b). We prove the following property: the σ_c^l for which the couples (c, l) verify $0 \leqslant l \leqslant c < b^n$ and $\binom{c}{l} \neq 0$ are uniformly distributed in the residue classes modulo b as n tends to infinity. The method, using the Perron-Frobenius theory, applies also to $\binom{c}{l}$ and gives a new proof of the well known result for the non-zero binomial coefficients modulo b.

2000 Mathematics Subject Classification: 11B65, 11A07, 15A18
Key words: Binomial coefficients, residue systems, eigenvalues

1. Introduction

The distribution of binomial coefficients in the residue classes modulo a prime number has been widely studied and precise results are now available; the last related papers on this topic, as far as we know, are [1], [2] and [3]; they contain many other interesting references, especially on the contributions of Carlitz, Garfield and Wilf, Howard, Singmaster and Stein.

In this paper, we are interested in the same distribution property for the sums of binomial coefficients; but the classical method using character sums computations do not apply here because there is no Lucas formula for these sums; in order to obtain the desired uniform distribution property (see Theorem 2 below), we have worked out a new method which applies also to the binomial coefficients and should be of some interest in this case (see Theorem 1).

Basically, the method consists in drawing out the algorithmic structure of the matrix C of binomial coefficients and of the corresponding matrix Σ of the sums of binomial coefficients. Then, it is possible to build up a universal matrix $A(C)$, resp. $A(\Sigma)$, which gives a recursion formula for the number of entries of C, resp. Σ, belonging to a fixed class. Finally, by means of the Perron-Frobenius theory applied to A, which is proved to be irreducible and primitive, we obtain the required distribution property for both C and Σ.

At the origin, we have met these sums of binomial coefficients modulo a prime in the context of irregularities of distribution of sequences generated by means of the binomial matrices (see [4] and [6]).

These results have been announced at the Conference on Algebraic Number Theory and Diophantine Analysis held in Graz in 1998, with a sketch of the proof in the proceedings [5]; the present full paper emphasizes the algorithmic structure of Σ and outlines the main ideas of the method (in particular the construction of $A(\Sigma)$) before it goes further in the very technical proofs of the lemmas (only stated in [5]).

We should like to thank the referees for pointing out the lack of readability of the first version and suggesting the actual presentation; in particular, we omit huge examples of matrices C, Σ and $A(\Sigma)$ and a recapitulation on Perron-Frobenius (firstly asked by the referee for the proceedings); we refer to Chapters 1 and 2 of [7] for the required elements of this theory.

The second section contains the results, the third the case of C and the fourth the case of Σ.

2. Definitions and Theorems

Given an infinite matrix $M = (m_c^l)_{c\geqslant 0, l\geqslant 0}$, we denote by $M(c, c'; l, l')$ the submatrix of M obtained by keeping the rows between l and $l'-1$ included and the columns between c and $c'-1$ included. To simplify, we write $M(c; l) = M(0, c; 0, l)$. Moreover we set ${}^tA$ for the transpose matrix of A.

Let $C = \left(\binom{c}{l}\right)$ be the binomial matrix mod b (b prime), with $\binom{c}{l} = 0$ if the row l is greater than the column c, and let $\Sigma = (\sigma_c^l)$ be the matrix of the sums of binomial coefficients modulo b (c index of columns, l index of rows):

$$\sigma_c^l = \sum_{h=0}^{l} \binom{c}{h} (\text{mod } b).$$

Theorem 1. *The non-zero binomial coefficients $\binom{c}{l}$ modulo b (b prime) with $0 \leqslant c < b^n$ and $0 \leqslant l < b^n$ are uniformly distributed in the non-zero residue classes modulo b as n tends to infinity. In other words, the non-zero entries of the matrix $C(b^n; b^n)$ are uniformly distributed in the $(b-1)$ non-zero residue classes modulo b as n tends to infinity.*

Remark 1. This property is easily deduced from previous studies on binomial coefficients (see for instance [3]); we give our new proof for C in Section 3 to introduce on a simple case the method to be used for Σ in Section 4.

Theorem 2. *The coefficients σ_c^l, with (c, l) such that $0 \leqslant c < b^n, 0 \leqslant l < b^n$ and $\binom{c}{l} \neq 0$ mod b (b prime), are uniformly distributed in the b residue classes modulo b, as n tends to infinity. In other words, the entries σ_c^l of the matrix $\Sigma(b^n; b^n)$ with $\binom{c}{l} \neq 0$ mod b are uniformly distributed in the b residue classes modulo b (included the zero class) as n tends to infinity.*

Remark 2. For both the matrices C and Σ, the distribution of entries is quite different under the diagonals and above (or on) the diagonals: under the diagonals of C, the binomial coefficients are all 0 whereas under the diagonals of Σ, the entries σ_c^l are of the form $a2^c \pmod b$ with $a \geqslant 0$; above (or on) the diagonals of C the binomial coefficients are never 0 whereas above (or on) the diagonals of Σ the entries σ_c^l can be 0 (see 3.1, 4.3 and 4.6 for more information). These properties explain the different formulations of Theorems 1 and 2.

Remark 3. The algorithmic structure of Σ is much more complicated than that of C; our method applies with a lot of technical difficulties due to the nature of Σ for which the construction needs b blocks instead of one for C (see Sections 3.1 and 4.8).

Remark 4. Both theorems are valid for arbitrary prime b, so their statement is unavoidably general and somewhat vague; but for fixed b, the method can lead to the exact computation of the number of entries belonging to a given class (see the examples).

Remark 5. All computations involving entries of C or Σ are performed modulo b, so in most cases we omit (mod b) in these computations to lighten the formulas; on the other hand, when we count the number of entries in the residue classes (in sections 3.3, 3.4, 4.9 and 4.10), we deal of course with non negative integers and in this case no confusion is possible.

3. The Case of C (Proof of Theorem 1)

In this section, we prove Theorem 1. We need two lemmas, the first on the structure of the matrix C, the second on linear algebra. For convenience of notations, we set $C_n = C(b^n; b^n)$.

