A combinatorial approach to rarefaction in b-multiplicative sequences.

Alexandre Aksenov

Journal de Théorie des Nombres
de Bordeaux 00 (XXXX), 000–000

A combinatorial approach to rarefaction in b-multiplicative sequences.

par Alexandre AKSENOV

Résumé. Pour une suite b-multiplicative donnée et un nombre premier p fixé, l'étude de la p-raréfaction consiste à caractériser le comportement asymptotique des sommes de premiers termes d'indices multiples de p. Sous une hypothèse (dite de «finitude») sur la suite, les valeurs entières du polynôme homogène «norme» à 3 variables, $\mathcal{N}_{p,i_1,i_2}(Y_0,Y_1,Y_2) := \prod_{j=1}^{p-1}\left(Y_0+\zeta_p^{i_1 j}Y_1+\zeta_p^{i_2 j}Y_2\right)$, où $i_1,i_2\in\{1,2,\ldots,p-1\}$, ζ_p est une racine p-ième primitive de l'unité, déterminent ce comportement asymptotique. On montre qu'une méthode combinatoire s'applique à $\mathcal{N}_{p,i_1,i_2}(Y_0,Y_1,Y_2)$ qui permet d'établir de nouvelles relations fonctionnelles entre les coefficients de ce polynôme «norme», diverses propriétés des coefficients de $\mathcal{N}_{p,i_1,i_2}(Y_0,Y_1,Y_2)$, notamment pour $i_1{=}1, i_2{=}2,3$; cette méthode fournit des relations entre coefficients binomiaux, de nouvelles preuves des deux identités $\prod_{j=1}^{p-1}\left(1+\zeta_p^j-\zeta_p^{2j}\right)=L_p$ (le p-ième nombre de Lucas) et $\prod_{j=1}^{p-1}\left(1-\zeta_p^j\right)=p$, le signe et le résidu modulo p des polynômes symétriques des $1+\zeta-\zeta_p^2$. Une méthode algorithmique de recherche des coefficients de $\mathcal{N}_{p,i_1,i_2}$ est développée.

Abstract. Given a b-multiplicative sequence and a prime p, studying the p-rarefaction consists in characterizing the asymptotic behaviour of the sums of the first terms indexed by the multiples of p. Under the "finiteness" assumption for the sequence, the integer values of the homogeneous "norm" 3-variate polynomial $\mathcal{N}_{p,i_1,i_2}(Y_0,Y_1,Y_2) := \prod_{j=1}^{p-1}\left(Y_0+\zeta_p^{i_1 j}Y_1+\zeta_p^{i_2 j}Y_2\right)$, where $i_1,i_2\in\{1,2,\ldots,p-1\}$, and ζ_p is a primitive p-th root of unity, determine this asymptotic behaviour. It will be shown that a combinatorial method can be applied to $\mathcal{N}_{p,i_1,i_2}(Y_0,Y_1,Y_2)$. The method enables deducing functional relations between the coefficients as well as various properties of the coefficients of $\mathcal{N}_{p,i_1,i_2}(Y_0,Y_1,Y_2)$, in particular for $i_1{=}1, i_2{=}2,3$. This method provides relations between binomial coefficients. It gives new proofs of the two identities $\prod_{j=1}^{p-1}\left(1-\zeta_p^j\right)=p$ and $\prod_{j=1}^{p-1}\left(1+\zeta_p^j-\zeta_p^{2j}\right)=L_p$ (the p-th Lucas number). The sign and the residue modulo p of the symmetric

2010 *Mathematics Subject Classification.* 05 A 10, 05 A 18, 11 B 39, 11 R 18.

polynomials of $1+\zeta-\zeta_p^2$ can also be obtained. An algorithm for computation of coefficients of $\mathcal{N}_{p,i_1,i_2}(Y_0,Y_1,Y_2)$ is developed.

1. Introduction

This article deals with a combinatorial method adapted to the coefficients of homogeneous 3-variate "norm" polynomials which determine the asymptotic behaviour of rarified sums of a sub-class of b-multiplicative sequences. The general definition of a b-multiplicative sequence of complex numbers can be written as:

$$t_{n+mb^i} = t_n t_{mb^i} \text{ for each } n, m, i \in \mathbb{N} \text{ such that } n < b^i.$$

We will be interested in the case where $t_{mb^i} = t_m$ (this condition will be called *the finiteness condition*). If a b-multiplicative sequence satisfies the finiteness condition and its values are either 0 or roots of unity, it is b-automatic. An example of such sequence is the Thue-Morse sequence defined by $b = 2, t_1 = -1$. A survey on the b-multiplicative sequences with values in an arbitrary compact group can be found in [4].

Rarified sums (the term is due to [5]) of a sequence (t_n) are the sums of initial terms of the subsequence $(t_{pn})_n$ (the *rarefaction step* p is supposed to be a prime number in this paper). It is proved in [6] that if (t_n) is the Thue-Morse sequence and $b = 2$ is a generator of the multiplicative group $\mathbb{F}_p^\times$, then

$$\sum_{n<N, p|n} t_n = O\left(N^{\frac{\log p}{(p-1)\log 2}}\right) \tag{1.1}$$

and this exponent cannot be decreased. For some prime numbers p the rarified sums are always positive, this phenomenon is discussed in [5].

The equation (1.1) can be generalized as:

$$\sum_{n<N, p|n} t_n = O\left(N^{\frac{\log \mathbf{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\sum_{j=0}^{b-1} t_j \zeta_p^j)}{(p-1)\log b}}\right) \tag{1.2}$$

for any b-multiplicative sequence (t_n) satisfying the finiteness condition, with values only in $\{-1, 0, 1\}$, such that

$$\left|\mathbf{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\sum_{j=0}^{b-1} t_j \zeta_p^j\right)\right| > \max\left((\sum_{j=0}^{b-1} t_n)^{p-1}, 1\right)$$

and such that $b < p$ is a generator of the multiplicative group $\mathbb{F}_p^\times$. The equation (1.2) uses the notation ζ_p for a primitive p-th root of unity and $\mathbf{N}_{L/K}$ for the norm. This result is proved in the Ph.D. thesis [1].

Indeed, the equation (1.2) generalizes (1.1) as the Thue-Morse sequence satisfies the conditions of validity of (1.2) and we get the following:

$$\mathbf{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\sum_{j=0}^{b-1} t_j\zeta_p^j\right) = \mathbf{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1-\zeta_p) = p.$$

The norms

$$\mathbf{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\sum_{j=0}^{b-1} t_j\zeta_p^j\right) \tag{1.3}$$

can also be calculated in a straightforward way if $b=3, t_0{=}t_1{=}1, t_2{=}{-}1$. Using the resultant of the two polynomials $S(X) = X^{p-1}+\ldots+1$ and $R(X){=}X^2{-}X{-}1$, one obtains

$$\mathbf{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1+\zeta_p-\zeta_p^2) = L_p \tag{1.4}$$

the p-th term of the Lucas sequence (referred as $A000032$ by OEIS, cf [11]) defined recursively by $L_0{=}2, L_1{=}1, L_{n+2} = L_n{+}L_{n+1}$.