The idea is to use the simple recursion formula from C_n to C_{n+1} (Lemma 3.1) to obtain a relation between the number of entries, in C_{n+1}, belonging to some non-zero residue class and the whole number of entries, in C_n, distributed in all the non-zero residue classes; of course, such a relation for $(b-1)$ integers to be found (for C_{n+1}) depending on $(b-1)$ integers already known (for C_n) should be given by means of a $(b-1) \times (b-1)$ matrix, the so-called counting matrix of Section 3.3; then the problem of counting the entries in the non-zero residue classes is brought back to a matrix iterative problem for which powerfull tools exist; actually, this method has been first worked out for the matrix Σ for which no results by the classical way were available.

Recall that in the following lemmas all computations are modulo b, according to remark 5 in section 2.

3.1 Lemma *(Algorithmic construction of C). For all integers $n \geqslant 1, 0 \leqslant c < b$, $0 \leqslant l < b$, we have $C(cb^n, (c+1)b^n; lb^n, (l+1)b^n) = \binom{c}{l} C_n$. In other words, the square matrix C_{n+1} arises from C_n by the algorithmic block construction $C_{n+1} = \left(\binom{c}{l} C_n\right)$.*

Proof. This property follows from $\binom{cb^n+r}{lb^n+s} = \binom{c}{l}\binom{r}{s}$ with $0 \leqslant r < b^n$, $0 \leqslant s < b^n$, which is a consequence of the Lucas formula:

$$\binom{c}{l} = \prod_{i=1}^{\infty}\binom{c_i}{l_i}$$

where $c = \sum_{i=0}^{\infty} c_i b^i$ and $l = \sum_{i=0}^{\infty} l_i b^i$ are the b-adic expansions of c and l. □

Corollary and Definition. *An arbitrary entry $\binom{c}{l}$ of C is naught if and only if it is strictly under the diagonal of some block containing it. By definition, given a prime b and an infinite matrix M, an arbitrary entry m_c^l of M is called (strictly) under the diagonals if $\binom{c}{l} = 0$ (mod b) and above (or on) the diagonals if $\binom{c}{l} \neq 0$ (mod b).*

This corollary is a direct consequence of the lemma (i. e. of the Lucas formula) and of the well known properties of C_1, the first block of the binomial matrix modulo b.

3.2 Lemma. *Let $A = (a_c^l)$ be a $d \times d$ complex matrix such that $\sum_{c=1}^{d} a_c^l = \sum_{l=1}^{d} a_c^l = \lambda$ with λ simple eigenvalue of A; let $A = PJP^{-1}$ with J the Jordan normal form of A in which λ is the first entry of J. Then the first column of P is ${}^t(1,1,\ldots,1)$ and the first row of P^{-1} is $d^{-1}(1,1,\ldots,1)$.*

Proof. The first part is straightforward since ${}^t(1,1,\ldots,1)$ is an eigenvector for the eigenvalue λ.

For the second part, we note that ${}^tA$ has the same eigenvalues as A and that ${}^tA = {}^t(P^{-1}){}^tJ\,{}^tP$; now, if B is a $d \times d$ complex matrix with the simple eigenvalue λ such that $K = Q^{-1}BQ$ is the Jordan normal form of B in which λ is the first entry, then the first column of Q is an eigenvector for the eigenvalue λ, as verified by direct computation; applying this property with $B = {}^tA$ and $Q = {}^t(P^{-1}) = ({}^tP)^{-1}$ shows that the first column of ${}^t(P^{-1})$ is an eigenvector of ${}^tA$ for λ; on the other hand, $\sum_{l=1}^{d} a_c^l = \lambda$ implies that this eigenvector is proportional to ${}^t(1,1,\ldots,1)$ and $P^{-1}P = I$ gives d^{-1} for the constant. □

3.3. The counting matrix $A(C)$. Let $\nu_l^{(n+1)}$ be the number of entries belonging to the residue class l (mod b) in $C_{n+1} = C(b^{n+1}; b^{n+1})$.

With Lemma 3.1 or its corollary, it is easy to verify that $\nu_0^{(n+1)} = \frac{b(b-1)}{2}b^{2n} + \frac{b(b+1)}{2}\nu_0^{(n)}$, so that $\nu_0^{(n)} = b^{2n} - \left(\frac{b(b+1)}{2}\right)^n$. After this special case of the zero class, we deal with the number of entries belonging to the class l with $1 \leqslant l < b$.

In order to express $\nu_l^{(n+1)}$ $(1 \leqslant l < b)$ by means of the $\nu_c^{(n)}$ $(1 \leqslant c < b)$, applying Lemma 3.1, we must count the number A_c^l of sub-matrices of C_{n+1} with the form αC_n where $\alpha = l/c$ (mod b); because by this way, an entry of C_n belonging to the residue class c (counted in $\nu_c^{(n)}$) becomes congruent to $\alpha c = l$ and so must be counted in $\nu_l^{(n+1)}$.

Collecting the numbers A_c^l in rows of indexes l and columns of indexes c, we obtain the $(b-1)\times(b-1)$ matrix $A = A(C) = (A_c^l)$ which gives the fundamental relation:

$$N^{(n+1)} = AN^{(n)} \quad \text{with} \quad N^{(n)} = {}^t(\nu_1^{(n)}, \dots, \nu_{b-1}^{(n)}).$$

It is easy to obtain the matrix $A(C)$ for small b; for instance, with $b = 3$ and $b = 5$, we have respectively:

$$A(C) = \begin{pmatrix} 5 & 1 \\ 1 & 5 \end{pmatrix} \qquad A(C) = \begin{pmatrix} 10 & 2 & 1 & 2 \\ 1 & 10 & 2 & 2 \\ 2 & 2 & 10 & 1 \\ 2 & 1 & 2 & 10 \end{pmatrix}.$$

But moreover, this matrix has two nice properties which allow us to apply the Perron-Frobenius theory:

Proposition. *The matrix A is positive (i.e. all entries are positive) and $\sum_{c=1}^{b-1} A_c^l = \sum_{l=1}^{b-1} A_c^l = \frac{b(b+1)}{2}$ for all integers c, l with $1 \leqslant c \leqslant b-1$ and $1 \leqslant l \leqslant b-1$.*

Proof. We apply the first lemma: A is positive because $C_{n+1} = \left(\binom{c}{l} C_n\right)$ and $\binom{\alpha}{1} = \alpha$, so there is at least one sub-matrix of C_{n+1} with the form αC_n, so $A_c^l \geqslant 1$.