The objective of this article is to study a "norm" expression similar to (1.3) in the case of some b-multiplicative sequences, which is constructed by introducing a finite number of new formal variables $Y_0, Y_1, \ldots, Y_d$ with $d \leqslant p-1$. The integer d can be defined as the number of nonzero terms in $t_1, t_2, \ldots, t_{b-1}$. The combinatorial method developed here concerns the case $d=2$; in general, if $d \geqslant 3$, it leads to too difficult computations[1]. Then, we are interested in the homogeneous polynomial of degree $p-1$ in 3 variables with integer coefficients

$$\mathcal{N}_{p,i_1,i_2}(Y_0,Y_1,Y_2) = \prod_{j=1}^{p-1}\left(Y_0+\zeta_p^{i_1 j}Y_1+\zeta_p^{i_2 j}Y_2\right), \tag{1.5}$$

where i_1, i_2 are two distinct elements of $\mathbb{F}_p^\times$. If all numbers t_c for $c \in \{1,\ldots,b-1\}\setminus\{i_1,i_2\}$ are zeroes, then the norm (1.3) is recovered as $\mathcal{N}_{p,i_1,i_2}(1,t_{i_1},t_{i_2})$. By definition, $\mathcal{N}_{p,i_1,i_2}(Y_0,Y_1,Y_2)$ is the norm of $(Y_0+\zeta_p^{i_1}Y_1+\zeta_p^{i_2}Y_2)$ as a polynomial in the 4 variables Y_0, Y_1, Y_2, ζ_p relative to the extension of fields $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ in the sense of the extended definition of norm introduced in [13].

The form (1.5) of "norm" polynomial reveals to be common for a large class of b-multiplicative sequences, either by setting the formal variables Y_0, Y_1, Y_2 to special values and/or fixing the two residue classes i_1, i_2. Since the form (1.5) inherits the properties of its coefficients, any functional relation between these coefficients can be considered as a key result.

[1] In [1] it is proved that the functional equation (Theorems 3.2 and 3.3) generalizes to the case $d \geqslant 3$

In this context, Sections 2 and 3 enunciate a combinatorial interpretation of the coefficients of $\mathcal{N}_{p,i_1,i_2}$ and the proof of a functional relation between them, which looks like the recurrence equation of the Pascal's triangle. This relation can be used to find closed formulas for some classes of coefficients (for *all* of them in the case $i_1 = 1, i_2 = 2$) and to find the remaining coefficients in a fast algorithmic way. A closed formula for these coefficients is a final goal.

In Section 4 we describe an algorithm in $O(p^2)$ additions that calculates the coefficients of (1.5) using this relation. We also re-prove the result (1.4) about the case $i_1 = 1, i_2 = 2$ and formulate two corollaries of the new proof. We also state some results about the case $i_1 = 1, i_2 = 3$.

Throughout the paper, $|X|$ and $\#X$ will both refer to the size of a finite set X, the symbol $\#$ followed by a system of equations, congruences or inequalities will denote the number of solutions; and $\sum X$, standing for $\sum_{x\in X} x$, will refer to the sum of a finite subset X of a commutative group with additive notation.

2. Combinatorics of partitions of a set.

In this section we are going to give an alternative proof of the formula

$$\prod_{j=1}^{j=p-1} \left(X - \zeta^j\right) = 1 + X + \ldots + X^{p-1}, \tag{2.1}$$

and the methods of this proof will be re-used in the proof of the functional equation in Section 3. The new proof uses the properties of the partially ordered sets Π_n of partitions of a set of size n (a good reference about the properties of those is the Chapter 3.10.4 of [12]). We are going to prove the following statement, which is equivalent to (2.1).

Lemma 2.1. *Let p be a prime number and $0 \leqslant n < p$ an integer. Define $A_0(n,p)$ as the number of subsets of $\mathbb{F}_p^\times$ of n elements that sum up to 0 modulo p and $A_1(n,p)$ the number of those subsets that sum up to 1. Then*

$$A_0(n,p) - A_1(n,p) = (-1)^n.$$

Let us begin the proof with an obvious observation: if we define similarly the numbers $A_2(n,p)$, $A_3(n,p)$, $\ldots$, $A_{p-1}(n,p)$, they will all be equal to $A_1(n,p)$, since multiplying a set that sums to 1 by a constant residue $c \in \mathbb{F}_p^\times$ gives a set that sums to c, and this correspondence is one-to-one.

Let us deal with a simpler version of the Lemma that allows repetitions and counts sequences instead of subsets, which is formalized in the following

Definition 1. Denote $E_x^{k_1,k_2,\ldots,k_n}(n,p)$ (where $x \in \mathbb{F}_p$ and $k_1, k_2, \ldots, k_n \in \mathbb{F}_p^\times$) the number of sequences $(x_1, x_2, \ldots, x_n)$ of elements of $\mathbb{F}_p^\times$ such that

$$\sum_{i=1}^{n} k_i x_i = x.$$

Then we get the following

Lemma 2.2. *If n is even,*

$$E_0^{k_1,k_2,\ldots,k_n}(n,p) = \frac{(p-1)^n+p-1}{p} \quad \text{and} \quad E_1^{k_1,k_2,\ldots,k_n}(n,p) = \frac{(p-1)^n-1}{p};$$

if n is odd,

$$E_0^{k_1,k_2,\ldots,k_n}(n,p) = \frac{(p-1)^n-p+1}{p} \quad \text{and} \quad E_1^{k_1,k_2,\ldots,k_n}(n,p) = \frac{(p-1)^n+1}{p}.$$

In both cases,

$$E_0^{k_1,k_2,\ldots,k_n}(n,p) - E_1^{k_1,k_2,\ldots,k_n}(n,p) = (-1)^n.$$

Proof. By induction on n. For $n = 0$ or $n = 1$ the result is trivial. For bigger n we always get:

$$E_0^{k_1,k_2,\ldots,k_n}(n,p) = (n-1)E_1^{k_1,k_2,\ldots,k_{n-1}}(n-1,p)$$

and

$$E_1^{k_1,k_2,\ldots,k_n}(n,p) = E_0^{k_1,k_2,\ldots,k_{n-1}}(n-1,p) + (p-2)E_1^{k_1,k_2,\ldots,k_{n-1}}(n-1,p),$$

since the sequences of length n of linear combination (with coefficients k_i) equal to x are exactly expansions of sequences of length $n-1$ of linear combination different from x, and this correspondence is one-to-one. Injecting formulas for $n-1$ concludes the induction. □

Now we are going to prove Lemma 2.1 for small n. If $n = 0$ or $n = 1$, Lemma is clear. For $n = 2$, there is one more sequence $(x, y) \in \mathbb{F}_p^{\times 2}$ that sums up to 0, but that counts the sequences of the form (x, x) which should be removed. Since p is prime, these sequences contribute once for every nonzero residue modulo p, and removing them increases the zero's "advantage" to 2. Now, we have to identify (x, y) and (y, x) to be the same, so we get the difference 1 back, establishing Lemma 1 for $n = 2$.

For $n = 3$, counting all the sequences $(x, y, z) \in \mathbb{F}_p^\times$ gives a difference $E_0 - E_1 = -1$. The sequences (x, x, z) contribute one time more often to the sum equal to 0, so removing them adds -1 to the total difference. The same thing applies to sequences of the form (x, y, y) and (x, y, x). After removing them, we get an intermediate difference of -4, but the triples of the form (x, x, x) have been removed 3 times, which is equivalent to saying they count -2 times. Therefore, they should be "reinjected" with coefficient 2. As p is prime and bigger than 3, the redundant triples contribute once for each

nonzero residue; therefore we accumulate the difference of $-4-2=-6$. We have then to identify permutations, that is to divide the score by 6 which gives the final result -1.

Here is the explicit calculation for the case $n=4$:

$$\begin{array}{ll}
1 & \text{(corresponds to } E_0(4,p)-E_1(4,p)\text{)} \\
+6 & \text{(for removing } \begin{array}{lll}(x,x,y,z), & (x,y,x,z), & (x,y,z,x),\\ (x,y,y,z), & (x,y,z,y), & (x,y,z,z)\end{array}\text{)} \\
+2\times 4 & \text{(for re-injecting } \begin{array}{lll}(x,x,x,y), & (x,x,y,x),\\ (x,y,x,x) & \text{and } (x,y,y,y)\end{array}\text{)} \\
+1\times 3 & \text{(for re-injecting } (x,x,y,y),(x,y,x,y) \text{ and } (x,y,y,x)\text{)} \\
+6\times 1 & \text{(for removing } (x,x,x,x)\text{)} \\
=24 &
\end{array}$$

which is 4!, therefore Lemma 2.1 is proved for $n=4$.

For a general n we can calculate the difference between the number of sequences that sum up to 0 and the number of those that sum up to 1 by assigning to all sequences in $\mathbb{F}_p^{\times n}$ an intermediate coefficient equal to one, then by reducing it by one for each couple of equal terms, then increasing by 2 for each triple of equal terms, and so on, proceeding by successive adjustments of coefficients, each step corresponding to a "poker combination" of n cards. If after adding the contributions of all the steps and the initial $(-1)^n$, we get $(-1)^n n!$, Lemma 2.1 is valid for n independently from p provided that $p>n$ is prime.

Let us introduce a formalization of these concepts using the notions exposed in [7]. Call a *partition* of the set $\{1,2,\ldots,n\}$ a choice of pairwise disjoint nonempty subsets $B_1,B_2,\ldots,B_c$ of $\{1,2,\ldots,n\}$ of non-increasing sizes $|B_i|$, and such that $B_1\cup B_2\cup\ldots\cup B_c=\{1,2,\ldots,n\}$. The set Π_n of all partitions of $\{1,2,\ldots,n\}$ is partially ordered by reverse refinement: for each two partitions τ and π, we say that $\tau\geqslant\pi$ if each block of π is included in a block of τ. We define the Möbius function $\mu(\hat{0},x)$ on Π_n recursively by:
if $x=\{\{1\},\{2\},\ldots,\{n\}\}=\hat{0}$, then $\mu(\hat{0},x)=1$;
if x is bigger than $\hat{0}$, then

$$\mu(\hat{0},x)=-\sum_{\substack{y\in\Pi_n\\ y<x}}\mu(\hat{0},y).$$

By the Corollary to the Proposition 3 section 7 of [10] and the first Theorem from the section 5.2.1 of [7], if x is a subdivision of type $(\lambda_1,\lambda_2,\ldots,\lambda_n)$,

then

$$\mu(\hat{0}, x) = \prod_{i=1}^{n} (-1)^{\lambda_i - 1}(\lambda_i - 1)! \tag{2.2}$$

This formula will be useful in Section 3.

We are also going to use the following definition: let $x = (x_1, x_2, \ldots, x_n)$ be a sequence of n nonzero residues modulo p seen as a function

$$x : \{1, 2, \ldots, n\} \to \mathbb{F}_p^\times.$$

Then the *coimage* of x is the partition of $\{1, 2, \ldots, n\}$, whose blocks are the nonempty preimages of elements of $\mathbb{F}_p^\times$. Now we can prove the following proposition that puts together all the previous study.

Lemma 2.3. *The difference*

$$A_0(n, p) - A_1(n, p)$$

does not depend on p provided that p is a prime number bigger than n.

Proof. We are going to describe an algorithm that computes this difference (which is the one applied earlier for small values of the argument). For each subdivision $x \in \Pi_n$, denote by $r_0(x, p)$ the number of sequences $(x_1, x_2, \ldots, x_n)$ of elements of $\mathbb{F}_p^\times$ of coimage x that sum up to 0, and denote by $r_1(x, p)$ the number of those sequences of coimage x that sum up to 1 and denote $r(x, p) = r_0(x, p) - r_1(x, p)$. Then,

$$n!(A_0(n, p) - A_1(n, p)) = r(\hat{0}, p).$$

Denote, for each subdivision y of $\{1, 2, \ldots, n\}$,

$$s(y, p) = \sum_{x \geqslant y} r(x, p).$$

Then, by Proposition 2.2,

$$s(y, p) = (-1)^{c(y)} \tag{2.3}$$

where $c(y)$ is the number of blocks in the subdivision y. By the Möbius inversion formula (see [7]),

$$r(\hat{0}, p) = \sum_{y \in \Pi_n} \mu(\hat{0}, y) s(y, p) = \sum_{y \in \Pi_n} (-1)^{c(y)} \mu(\hat{0}, y). \tag{2.4}$$

If we compute this sum, we get the value of $A_0(n, p) - A_1(n, p)$ in a way that does not depend on p. □

The last move consists in proving that

$$\sum_{y \in \Pi_n} (-1)^{c(y)} \mu(\hat{0}, y) = (-1)^n n! \tag{2.5}$$

in a way that uses the equivalence with Lemma 2.1. This proof may seem to be artificial because it is no longer used in the Section 3, and a purely combinatorial and more general proof exists: see the final formula of Chapter 3.10.4 of [12].

Remark that $A_0(n,p) = A_0(n,p-1-n)$ since saying that the sum of some subset of $\mathbb{F}_p^\times$ is 0 is equivalent to saying that the sum of its complement is 0. For the same kind of reason, $A_1(n,p) = A_{-1}(n,p-1-n) = A_1(n,p-1-n)$.

Now we can prove Lemma 2.1 by induction on n. It has already been proved for small values of n. If $n > 4$, by Bertrand's postulate, there is a prime number p' such that $n < p' < 2n$. Replace p by p' (by the proposition 2.3 this leads to an equivalent statement), then n by $p' - 1 - n$ (using the above remark). As $p' - 1 - n < n$, the step of induction is done.

This proof can be analysed from the following point of view: how fast does the number of steps of induction grow as function of n? Suppose that one step of induction reduces Lemma 2.1 for n to Lemma 2.1 for the number $f(n)$ and denote by $R(n)$ the number of steps of induction needed to reach one of the numbers 0 or 1 (the formal definitions will follow). We can prove then the following upper bound on $R(n)$.

Theorem 2.1. *Let*

$$\text{nextprime}(n) := \min\{p > n, p \text{ prime}\}$$

and

$$f(n) := \text{nextprime}(n) - n - 1$$

for each $n \in \mathbb{N}$. Further, denote

$$R(n) := \min\{k, f^k(n) \in \{0,1\}\}.$$

This definition makes sense, for $f(n) < n$ for each $n > 1$ by the Bertrand's postulate.