Moreover, $\sum_{c=1}^{b-1} A_c^l = \sum_{l=1}^{b-1} A_c^l = \frac{b(b+1)}{2}$ because there are $\frac{b(b+1)}{2}$ sub-matrices of the form αC_n, different from the zero matrix, in C_{n+1}. In other words, the first column A_1 of A corresponds to the number of sub-matrices $lC_n (1 \leqslant l < b)$, and the following columns A_c are obtained by permutations of the entries of A_1, according to the square table of values of $\alpha = l/c \pmod b$. □

Corollary. *The spectral radius of A is $\rho = \frac{b(b+1)}{2}$ and A is primitive (i.e. all the other eigenvalues λ of A verify $|\lambda| < \rho$).*

Proof. Recall that the spectral radius ρ (the maximum of the absolute values of the eigenvalues) is less than the maximum of the sums of the absolute values of the rows (resp. of the columns); therefore $\rho = \frac{b(b+1)}{2}$, since $\frac{b(b+1)}{2}$ is an eigenvalue. On the other hand, recall too that a positive matrix is primitive which proves the second part. □

We remark that the eigenvalues of $A(C)$ could be written in terms of the character sums involved in the method of [3].

3.4 Proof of Theorem 1. According to 3.3, we have $N^{(n)} = A^n N^{(0)}$ with $A^n = PJ^nP^{-1}$ and $N^{(0)} = {}^t(1, 0, \dots, 0)$ (because $\nu_l^{(0)}$ is the number of l in $C_0 = (1)$); computing the matrix product with the property of Lemma 3.2 for P and P^{-1}, see for instance [7] for the expression of J^n, we get the entries of A^n in the form $\frac{1}{b-1}\rho^n + \sum_{i=1}^{r} P_i(\lambda_i)$ where P_i is a polynomial of degree n with less than $(b-1)$ terms and where the λ_i are the other eigenvalues, so that $|\lambda_i| < \rho$.

Finally, we get $\nu_l^{(n)} = \frac{1}{b-1}\rho^n + o(\rho^n)$ for $1 \leqslant l < b$ and the theorem follows since $\rho^n = \left(\frac{b(b+1)}{2}\right)^n$ is the number of non-zero entries in C_n (compare with the number of zero entries at the beginning of Section 3.3). □

Example. With $b = 3$, we obtain:

$$J = \begin{pmatrix} 6 & 0 \\ 0 & 4 \end{pmatrix} \qquad P = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad P^{-1} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

so that the number of entries in C_n congruent respectively to 1 and 2 is:

$$\nu_1^{(n)} = \frac{1}{2}(6^n + 4^n) \quad \text{and} \quad \nu_2^{(n)} = \frac{1}{2}(6^n - 4^n);$$

and with $b = 5$:

$$J = \begin{pmatrix} 15 & 0 & 0 & 0 \\ 0 & 9 & 0 & 0 \\ 0 & 0 & 8-i & 0 \\ 0 & 0 & 0 & 8+i \end{pmatrix}$$

$$P = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -i & i \\ 1 & -1 & i & -i \\ 1 & 1 & -1 & -1 \end{pmatrix} \qquad P^{-1} = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & i & -i & -1 \\ 1 & -i & i & -1 \end{pmatrix},$$

so that the number of entries in C_n congruent respectively to 1, 2, 3 and 4 is:

$$\nu_1^{(n)} = \frac{1}{4}(15^n + 9^n + 2\cos(n\alpha)(\sqrt{65})^n) \quad \nu_2^{(n)} = \frac{1}{4}(15^n - 9^n - 2\sin(n\alpha)(\sqrt{65})^n)$$
$$\nu_3^{(n)} = \frac{1}{4}(15^n - 9^n + 2\sin(n\alpha)(\sqrt{65})^n) \quad \nu_4^{(n)} = \frac{1}{4}(15^n + 9^n - 2\cos(n\alpha)(\sqrt{65})^n),$$

where $\alpha = \arctan\left(\frac{1}{8}\right)$.

4. The Case of Σ (Proof of Theorem 2)

Again all computations implying entries of Σ are modulo b; as in 3.3 for C, we set $\Sigma_n = \Sigma(b^n; b^n)$ and to avoid heavy indexes we write $\sigma_c^l = \sigma(c, l)$.

4.1. Introduction. Before going ahead to the technical Lemmas 4.2 to 4.8 which describe the structure of Σ_{n+1} and, then, to construct the counting matrix $A(\Sigma)$, we are going to set off this structure and to outline the definition of $A(\Sigma)$; the end of the proof follows that for C, but requires a deeper analysis of $A(\Sigma)$ with regards to Peron-Frobenius because it is only non-negative (see 4.9), contrary to $A(C)$ which is positive. In order to seize more easily the following statements, it should be very useful for the reader to write down an example of Σ_2 (with $b = 3$ or 5 or even 7).

From the definition of Σ, it is straightforward that the entries of the first row and the first column are equal to 1 and that the main diagonal is formed by the successive powers of 2 (mod b); also the entries under the main diagonal (included) are constant on the columns; more generally, we can prove that, as for C, the structure under the diagonals (see Corollary and Definition 3.1) is still very simple: the entries are constant on the columns (see Lemma and Corollary 4.3).