The function $R(n)$ satisfies the estimation

$$R(n) = O(\log\log n). \tag{2.6}$$

Proof. Denote $\theta = 0.525$. By Theorem 1 of [2], there is a constant N_0 such that for all $n > N_0$, the interval $[n - n^\theta, n]$ contains a prime number. We are going to deduce from this the following result: for each $\bar\theta \in]0.525, 1[$ there exists a constant N_1 such that $n > N_1$ implies $f(n) < n^{\bar\theta}$.

Indeed, suppose $n > N_0$ and denote $\bar p = \text{nextprime}(n) - 1$. Then, by the result cited above,

$$n \geqslant \bar p - \bar p^\theta. \tag{2.7}$$

The function

$$\begin{array}{rccc} u: & [N_0, +\infty[& \to & [u(N_0), +\infty[\\ & x & \mapsto & x - x^\theta \end{array}$$

is strictly increasing, continuous and equivalent to x. Therefore, the same is valid for its inverse u^{-1}. By (2.7), $\bar{p} \leqslant u^{-1}(n)$, therefore

$$\forall n > N_1 \ f(n) = \bar{p} - n \leqslant \bar{p}^{\theta} \leqslant (u^{-1}(n))^{\theta} < n^{\bar{\theta}} \tag{2.8}$$

for each $\bar{\theta} \in]\theta, 1[$ and for a bound $N_1 \geqslant N_0$ that may depend on $\bar{\theta}$.

The end of the proof is analogous to that of Theorem 1.1 of [8]. Denote by l the integer such that $f^{l+1}(n) < N_1 \leqslant f^l(n)$. Then:

$$n^{\bar{\theta}^l} \geqslant N_0$$

therefore

$$l \log \bar{\theta} + \log \log n \geqslant \log \log N_1$$

which implies

$$l \leqslant -\frac{\log \log n}{\log \bar{\theta}}.$$

Put $b = \max_{1 \leqslant m \leqslant N_0} R(m)$, it is a constant. We get:

$$R(n) \leqslant l + 1 + b \leqslant -\frac{\log \log n}{\log \bar{\theta}} + 1 + b$$

which proves our claim. □

3. Pascal's equation.

We are going to prove the functional equation verified by the coefficients of the polynomial $P_{i_1,i_2}(Y_0, Y_1, Y_2)$ (introduced in (1.5)). To do this, we are going to describe a combinatorial interpretation of these numbers.

Definition 2. Let p, i_1, i_2 be fixed as in Introduction and n_1, n_2 be non-negative integers such that $n_1 + n_2 \leqslant p - 1$. Define

(3.1)

$$C_i^{i_1,i_2}(n_1, n_2, p) = \#\left\{ (x_1, \ldots, x_{n_1+n_2}) \in \mathbb{F}_p^{\times n_1+n_2} \;\middle|\; \begin{array}{c} x_k \neq x_l \text{ if } k \neq l, \\ i_1 \sum_{k=1}^{n_1} x_k + i_2 \sum_{k=n_1+1}^{n_1+n_2} x_k = i \end{array} \right\}$$

and

(3.2)

$$A_i^{i_1,i_2}(n_1, n_2, p) = \#\left\{ (X_1, X_2) \in \mathcal{P}(\mathbb{F}_p^{\times})^2 \;\middle|\; \begin{array}{c} |X_1| = n_1, |X_2| = n_2, \\ X_1 \cap X_2 = \emptyset, \\ i_1 \sum X_1 + i_2 \sum X_2 = i \end{array} \right\}.$$

Definition 2 matches with the notations from the previous section because of the identity $A_i^{i_1,i_2}(n,0,p) = A_i^{i_1,i_2}(0,n,p) = A_i(n,p)$ (independently from i_1, i_2).

From this definition one can see that

$$C_1^{i_1,i_2}(n_1,n_2,p) = \ldots = C_{p-1}^{i_1,i_2}(n_1,n_2,p),$$
$$\sum_{i=0}^{p-1} C_i^{i_1,i_2}(n_1,n_2,p) = (p-1)\ldots(p-n_1-n_2),$$

and for any i, $A_i^{i_1,i_2}(n_1,n_2,p) = \frac{C_i^{i_1,i_2}(n_1,n_2,p)}{n_1!n_2!}$.

Only one linear equation should be added to these in order to be able to determine all the numbers defined by (3.1) and (3.2). Proposition 3.1 below suggests to research the value of

$$\triangle^{i_1,i_2}(n_1,n_2,p) = A_0^{i_1,i_2}(n_1,n_2,p) - A_1^{i_1,i_2}(n_1,n_2,p) = \sum_{\substack{X_1, X_2 \subset \mathbb{F}_p^\times \\ |X_1| = n_1, |X_2| = n_2, \\ X_1 \cap X_2 = \emptyset}} \zeta_p^{i_1 \sum X_1 + i_2 \sum X_2}.$$

We can express the symmetric polynomials of the quantities $(Y_0 + \zeta_p^{i_1 j} Y_1 + \zeta_p^{i_2 j} Y_2)$ in terms of the previously defined numbers via the following

Proposition 3.1. *Let i_1, i_2 be two different elements of $\mathbb{F}_p^\times$ and denote by $\sigma_{v,(j=1,\ldots,p-1)}$ the elementary symmetric polynomial of degree v in quantities that depend on an index j varying from 1 to $p-1$. Then we have the following formal expansion:*

$$\sigma_{p-1-\delta,(j=1,\ldots,p-1)}\left(Y_0 + \zeta_p^{i_1 j} Y_1 + \zeta_p^{i_2 j} Y_2\right) = \sum_{\substack{0 \leqslant n_0, n_1, n_2 \leqslant p-1 \\ n_0 + n_1 + n_2 = p-1 \\ n_0 \geqslant \delta}} \binom{n_0}{\delta} \triangle^{i_1,i_2}(n_1,n_2,p) Y_0^{n_0-\delta} Y_1^{n_1} Y_2^{n_2}. \tag{3.3}$$

In particular,

$$\mathcal{N}_{p,i_1,i_2}(Y_0,Y_1,Y_2) = \sum_{\substack{0 \leqslant n_0, n_1, n_2 \leqslant p-1 \\ n_0 + n_1 + n_2 = p-1}} \triangle^{i_1,i_2}(n_1,n_2,p) Y_0^{n_0} Y_1^{n_1} Y_2^{n_2}. \tag{3.4}$$

Proof. The symmetric polynomial develops as:

$$\begin{aligned}
&\sigma_{p-1-\delta,(j=1,\dots,p-1)}\left(Y_0+\zeta_p^{i_1 j}Y_1+\zeta_p^{i_2 j}Y_2\right)\\
&\qquad=\sum_{\substack{X\subset\mathbb{F}_p^\times,\\ |X|=p-1-\delta}}\ \prod_{j\in X}\left(Y_0+\zeta_p^{i_1 j}Y_1+\zeta_p^{i_2 j}Y_2\right)\\
&=\sum_{\substack{X\subset\mathbb{F}_p^\times,\\ |X|=p-1-\delta}}\ \sum_{\substack{X_0,X_1,X_2,\\ X_0\cup X_1\cup X_2=X,\\ X_0,X_1,X_2 \text{ disjoint}}}\zeta_p^{i_1\sum X_1+i_2\sum X_2}Y_0^{|X_0|}Y_1^{|X_1|}Y_2^{|X_2|}\\
&\qquad=\sum_{\substack{X_0',X_1,X_2,\\ X_0'\cup X_1\cup X_2=\mathbb{F}_p^\times\\ X_0',X_1,X_2 \text{ disjoint}}}\binom{|X_0'|}{\delta}\zeta_p^{i_1\sum X_1+i_2\sum X_2}Y_0^{|X_0'|-\delta}Y_1^{X_1}Y_2^{X_2}.
\end{aligned}$$