On the contrary, the structure above the diagonals is much more complex, but we can point out some basic facts:

Split Σ_{n+1} into b^2 blocks of $b^n \times b^n$ sub-matrices; it is easy to see that the first row of such blocks is formed by repetitions of the first one, that is $B_1^n := \Sigma_n$ (go to Lemma 3.1 and sum the coefficients).

Now, look at the second row of blocks above (or on) the main diagonal: there are $(b-1)$ different blocks (noted $B_i^n, 2 \leqslant i \leqslant b$), the first entries of which are $2, 3, \ldots, b-1, 0$ (go to Lemma 3.1 and sum with one more coefficient); useful properties on the last 2 columns of $B_1^n, \ldots, B_b^n$ are given in Lemmas 4.6 and 4.7.

What's about the other blocks above (or on) the main diagonal? This is the critical part of the algorithmic properties of Σ: it can be proved that these blocks are the same as the b preceding ones, up to a constant factor! Essentially, the reason is that the last column of any such block presents an alternance of two different digits only (see Lemma and Corollary 4.5); Lemma 4.8 makes explicit the relation between an arbitrary block and the block, among $B_1^n, \ldots, B_b^n$, from which it results by multiplication via a constant factor.

Corollary 4.8 summarizes the algorithm; our knowledge of Σ is now sufficient to build the counting matrix and prove its primitivity in all generality (proposition 4.9), which brings us to the asymptotic result we are looking for (4.10).

As announced at the beginning, we shall now outline the construction of $A(\Sigma)$: come back to the beginning of Section 3 where $A(C)$ appeared to be the $(b-1) \times (b-1)$ matrix relating $(b-1)$ integers to be found to $(b-1)$ integers already known: here we have the same situation, but we must manage with b blocks $B_1^n, \ldots, B_b^n$ instead of one (C_n); and get the number of entries, above (or on) the diagonals belonging to some non-zero residue class l in B_j^{n+1} by means of the whole number of entries (above (or on) the diagonals), in all the B_i^n, distributed in all the non-zero residue classes $c (1 \leqslant c < b)$; therefore, we are looking for $b(b-1)$ integers to be found (for the B_j^{n+1}) depending on $b(b-1)$ integers already known (for the B_i^n); so the counting matrix $A(\Sigma)$ in the present case is a $b(b-1) \times b(b-1)$ matrix whose indexes are described by 4 variables, (l,j) for the rows and (c, i) for the columns (see 4.9 for the explicit construction of that matrix); so far, we have worked out the number of entries in non-zero residue classes; now with Σ, the zero class occurs also above (or on) the diagonals, but the number of such entries is the only one we don't know, so by difference with the total number, we get it too (see the end of the proof, 4.10).

4.2 Lemma *(Recursion formula). The sums of binomial coefficients satisfy the following relations:* $\sigma(c, 0) = \sigma(0, l) = 1$ *for all integers* $c \geqslant 0, l \geqslant 0$ *and*

$$\sigma(c, l) = \sigma(c-1, l) + \sigma(c-1, l-1) \textit{ for all integers } c \geqslant 1,\ l \geqslant 1.$$

In other words, the binomial coefficients and their sums satisfy the same recursion formula.

Proof. The first equalities follow directly from the definition of Σ; for the recursion formula, we express the sum on the right hand side:

$$\sigma(c-1,l)+\sigma(c-1,l-1)=\sum_{h=0}^{l}\binom{c-1}{h}+\sum_{h=0}^{l-1}=\binom{c-1}{0}$$
$$+\sum_{h=1}^{l}\left(\binom{c}{h}-\binom{c-1}{h-1}\right)+\sum_{h=0}^{l-1}\binom{c-1}{h}$$

because

$$\binom{c}{h}=\binom{c-1}{h}+\binom{c-1}{h-1};$$

but

$$\binom{c-1}{0}=\binom{c}{0}\quad\text{and}\quad\sum_{h=1}^{l}\binom{c-1}{h-1}=\sum_{h'=0}^{l-1}\binom{c-1}{h'},$$

so finally, the right hand side of the above equality is equal to $\sigma(c,l)$. □

In the following lemmas, we are mainly concerned with the properties of the $b^n\times b^n$ blocks issued from the splitting of Σ_{n+1}; with the notations introduced at the beginning of section 2, they read as $\Sigma(rb^n,(r+1)b^n;sb^n,(s+1)b^n)$; the comments between brackets in the statements of lemmas refer to these blocks (for instance entries of corners (4.4) means the left (resp. right) upper (resp. lower) entries of such a block).

4.3 Lemma *(Entries of columns rb^n). Given integers $n\geqslant 1, r\geqslant 0, s\geqslant 0$, we have $\sigma(rb^n,l)=\sigma(rb^n,sb^n)$ for all integers l with $sb^n\leqslant l<(s+1)b^n$. In other words, the entries of columns (rb^n) are constant.*

Proof. We have

$$\sigma(rb^n,l)=\sum_{h=0}^{l}\binom{rb^n}{h}=\sum_{h=0}^{sb^n}\binom{rb^n}{h}+\sum_{h=sb^n+1}^{l}\binom{rb^n}{h}=\sigma(rb^n,sb^n),$$

because

$$\sum_{h=sb^n+1}^{l}\binom{rb^n}{h}=\sum_{h'=1}^{l-sb^n}\binom{rb^n}{sb^n+h'}=\sum_{h'=1}^{l-sb^n}\binom{r}{s}\binom{0}{h'}=0,$$

which is a consequence of the Lucas formula, see the proof of Lemma 3.1. □

Corollary *(Structure under the diagonals). The entries under the diagonal (included) of columns of $\Sigma(rb^n,(r+1)b^n;sb^n,(s+1)b^n)$ are constant of the form $a2^c$ with fixed a $(0\leqslant a<b)$ and $c=0,1,2,\ldots$.*

Proof. By Lemma 4.3, the first column is a constant, say a; then, by the recursion formula 4.2, we get $a+a=2a$ for the entries under the diagonal of the second column; and so on until the last column (reduced to its diagonal entry) for which we obtain $a2^{b^n-1} = a$. □

4.4 Lemma *(Entries of corners). Given integers* $n \geqslant 1, r \geqslant 0, s \geqslant 0$, *we have* $\sigma(r,s) = \sigma(rb^n, sb^n) = \sigma(rb^n, (s+1)b^n - 1) = \sigma((r+1)b^n - 1, (s+1)b^n - 1) = \sigma((r+1)b^n - 1, sb^n)$.

Proof. First we have:

$$\begin{aligned}\sigma(rb, sb) &= \sum_{h=0}^{sb} \binom{rb}{h} = \sum_{l=0}^{s-1}\sum_{h'=0}^{b-1} \binom{rb}{lb+h'} + \binom{rb}{sb} \\ &= \sum_{l=0}^{s-1}\sum_{h'=0}^{b-1} \binom{r}{l}\binom{0}{h'} + \binom{r}{s} = \sigma(r,s).\end{aligned}$$

Then the first equality results by iteration and the second is a direct consequence of Lemma 4.3; for the third, we note that if $\sigma(rb^n, (s+1)b^n - 1) = a$, then, by Corollary 4.3, $\sigma((r+1)b^n - 1, (s+1)b^n - 1) = a2^{b^n-1} = a$; finally, for the fourth equality, we use the recursion formula 4.2 with the last row of $\Sigma(rb^n; (s-1)b^n)$ and get $\sigma((r+1)b^n - 1, sb^n) = a + \alpha + 2\alpha + \cdots + 2^{b^n-2}\alpha$ (see Corollary 4.3) where $\alpha = \sigma(rb^n, sb^n - 1)$; therefore $\sigma((r+1)b^n - 1, sb^n) = a + \alpha(2^{b^n-1} - 1) = a$. □

4.5 Lemma *(Entries of columns* $(rb^n - 1)$*). Given integers* $n \geqslant 1, s \geqslant 0, r > s$, *we have* $\sigma(rb^n - 1, l) = \sigma(rb^n - 1, l+2)$ *and* $\sigma(rb^n - 1, l) \neq \sigma(rb^n - 1, l+1)$ *for all integers* l *with* $sb^n \leqslant l < (s+1)b^n - 2$. *In other words, the entries of columns* $(rb^n - 1)$ *present an alternance of two different digits only.*

Proof. To prove the equality, we first use the recursion formula 4.2: $\sigma(rb^n - 1, l) + \sigma(rb^n - 1, l+1) = \sigma(rb^n, l+1)$ and $\sigma(rb^n - 1, l+1) + \sigma(rb^n - 1, l+2) = \sigma(rb^n, l+2)$; then, from Lemma 4.3, we see that $\sigma(rb^n, l+1) = \sigma(rb^n, l+2)$, so we get $\sigma(rb^n - 1, l) = \sigma(rb^n - 1, l+2)$.

For the inequality, we note, from the definition of Σ, that $\sigma(rb^n - 1, l+1) - \sigma(rb^n - 1, l) = \binom{rb^n - 1}{l+1} \neq 0$, as usual with binomial coefficients modulo a prime. □

Corollary *(Structure above the diagonals). Given integers* $s \geqslant 0$ *and* $r \geqslant s$, *the entries above the diagonal (not included) of* $\Sigma(rb^n, (r+1)b^n; sb^n, (s+1)b^n)$ *are completely determined by the last (or first) two entries of the last column.*

Proof. This corollary results from the recursion formula 4.2: the diagonal is already known by Corollary 4.3 and starting from the right corner down, by difference with 4.2, we get step by step all the entries above the diagonal. □

4.6 Lemma *(Properties of* $B_1^n := \Sigma_n$*). Given integers* $n \geqslant 1, 0 \leqslant c < b^n$, $0 \leqslant l < b^n$, *we have* $\sigma(c, 1) = c + 1$,

$$\sigma(b^n - 1, l) = \begin{cases} 1 & \text{if } l \text{ is even} \\ 0 & \text{if } l \text{ is odd} \end{cases}$$

and

$$\sigma(b^n-2,l)=\begin{cases}1+l/2 & \textit{if } l \textit{ is even}\\ -(l+1)/2 & \textit{if } l \textit{ is odd.}\end{cases}$$

Proof. The first formula results by induction from Lemma 4.2 (with the first row $\sigma(c,0)=1$).

For the second one, we note that, from Lemma 4.5, $\sigma(b^n-1,l)$ can take only two values; but $\sigma(b^n-1,0)=1$ and $\sigma(b^n-1,1)=b^n=0$ from the first formula of the present lemma.

Finally, the third formula is a consequence of the second together with lemma 4.2: $\sigma(b^n-2,l)+\sigma(b^n-2,l+1)=\sigma(b^n-1,l+1)$, so starting with $\sigma(b^n-2,0)=1$, step by step we get $\sigma(b^n-2,l+1)=-\left(1+\frac{l}{2}\right)=-\frac{(l+1)+1}{2}$ if l is even and $\sigma(b^n-2,l+1)=1+\frac{l+1}{2}$ if l is odd. □

4.7 Lemma *(Properties of $B_i^n:=\Sigma((i-1)b^n,ib^n;b^n,2b^n)$). Given integers $n\geqslant 1, 2\leqslant i\leqslant b, b^n\leqslant l<2b^n$, we have*

$$\sigma(ib^n-1,l)=\begin{cases}i & \textit{if } l \textit{ is odd}\\ 1 & \textit{if } l \textit{ is even}\end{cases};$$

moreover, there exist b^{n-1} integers l such that $\sigma(ib^n-2,l)=0$.