When we group the terms of this sum by sizes $n_0=|X_0'|, n_1=|X_1|, n_2=|X_2|$ we obtain (3.3). □

The following closed formula for the coefficients $\triangle^{i_1,i_2}(n_1,n_2,p)$ is valid under a condition: the multiset consisting of i_1 with multiplicity n_1 and of i_2 with multiplicity n_2 should have no nonempty subset of sum multiple of p (this holds, for example, if the smallest positive representatives of i_1 and i_2 verify $n_1 i_1+n_2 i_2<p$). The proof of Lemma 2.1 can then be generalized to get:

$$\triangle^{i_1,i_2}(n_1,n_2,p)=(-1)^{n_1+n_2}\binom{n_1+n_2}{n_1}. \tag{3.5}$$

The complete proof of this statement can be established as a corollary of the Theorem 3.3 below.

Without this condition (3.5) becomes false: for example, $\triangle^{2,3}(1,1,5)=-3$. For the general case, we are going to replace the closed formula by a recursive equation in which the parameters i_1,i_2,p are fixed, and the recursion is on different values of n_1,n_2. The equation is similar to the equation of the Pascal's triangle, and can be formulated as follows:

Theorem 3.2 ("Colored" Pascal's equation)**.** *Let p be an odd prime, and $i_1,i_2\in\mathbb{F}_p^\times$, $n_1,n_2\in\{1,\dots,p-2\}$ such that $i_1\neq i_2$ and $n_1+n_2<p$.*

Then,

$$C_0^{i_1,i_2}(n_1,n_2,p) - C_1^{i_1,i_2}(n_1,n_2,p) \equiv \tag{3.6}$$
$$n_1 C_1^{i_1,i_2}(n_1-1,n_2,p) + n_2 C_1^{i_1,i_2}(n_1,n_2-1,p) -$$
$$- n_1 C_0^{i_1,i_2}(n_1-1,n_2,p) - n_2 C_0^{i_1,i_2}(n_1,n_2-1,p) \bmod p$$

and if $p \nmid n_1 i_1 + n_2 i_2$*, the equality*

$$C_0^{i_1,i_2}(n_1,n_2,p) - C_1^{i_1,i_2}(n_1,n_2,p) = \tag{3.7}$$
$$n_1 C_1^{i_1,i_2}(n_1-1,n_2,p) + n_2 C_1^{i_1,i_2}(n_1,n_2-1,p) -$$
$$- n_1 C_0^{i_1,i_2}(n_1-1,n_2,p) - n_2 C_0^{i_1,i_2}(n_1,n_2-1,p)$$

holds.

Proof. Define

$$f_k = \begin{cases} i_1 & \text{if } k \in \{1,\dots,n_1\} \\ i_2 & \text{if } k \in \{n_1+1,\dots,n_1+n_2\} \end{cases} \tag{3.8}$$

We are going to call a *hindrance* a subset X of $\{1,\dots,n_1+n_2\}$ such that $\sum_{m\in X} f_m \equiv 0 \bmod p$. If there are no hindrances, then, by following the proof of Lemma 2.1, we get

$$C_0^{i_1,i_2}(n_1,n_2,p) - C_1^{i_1,i_2}(n_1,n_2,p) = (-1)^{n_1+n_2}(n_1+n_2)!$$

and this number is the opposite of n times $(-1)^{n-1}(n-1)!$.

In general, the formula (2.4) should be replaced by:

$$s(y,p) = (1-p)^{d(y)}(-1)^{c(y)} \tag{3.9}$$

if the partition y of $\{1,\dots,n_1+n_2\}$ contains $d(y)$ blocks that are hindrances. Indeed, suppose that the blocks of y are $B_1,\dots,B_c$, and for each bloc B_j we denote $f_{B_j} = \sum_{m\in B_j} f_m \in \mathbb{F}_p$. Then, the solutions $(x_1,\dots,x_{n_1+n_2})$ of

$$\sum_{k=1}^{n_1+n_2} f_k x_k = i,$$

such that the coimages x of $(x_1,\dots,x_{n_1+n_2})$ satisfy $x \geqslant y$ (as partitions), are in one-to-one correspondence to solutions $(x_{B_1},\dots,x_{B_c})$ of

$$\sum_{j=1}^{c} f_{B_j} x_{B_j} = i$$

where $x_{B_j} \in \mathbb{F}_p^\times$ are no longer required to be distinct. Proposition 2.2 states that if we pay no attention to the indices j that correspond to hindrances (i.e. such that $f_{B_j} = 0$), the difference between numbers of solutions of $\sum_j f_{B_j} x_{B_j} = 0$ and $\sum_j f_{B_j} x_{B_j} = 1$ is $(-1)^{c-d(y)}$. Moreover, the values of

x_{B_j} where B_j are hindrances can be chosen arbitrarily (from $p-1$ options each). The product of these contributions leads to (3.9).

The formula (3.9) can be rewritten as

$$s(y,p) = \sum_{l=0}^{d(y)} \sum_{\substack{X_1, X_2, \ldots, X_l \\ \text{hindrances contained in } y}} (-1)^{c(y)-l} p^l$$

where the order of $X_1, X_2, \ldots, X_l$ is irrelevant in the sum. Then we get:

(3.10)
$$C_0^{i_1,i_2}(n_1,n_2,p) - C_1^{i_1,i_2}(n_1,n_2,p) = \sum_{y \in \Pi_n} \mu(\hat{0},y) s(y,p)$$

(3.11)
$$= \sum_{\substack{X_1, X_2, \ldots, X_l \\ \text{disjoint hindrances}}} \sum_{\substack{y \in \Pi_n \\ y \text{ contains } X_1, \ldots, X_l \\ \text{as blocks}}} (-1)^{c(y)-l} \mu(\hat{0},y) p^l$$

(3.12)
$$= \sum_{X_1,\ldots,X_l} (-1)^{|X_1|+|X_2|+\ldots+|X_l|-l} (|X_1|-1)!(|X_2|-1)! \ldots (|X_l|-1)! p^l$$
$$\times \sum_{\substack{y \in \Pi_n \\ y \text{ contains } X_1, \ldots, X_l}} \mu(\hat{0}, y - X_1 - X_2 - \ldots - X_l) (-1)^{c(y-X_1-X_2-\ldots-X_l)}$$

by factoring $\mu(\hat{0},y)$ according to the formula (2.2). In the last sum, $(y - X_1 - X_2 - \ldots - X_l)$ denotes the partition y, where the blocs $X_1, \ldots, X_l$ are removed (which is a partition of $(n_1 + n_2 - |X_1| - \ldots - |X_l|)$ elements). By applying (2.5) to the last sum of (3.12), we get

(3.13)
$$C_0^{i_1,i_2}(n_1,n_2,p) - C_1^{i_1,i_2}(n_1,n_2,p) = \sum_{X_1,\ldots,X_l} (|X_1|-1)!(|X_2|-1)! \ldots (|X_l|-1)! (-1)^{n_1+n_2-l} p^l (n_1+n_2-|X_1|-\ldots-|X_l|)!.$$

From (3.13),

(3.14)
$$C_0^{i_1,i_2}(n_1,n_2,p) - C_1^{i_1,i_2}(n_1,n_2,p) \equiv (-1)^{n_1+n_2}(n_1+n_2)! \bmod p,$$

which implies (3.6).