Proof. From Lemma 4.4, we have $\sigma(ib^n-1,b^n)=\sigma((i-1)b^n,b^n)=\sigma(i-1,1)=i$ (by Lemma 4.6); then Lemma 4.5 implies that $\sigma(ib^n-1,l)=i$ if l is odd; on the other hand, from Lemma 4.3, $\sigma(ib^n,l)=\sigma(ib^n,b^n)=i+1$ (by Lemma 4.4 and 4.6); but $\sigma(ib^n-1,l)+\sigma(ib^n-1,l+1)=\sigma(ib^n,l+1)=i+1$, so that $\sigma(ib^n-1,l+1)=1$ if l is odd and the first part is proved.

For the second part, it suffices to look at $\sigma(ib^n-2,l)$ for $b^n\leqslant l<b^n+b$; these entries are the sum of a power of 2 (sum of binomial coefficients from 0 to b^n-1) and of entries given by the third part of Lemma 4.6 times $(i-1)$ (because of the structure of the matrix C, see Lemma 3.1, the second row of blocks is $(i-1)C_1$ in the present case); therefore we add a power of 2 to $(i-1)$ times the integers between 1 and $b-1$ in the order $1,b-1,2,b-2,\ldots,\frac{b+1}{2}$; necessarily, we must get a zero entry. □

4.8 Lemma *(Property of the sub-matrix $\Sigma(rb^n,(r+1)b^n;sb^n,(s+1)b^n)$). Given integers $n\geqslant 1$, $s\geqslant 0$, $r\geqslant s$, we have (with the notations of Lemmas 4.6 and 4.7):*

$\Sigma(rb^n,(r+1)b^n;0,b^n)=B_1^n$

and for $s\geqslant 1, \Sigma(rb^n,(r+1)b^n;sb^n,(s+1)b^n))=uB_v^n$ with

$$u=\sigma(r,s-1) \textit{ and } \begin{cases}v=\sigma(r,s)/\sigma(r,s-1) & \textit{if } \sigma(r,s)\neq 0\\ v=b & \textit{if } \sigma(r,s)=0\end{cases},$$

if $\sigma(r,s-1)\neq 0$ and $(u=\sigma(r,s)$ and $v=1)$ if $\sigma(r,s-1)=0$.

In particular,

$$\Sigma((b-1)b^n,b^{n+1};lb^n,(l+1)b^n))=\begin{cases}B_1^n & \textit{if } l \textit{ is even}\\ B_b^n & \textit{if } l \textit{ is odd}\end{cases}\quad (0\leqslant l<b),$$

for $2 \leqslant i < b$

$$\Sigma((ib-1)b^n, ib^{n+1}; (b+l)b^n, (b+l+1)b^n)) = \begin{cases} B_i^n & \textit{if } l \textit{ is even} \\ iB_{1/i}^n & \textit{if } l \textit{ is odd} \end{cases} \quad (0 \leqslant l < b)$$

and

$$\Sigma((b^2-1)b^n, b^{n+2}; (b+l)b^n, (b+l+1)b^n) = \begin{cases} B_b^n & \textit{if } l \textit{ is even} \\ B_1^n & \textit{if } l \textit{ is odd} \end{cases} \quad (0 \leqslant l < b).$$

Proof. The first part is straightforward since the entries of the first row of Σ are equal to 1 and the entries under the diagonal are constant.

The second part is a direct consequence of Corollary 4.5: the last two entries (c,d) of the last column of a given block B determine the good multiple u of the good block B_v^n (with $(1,v)$ for the last two entries of the last column), such that $B = uB_v^n$: one has $u = c$ and $vc = d$; by reduction of the entries of the corners (Lemma 4.4) and taking into account the special cases $\sigma(r,s) = 0$ and $\sigma(r,s-1) = 0$, we get the formula of the second part of the lemma.

The particular cases will be useful in the next paragraphs; they describe the blocks of the last column of blocks of B_i^{n+1} and they follow by direct computation of the convenient uB_v^n from the results of the preceding lemmas: the first with $r = b-1$ and $s = l$, so that $u = \sigma(r, s-1) = 1$ or 0, and $v = 1$ or b; the second with $r = (i-1)b + b - 1 = ib - 1$ and $s = b + l$, so that $u = 1$ or i and $v = i$ or $1/i$; and the third with $r = b^2 - 1$ and $s = b + l$, so that $u = 1$, and $v = 1$ or b. □

Corollary *(Algorithmic construction of Σ). Above the diagonal (included), the $b^{n+1} \times b^{n+1}$ matrix $\Sigma_{n+1} = B_1^{n+1}$ is formed by $\frac{b(b+1)}{2}$ $b^n \times b^n$ sub-matrices which arise by multiplication from $B_1^n, B_2^n, \cdots, B_b^n$, the sub-matrices of the first two rows of Σ_{n+1}; therefore, it suffices to know the algorithm by which $B_1^n, B_2^n, \cdots, B_b^n$ arise from $B_1^{n-1}, B_2^{n-1}, \cdots, B_b^{n-1}$ to pass through n to $n+1$ and get Σ_{n+1} from Σ_n.*

See the example $b = 3$ in the next paragraph.

4.9 The counting matrix $A(\Sigma)$. From Lemma and Corollary 4.8, we know the algorithmic construction of Σ involves b blocks, $B_1^n, \ldots, B_b^n$ instead of one in the case of C; so we must take into account the composition of each block B_j^{n+1} by means of the b blocks B_i^n if we want to obtain the induction formula for the number of entries as in 3.3.

In the following, the indexes i, j, c, l are integers with $1 \leqslant i \leqslant b, 1 \leqslant j \leqslant b, 1 \leqslant c < b, 1 \leqslant l < b$.

Let $\nu_{l,j}^{(n+1)}$ be the number of entries in B_j^{n+1}, above (or on) the diagonals, belonging to the residue class l (remember corollary and definition 3.1 for the meaning of above (or on) the diagonals).

In order to express $\nu_{l,j}^{(n+1)}$ by means of the $\nu_{c,i}^{(n)}$, we need to compute the number $A_{c,i}^{l,j}$ of blocks of the form αB_i^n, where $\alpha = l/c \pmod b$, appearing in B_j^{n+1}; because again, in this way, an entry of B_i^n belonging to the residue class c (counted in $\nu_{c,i}^{(n)}$) becomes congruent to $\alpha c = l$ and so must be counted in $\nu_{l,j}^{(n+1)}$.

And again, as in 3.3, collecting the numbers $A_{c,i}^{l,j}$ in rows of indexes (l,j) and columns of indexes (c,i), we obtain the $b(b-1) \times b(b-1)$ matrix $A = A(\Sigma) = (A_{c,i}^{l,j})$ which gives the fundamental relation:

$$N^{(n+1)} = AN^{(n)} \quad \text{with} \quad {}^tN^{(n)} = (\nu_{1,1}^{(n)}, \cdots, \nu_{1,b}^{(n)}, \nu_{2,1}^{(n)}, \cdots, \nu_{2,b}^{(n)}, \cdots, \nu_{b-1,1}^{(n)}, \cdots \nu_{b-1,b}^{(n)}).$$

Remark. For our purpose, we need only the $\nu_{l,1}^{(n+1)}$, because $\Sigma_{n+1} = B_1^{n+1}$ and we are only interested by the entries of this matrix; but to obtain the $\nu_{l,1}^{(n+1)}$, we must compute all the $\nu_{c,i}^{(n)}$ and so we need the general recursion formula for all the blocks B_j^{n+1}.

Example. For $b = 3$, applying 4.8, we get the following expressions for the B_j^{n+1}, from which we deduce the matrix $A(\Sigma)$ (see [5] appendix for $b = 5$ and 7):

$$B_1^{n+1} = \begin{pmatrix} B_1^n & B_1^n & B_1^n \\ & B_2^n & B_3^n \\ & & B_1^n \end{pmatrix}, \qquad B_2^{n+1} = \begin{pmatrix} B_2^n & 2B_3^n & B_2^n \\ & B_1^n & 2B_2^n \\ & & B_2^n \end{pmatrix},$$

$$B_3^{n+1} = \begin{pmatrix} B_3^n & 2B_2^n & B_3^n \\ & B_3^n & B_1^n \\ & & B_3^n \end{pmatrix}, \qquad A(\Sigma) = \begin{pmatrix} 4 & 1 & 1 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 & 1 & 1 \\ 1 & 0 & 4 & 0 & 1 & 0 \\ 0 & 0 & 0 & 4 & 1 & 1 \\ 0 & 1 & 1 & 1 & 3 & 0 \\ 0 & 1 & 0 & 1 & 0 & 4 \end{pmatrix}.$$

By construction, the matrix $A(\Sigma)$ consists of $b \times b$ sub-matrices according to the following rule: given the first column (or row) of sub-matrices, the next ones result by permutations according to the square table of values of $\alpha = l/c \pmod b$, as in 3.3.

Proposition. *The matrix $A(\Sigma)$ is non-negative, irreducible, primitive and $\sum_{c,i} A_{c,i}^{l,j} = \sum_{l,j} A_{c,i}^{l,j} = \frac{b(b+1)}{2}$ for all integers i, j, c, l with $1 \leqslant i \leqslant b, 1 \leqslant j \leqslant b$, $1 \leqslant c < b$ and $1 \leqslant l < b$.*

Proof. For the irreducibility, we show that the directed graph associated to A is strongly connected (see [7]); we proceed in two steps: first, we prove that the diagonal $b \times b$ sub-matrix is irreducible; secondly we note that the connexions between the partial graphs corresponding to the diagonal sub-matrices exist if there is a non-zero entry in the non-diagonal sub-matrices, which is proved in the second step.

The first step is essentially a consequence of Lemmas 4.7 and 4.8: in each block B_j^{n+1} there is a block of the form B_1^n or B_b^n, because the naught entry of the penultimate column gives rise to the block B_b if the entry on its right is 1 and if not, it is the entry below which gives rise to the block B_1 (due to the structure of the last column and to Lemma 4.2); next the structure of B_1 (Lemma 4.6) shows that the first row of the diagonal $b \times b$ sub-matrix has non-zero entries and the structure of B_b (last column) shows that $A_{1,1}^{1,b} = \frac{(b-1)}{2} \neq 0$; this achieves the first part: the directed graph of the diagonal $b \times b$ sub-matrix is strongly connected.

The second step follows from the second particular case of Lemma 4.8: the last column of blocks in B_α^{n+1} contains $\frac{b-1}{2}$ blocks of the form $\alpha B_{1/\alpha}^n$, so we have $A_{c,i}^{l,j} \neq 0$ with $\alpha = l/c \neq 0$ corresponding to the non diagonal sub-matrix, $j = \alpha$ and $i = 1/\alpha$; qed for the second step.

The primitivity is straightforward because the diagonal entries of A are different from zero (see [7]) and the sums with fixed rows also, because we have exactly $\frac{b(b+1)}{2}$ blocks of order n in B_j^{n+1}.

The sums with fixed columns need more explanation: for c, i fixed, we are interested in the terms αB_i^n, with $\alpha = l/c$, appearing in B_j^{n+1} (for variable l,j); we show below that at the same place in every block B_j^{n+1} we have blocks uB_v^n with distincts values of v; in other words the correspondance $j \to v$ is one to one; so, for fixed c, i we get exactly $\frac{b(b+1)}{2}$ blocks uB_i^n with various u according to the value of l and to the selected place in B_j^{n+1}, hence $\sum_{l,j} A_{c,i}^{l,j} = \frac{b(b+1)}{2}$.