Suppose that $\{1,\dots,n_1+n_2\}$ is not a hindrance. In order to prove (3.7), remark that the sum (3.13) can be split as

$$\sum_{X_1,\dots,X_l} (|X_1|-1)!(|X_2|-1)!\dots(|X_l|-1)!(-1)^{n_1+n_2-l}$$
$$p^l(n_1+n_2-|X_1|-\dots-|X_l|)! =$$
$$-\sum_{m=1}^{n_1+n_2} \sum_{\substack{X_1,X_2,\dots,X_l \\ \text{disjoint hindrances} \\ \text{not containing } m}} (|X_1|-1)!(|X_2|-1)!\dots(|X_l|-1)!$$
$$(-1)^{n_1+n_2-l-1}p^l(n_1+n_2-|X_1|-\dots-|X_l|-1)!$$

then gathered into two parts according to the values of f_m:

$$C_0^{i_1,i_2}(n_1,n_2,p) - C_1^{i_1,i_2}(n_1,n_2,p) =$$
$$-n_1 \sum_{\substack{X_1,X_2,\dots,X_l \\ \text{disjoint hindrances} \\ \text{not containing } 1}} (|X_1|-1)!(|X_2|-1)!\dots(|X_l|-1)!$$
$$(-1)^{n_1+n_2-l-1}p^l(n_1+n_2-|X_1|-\dots-|X_l|-1)!$$
$$-n_2 \sum_{\substack{X_1,X_2,\dots,X_l \\ \text{disjoint hindrances} \\ \text{not containing } n_1+1}} (|X_1|-1)!(|X_2|-1)!\dots(|X_l|-1)!$$
$$(-1)^{n_1+n_2-l-1}p^l(n_1+n_2-|X_1|-\dots-|X_l|-1)!$$

By identifying each sum in the last formula to the right-hand side of (3.13) with one of the arguments n_1 or n_2 decreased by 1, we get (3.7). □

The numbers $\triangle^{i_1,i_2}(n_1,n_2,p)$ satisfy a similar equation.

Theorem 3.3 ("Uncolored" Pascal's equation)**.** *Let p be an odd prime, and $i_1,i_2 \in \mathbb{F}_p^\times$, $n_1,n_2 \in \{1,\dots,p-2\}$ such that $i_1 \neq i_2$ and $n_1+n_2<p$. Then,*

(3.15)
$$\triangle^{i_1,i_2}(n_1,n_2,p) \equiv -\triangle^{i_1,i_2}(n_1-1,n_2,p) - \triangle^{i_1,i_2}(n_1,n_2-1,p) \bmod p$$

and if $p \nmid n_1i_1+n_2i_2$, the equality

(3.16)
$$\triangle^{i_1,i_2}(n_1,n_2,p) = -\triangle^{i_1,i_2}(n_1-1,n_2,p) - \triangle^{i_1,i_2}(n_1,n_2-1,p)$$

holds.

Proof. Division of both sides of (3.6) by $n_1!n_2!$ (which is not multiple of p) gives (3.15) and division by the same number of (3.7) gives (3.16). □

4. Some properties of finite Pascal's triangles.

4.1. Algorithm. Let us define formally $\triangle^{i_1,i_2}(n_1,n_2) = 0$ when one of n_1, n_2 is negative or $n_1+n_2 \geqslant p$. Then (3.16) is valid for any $n_1, n_2 \in \mathbb{N}^2$ such that $p \nmid n_1 i_1 + n_2 i_2$. Indeed: if $n_1 = 0$ or $n_2 = 0$, the identification $A^{i_1,i_2}(n_1,n_2,p) = A(\max(n_1,n_2),p)$ implies (3.16) via Lemma 2.1. When $n_1+n_2 = p-1$, one can use the hypothesis $X_1 \cup X_2 = \mathbb{F}_p^\times$ and the identity $\sum \mathbb{F}_p^\times = 0$ to prove

$$i_1 \sum X_1 + i_2 \sum X_2 = (i_1 - i_2) \sum X_1,$$

which implies $A_i^{i_1,i_2}(n_1,n_2,p) = A_i^{i_1-i_2,i_2}(n_1,0,p)$, therefore $\triangle^{i_1,i_2}(n_1,n_2) = (-1)^{n_1}$. The equation (3.16) is valid, therefore, when $n_1+n_2 = p$.

We can now prove that the functional relation (3.16), together with these border values, characterizes the function $\triangle^{i_1,i_2}(\cdot,\cdot,p)$ as a function defined on $\mathbb{Z}^2_{\geqslant -1}$, with values in $\mathbb{Z}$.

Theorem 4.1. *Let p be an odd prime, let i_1, i_2 be two distinct elements of $\{1,\dots,p-1\}$, and let $d : \mathbb{Z}^2_{\geqslant -1} \to \mathbb{Z}$ be a function such that*

(4.1) $\quad d(0,0) = 1,$

(4.2) $\quad d(n_1,n_2) = 0$ *if* $n_1 < 0, n_2 < 0$ *or* $n_1+n_2 \geqslant p,$

(4.3) $\quad d(n_1,n_2) + d(n_1-1,n_2) + d(n_1,n_2-1) = 0$ *if* $p \nmid n_1 i_1 + n_2 i_2.$

Then, $d(n_1,n_2) = \triangle^{i_1,i_2}(n_1,n_2,p)$.

Proof. Define $\delta(n_1,n_2) = d(n_1,n_2) - \triangle^{i_1,i_2}(n_1,n_2,p)$. Then the function δ satisfies (4.2), (4.3) and $\delta(0,0) = 0$. In order to prove the theorem we should prove that $\delta = 0$.

By applying (4.3) successively to $n_2 = 0$ and $n_1 = 1,\dots,p-1$ one proves that $\delta(0,0) = -\delta(1,0) = \delta(2,0) = \dots = \delta(p-1,0)$. By applying it to $n_1 = 0$ and $n_2 = 1,\dots,p-1$ one proves that $\delta(0,0) = -\delta(0,1) = \dots = \delta(0,p-1)$.

Let us prove the identity $\delta(n_1,n_2) = 0$ by induction on $\tilde{n} := p-n_1-n_2 \in \{0,\dots,p-2\}$. If $\tilde{n} = 0$, then $\delta(n_1,n_2) = 0$ as a part of the hypothesis (4.2).