To prove our assertion above, we consider a fixed block in B_j^{n+1} $(j \geqslant 2)$ defined by the pair (r,s) with $0 \leqslant s \leqslant r < b$:

$$\Sigma((j-1)b^{n+1} + rb^n, (j-1)b^{n+1} + (r+1)b^n; b^{n+1} + sb^n, b^{n+1} + (s+1)b^n));$$

from Lemma 4.8, we have $v = 1 + (j-1)\binom{r}{s}/(2^r + (j-1)\sigma(r, s-1))$ except for particular cases corresponding to $v = 1$ or $v = b$; hence the correspondance $j \to v$ is one to one. □

4.10 Proof of Theorem 2. The spectral radius of $A(\Sigma)$ is again $\rho = \frac{b(b+1)}{2}$ and, from the primitivity, all the other eigenvalues λ of $A(\Sigma)$ verify $|\lambda| < \rho$. According to 4.8, we have $N^n = A^n N^0$ with $N^0 = {}^t(\nu_{l,j}^{(0)})$ where $\nu_{l,l}^{(0)} = 1$ and $\nu_{l,j}^{(0)} = 0$ for $l \neq j$ (because $\nu_{l,j}^{(0)}$ is the number of l in $B_j^0 = (j)$, matrix of order 1); moreover we have again $A^n = PJ^nP^{-1}$ with J the Jordan normal form of A and computing the matrix product with lemma 3.2 as in 3.4, we get the entries of A^n in the form $\frac{1}{b(b-1)}\rho^n + \sum_{i=1}^r P_i(\lambda_i)$ where P_i is a polynomial of degree n with less than $b(b-1)$ terms and where the λ_i are the other eigenvalues.

Now, the vector $N^{(0)}$ has $(b-1)$ entries equal to 1 and all other naught, so that all the entries of $N^{(n)}$ are of the form $\frac{1}{b}\rho^n + o(\rho^n)$, in particular the $\nu_{l,1}^{(n)}$ (for $1 \leqslant l < b$) which are the number of entries in $\Sigma_n = B_1^n$, above (or on) the diagonals, belonging to the residue class l; it remains the zero class which occurs also for the entries above (or on) the diagonals; but since $\rho^n = \left(\frac{b(b+1)}{2}\right)^n$ is the total number of these entries, by difference, we obtain the same proportion for the zero class. □

Example. For $b = 3$, we obtain:

$$J = \begin{pmatrix} 6 & & & & & \\ & 5 & & & O & \\ & & 4 & & & \\ & & & 3 & & \\ & O & & & 3 & \\ & & & & & 1 \end{pmatrix},$$

$$P = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 & 0 & -2 \\ 1 & 1 & -1 & 0 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 \\ 1 & 0 & -1 & -1 & 0 & 2 \\ 1 & -1 & 1 & 0 & -1 & 1 \end{pmatrix},$$

$$P^{-1} = \frac{1}{12} \begin{pmatrix} 2 & 2 & 2 & 2 & 2 & 2 \\ 3 & 0 & 3 & -3 & 0 & -3 \\ 2 & 2 & -2 & -2 & -2 & 2 \\ 2 & -4 & 2 & 2 & -4 & 2 \\ 2 & 2 & -4 & 2 & 2 & -4 \\ 1 & -2 & -1 & -1 & 2 & 1 \end{pmatrix}$$

so that the number of entries above (or on) the diagonals of Σ_n equal respectively to the digits 1, 2 and 0 is:

$$\begin{aligned} \nu_{1,1}^{(n)} &= \tfrac{1}{12}(4 \times 6^n + 3 \times 5^n + 2 \times 3^n + 3) \\ \nu_{2,1}^{(n)} &= \tfrac{1}{12}(4 \times 6^n - 3 \times 5^n + 2 \times 3^n - 3) \\ \nu_{0,1}^{(n)} &= \tfrac{1}{12}(4 \times 6^n - 4 \times 3^n). \end{aligned}$$

4.11 Problem. It is possible to define generalized binomial coefficients by the relation $\binom{c}{l}_f = \binom{c}{l} f^{c-l}$ (mod b), where $1 \leqslant f < b$, for which the Lucas formula and the recursion formula $\binom{c}{l}_f = f\binom{c-1}{l}_f + \binom{c-1}{l-1}_f$ hold.

It is easy to verify that Theorem 1 is still valid for the $\binom{c}{l}_f$; but concerning the corresponding matrix Σ^f, we have no proof for the irreducibility of its counting matrix $A(\Sigma^f)$ in all generality; nevertheless, in each case where we have effectively computed $A(\Sigma^f)$, we have deduced this property by means of its associated directed graph; on the other hand, the other properties of proposition 4.9 are still verified, so we state the hypothesis that Theorem 2 is also valid for Σ^f.

Acknowledgements: This revised version has been written during the stay of the author at the Macquarie University, Sydney; I want to thank Professor William Chen for his invitation and valuable cooperation at this occasion.

References

[1] Allouche J-P, Haeseler Fv, Lange E, Petersen A, Skordev G (1997) Linear cellular automata and automatic sequences. Parallel Computing **23**: 1577–1592

[2] Allouche J-P, Haeseler Fv, Peitgen H-O, Skordev G (1996) Linear cellular automata, finite automata and Pascal's triangle. Discrete Appl Math **66**: 1–22

[3] Barbolosi D, Grabner PJ (1996) Distribution des coefficients multinomiaux et q-binomiaux modulo p. Indag Math **7**: 129–135

[4] Faure H (1982) Discrépance de suites associées à un système de numération (en dimension s). Acta Arith **XLI**: 337–351

[5] Faure H (2000) On the Distribution of the sums of binomial coefficients modulo a prime. Halter-Koch F, Tichy R (Eds) Proc Internat Conf on Algebraic Number Theory and Diophantine Analysis, held in Graz, 1998, pp. 143–151. Berlin: W. de Gruyter

[6] Faure H, Chaix H (1996) Minoration de discrépance en dimension deux. Acta Arith **LXXVI**: 149–164

[7] Varga RS (1962) Matrix Iterative Analysis. Prentice-Hall

Author's address: H. Faure, Institut de Mathématiques de Luminy, U.P.R. 9016 CNRS, 163 avenue de Luminy, case 907, F-13288 Marseille Cedex 09, France