Suppose that the Theorem is proved for $\tilde{n} \in \{0,\dots,p-3\}$, let us prove it for $\tilde{n}+1$. Denote (n_1^S, n_2^S) the solution of

$$\begin{cases} i_1 n_1^S + i_2 n_2^S \equiv 0 \bmod p \\ n_1^S + n_2^S = p - \tilde{n} \\ (n_1^S, n_2^S) \in \{1,\dots,p\}^2. \end{cases}$$

If one applies the functional relation (4.3) to a point where $n_2 = p - \tilde{n} - n_1$ (with the restriction $n_1 \neq n_1^S$), and uses the induction hypothesis, one gets

$$\delta(n_1 - 1, p - \tilde{n} - n_1) + \delta(n_1, p - \tilde{n} - n_1 - 1) = 0. \tag{4.4}$$

By applying (4.4) successively to $n_1 = 1, \ldots, n_1^S - 1$, we prove $\delta(n_1, p - \tilde{n} - n_1 - 1) = 0$ for n_1 in the same range $1, \ldots, n_1^S - 1$. If $n_1^S \geqslant p - \tilde{n} - 1$, this concludes the step of induction. Otherwise, by applying (4.4) successively to $n_1 = p - \tilde{n} - 1, \ldots, n_1^S + 1$ (in the decreasing order of values of n_1), we prove $\delta(n_1, p - \tilde{n} - n_1 - 1) = 0$ for n_1 in the range $p - \tilde{n}, \ldots, n_1^S$.

This concludes the induction and proves $\delta(n_1, n_2) = 0$ for all (n_1, n_2). □

The previous proof corresponds to the Algorithm 1, which computes the values of the function $\triangle^{a,b}(x, y, p)$ line by line. It executes one addition per number to compute, therefore its execution time is proportional to the size of the answer.

Given an odd prime p and two distinct elements i_1, i_2 of $\mathbb{F}_p^\times$, we are going to call the array of all values of $\triangle^{i_1,i_2}(n_1, n_2, p)$ for $n_1, n_2 \geqslant 0, n_1 + n_2 < p$ a *finite Pascal's triangle*, and we will use geometrical terminology when it seems to make exposition simpler.

We are going to call *sources* the points (n_1, n_2) such that $p | i_1 n_1 + i_2 n_2$. Define

$$f^{i_1,i_2}(n_1, n_2, p) = \triangle^{i_1,i_2}(n_1, n_2, p) + \triangle^{i_1,i_2}(n_1 - 1, n_2, p) + \triangle^{i_1,i_2}(n_1, n_2 - 1, p). \tag{4.5}$$

The value of $f^{i_1,i_2}(n_1, n_2, p)$ (which we will call *force*) is nonzero only at sources, where it can be computed using (3.13) combined with the end of the proof of Theorem 3.2:

$$n_1! n_2! f^{i_1,i_2}(n_1, n_2, p) = \sum_{\substack{X_1, X_2, \ldots, X_l \\ \text{partition of } \{1, \ldots, n_1 + n_2\}, \\ \forall j \; p | \sum_{m \in X_j} f_m}} (|X_1| - 1)!(|X_2| - 1)! \ldots (|X_l| - 1)! (-1)^{n_1 + n_2 - l} p^l (n_1 + n_2 - |X_1| - \ldots - |X_l|)!. \tag{4.6}$$

This formula uses the notation (3.8) in order to describe the fact that summation goes through all partitions of $\{1, \ldots, n_1 + n_2\}$ into hindrances.

The definition (4.5) implies, by linearity of the Pascal's equation:

$$\triangle^{i_1,i_2}(n_1, n_2, p) = \sum_{\substack{0 \leqslant k \leqslant n_1 \\ 0 \leqslant l \leqslant n_2 \\ p | i_1 k + i_2 l}} f^{i_1,i_2}(k, l, p) (-1)^{n_1 + n_2 - k - l} \binom{n_1 + n_2 - k - l}{n_1 - k}. \tag{4.7}$$

Algorithm 1 Calculate a finite Pascal's triangle. Arguments p, a, b: p prime, $0 < a < b < p$

Allocate *the integer array* data$[0..p-1][0..p-1]$ (values of $\triangle^{a,b}(x, y, p)$),
the boolean array reg$[0..p-1][0..p-1]$ (information about sources)
for $x = 0, .., p-1, y = 0, .., p-1$ **do**
    reg$[x][y] = (a \cdot x + b \cdot y \not\equiv 0 \bmod p)$
end for
data$[0][0]$ =data$[p-1][0]$ =data$[0][p-1] = 1$
  resolution at the edges
for $x = 1, \ldots, p-2$ **do** data$[x][p-1-x] = -$data$[x-1][p-x]$ **end for**
for $x = 1, \ldots, p-2$ **do** data$[x][0] = -$data$[x-1][0]$ **end for**
for $y = 1, \ldots, p-2$ **do** data$[0][y] = -$data$[0][y-1]$ **end for**
  resolution inside
for $n = p-2, .., 1$ **do**
    for $x = 1, .., n-1$ **do**
        $y \leftarrow n - x$
        if reg$[x][y+1]$ **then**
            data$[x][y] = -$data$[x-1][y+1] -$ data$[x][y+1]$
        else
            Stop the inner loop
        end if
    end for
    for $y = 1, .., n-1$ **do**
        $x \leftarrow n - y$
        if reg$[x+1][y]$ **then**
            data$[x][y] = -$data$[x+1][y-1] -$ data$[x+1][y]$
        else
            Stop the inner loop
        end if
    end for
end for
  Print the result
for $n = 0, .., p-1$ **do**
    for $y = 0, .., n$ **do**
        Print data$[n-y][y]$, reg$[n-y][y]$
    end for
    Print newline
end for

$$
\begin{array}{ccccccccccccccccccccc}
 & & & & & & & & +1 & & & & & & & & & & \\
 & & & & & & & -1 & & -1 & & & & & & & & & \\
 & & & & & & +1 & & +2 & & +1 & & & & & & & & \\
 & & & & & -1 & & -3 & & -3 & & -1 & & & & & & & \\
 & & & & +1 & & +4 & & +6 & & +4 & & +1 & & & & & & \\
 & & & -1 & & -5 & & -10 & & -10 & & -5 & & -1 & & & & & \\
 & & +1 & & +6 & & +15 & & +20 & & +15 & & -5_{\blacklozenge} & & +1 & & & & \\
 & -1 & & -7 & & -21 & & -35 & & +20_{\blacklozenge} & & -10 & & +4 & & -1 & & & \\
+1 & & +8 & & +28 & & -21_{\blacklozenge} & & +15 & & -10 & & +6 & & -3 & & +1 & & \\
 & -1 & & -9 & & +8_{\blacklozenge} & & -7 & & +6 & & -5 & & +4 & & -3 & & +2 & & -1 \\
+1 & & -1_{\blacklozenge} & & +1 & & -1 & & +1 & & -1 & & +1 & & -1 & & +1 & & -1 & & +1
\end{array}
$$

FIGURE 1. Coefficients of $\prod_{j=1}^{10}\left(X+\zeta_{11}^{j}Y+\zeta_{11}^{2j}Z\right)$

4.2. The case $i_1 = 1, i_2 = 2$. We can find a closed formula for the numbers $\triangle^{1,2}(n_1, n_2, p)$ using the identity

$$\triangle^{1,2}(n_1, n_2, p) = \triangle^{1,2}(n_1, p-1-n_1-n_2, p). \tag{4.8}$$

It follows indeed from the fact that for each disjoint couple $X_1, X_2 \subset \mathbb{F}_p^\times$, as in the definition (3.2),

$$\sum X_1 + 2\sum X_2 = -\left(\sum X_1 + 2\sum(\mathbb{F}_p^\times \setminus X_1 \setminus X_2)\right).$$

Formula (3.5) applies to at least one side of (4.8) for each (n_1, n_2) (and to both sides of (4.8) if $n_1 + 2n_2 = p-1$), leading to

$$\triangle^{1,2}(n_1, n_2, p) = \begin{cases} (-1)^{n_1+n_2}\binom{n_1+n_2}{n_1} & \text{if } n_1+2n_2 \leqslant p-1 \\ (-1)^{n_2}\binom{p-1-n_2}{n_1} & \text{if } n_1+2n_2 \geqslant p-1. \end{cases} \tag{4.9}$$

Therefore, this Pascal's triangle is symmetric with respect to the axis $n_1 + 2n_2 = p-1$.

One can deduce (1.4) from (4.9) in the following way: by (3.4),

$$\prod_{j=1}^{j=p-1}\left(1+\zeta_p-\zeta_p^2\right)=\sum_{n_1,n_2\in\mathbb{N}}(-1)^{n_2}\triangle^{1,2}(n_1,n_2,p) \tag{4.10}$$

$$=\sum_{n_1,n_2\in\mathbb{N}}(-1)^{n_2-1}(\triangle^{1,2}(n_1-1,n_2,p)+\triangle^{1,2}(n_1,n_2-1,p)-f^{1,2}(n_1,n_2,p))$$

$$=\sum_{n_1,n_2\in\mathbb{N}}((-1)^{n_2-1}\triangle^{1,2}(n_1,n_2-1,p)-(-1)^{n_2}\triangle^{1,2}(n_1-1,n_2,p)$$

$$+(-1)^{n_2}f^{1,2}(n_1,n_2,p))$$

$$=\sum_{n_1,n_2\in\mathbb{N}}(-1)^{n_2}f^{1,2}(n_1,n_2,p)$$

because massive cancellation occurs in the sum of differences of values of the function $(-1)^y\triangle^{1,2}(x,y,p)$.

Suppose $n_1,n_2>0$ and $n_1+2n_2=p$ (therefore n_1 is odd). Then

(4.11)

$$f^{1,2}(n_1,n_2,p)=\triangle^{1,2}(n_1-1,n_2,p)+\triangle^{1,2}(n_1,n_2-1,p)+\triangle^{1,2}(n_1,n_2,p)$$

$$=(-1)^{n_2}\binom{n_1+n_2-1}{n_1-1}+2(-1)^{n_2}\binom{n_1+n_2-1}{n_1}$$

$$=(-1)^{n_2}\left(\binom{n_1+n_2}{n_1}+\binom{n_1+n_2-1}{n_1}\right)$$

$$=(-1)^{n_2}\left(\binom{p-n_2}{n_2}+\binom{p-n_2-1}{n_2-1}\right).$$

The absolute value of (4.11) can be interpreted as the number of ways to put n_2 identical disjoint dominoes on a discrete circle of length p. Indeed (see also [3]), for any $k\leqslant\frac{p-1}{2}$

$$\#\{k \text{ disjoint dominoes on a circle of length } p\} \tag{4.12}$$

$$=\#\{k \text{ disjoint dominoes on a line segment of length } p\}$$

$$+\#\{k-1 \text{ disjoint dominoes on a line segment of length } p-2\}$$

$$=\binom{p-k}{k}+\binom{p-k-1}{k-1}.$$

The sum (4.10) contains three terms not covered by the hypotheses of (4.11): these correspond to $n_1{=}n_2{=}0$, $n_1{=}p, n_2{=}0$, $n_1{=}0, n_2{=}p$ and they equal respectively 1, 1 and -1. The overall contribution of these terms can be identified to the number of ways to put 0 dominoes on a discrete circle of length p. Therefore, the norm (4.10) equals to the number of ways to

put any number of identical disjoint dominoes on a discrete circle of length p, which is proved in [3] to be L_p.

For example, if $p = 11$, the numbers are those of Figure 1 (⧫ denotes a source).

4.3. Application: an identity for binomial coefficients. The formulas (3.4) and (4.10) have another application. As $1 - \zeta_p + \zeta_p^2 = \frac{1+\zeta_p^3}{1+\zeta_p}$, we get in a similar way to (4.10):

$$1 = \prod_{j=1}^{j=p-1} \left(1 - \zeta_p + \zeta_p^2\right) = \sum_{n_1,n_2\in\mathbb{N}} (-1)^{n_1} \triangle^{1,2}(n_1, n_2, p) = \sum_{n_1,n_2\in\mathbb{N}} (-1)^{n_1} f^{1,2}(n_1, n_2, p). \tag{4.13}$$

We further get:

$$1 = 1 + \sum_{n_1,n_2\in\mathbb{N}^*} (-1)^{n_1} f^{1,2}(n_1, n_2, p) = 1 - \sum_{n_1,n_2\in\mathbb{N}^*} f^{1,2}(n_1, n_2, p). \tag{4.14}$$

The formula (4.11) leads to the following combinatorial identity[2]:

$$\sum_{k=1}^{\frac{p-1}{2}} (-1)^k \left(\binom{p-k}{k} + \binom{p-k-1}{k-1} \right) = 0. \tag{4.15}$$

4.4. Second application: expression for a symmetric polynomial. We can formulate an expression for an arbitrary symmetric polynomial of the numbers $(1 + \zeta_p^j - \zeta_p^{2j})$ which is:

Theorem 4.2. *Let $p \geqslant 5$ be prime and $\delta \in \{0, \ldots, p-2\}$ an integer. Then $\sigma_{p-1-\delta,(j=1,\ldots,p-1)}(1 + \zeta_p^j - \zeta_p^{2j})$ (see the notation of Proposition 3.1) equals $\binom{p-1}{\delta}$ plus the sum of "weights" of ways of putting a number $n>0$ of disjoint dominoes on a discrete circle of length p, the weights being $\binom{n-1}{\delta}$.*

As a consequence, $\sigma_{p-1-\delta}(1 + \zeta - \zeta^2) > 0$ and $\sigma_{p-1-\delta}(1 + \zeta - \zeta^2) \equiv \binom{p-1}{\delta} \bmod p$.

[2]The previous proof implies (4.15) in the case of prime $p\geqslant 5$. The Zeilberger's algoritm (implemented in Maple 17, see also Chapter 6 of the book [9]) generalizes it for any $p\geqslant 5$ congruent to 1 or 5 modulo 6

Proof. By Proposition 3.1, we get a similar expression to (4.10)

$$\begin{aligned}(4.16)\quad &\sigma_{p-1-\delta,(j=1,\dots,p-1)}\left(1+\zeta_p^j+\zeta_p^{2j}\right)\\ &=\sum_{n_1,n_2\in\mathbb{N}}(-1)^{n_2}\binom{p-1-n_1-n_2}{\delta}\triangle^{1,2}(n_1,n_2,p)\\ &=\sum_{\tilde{n}=1}^{p}\sum_{\substack{n_1,n_2\\ n_1+n_2=p-\tilde{n}}}(-1)^{n_2}\binom{\tilde{n}-1}{\delta}\\ &\quad(-\triangle^{1,2}(n_1-1,n_2,p)-\triangle^{1,2}(n_1,n_2-1,p)+f^{1,2}(n_1,n_2,p))\\ &=\sum_{\tilde{n}=1}^{p}\sum_{\substack{n_1,n_2\\ n_1+n_2=p-\tilde{n}}}(-1)^{n_2}\binom{\tilde{n}-1}{\delta}f^{1,2}(n_1,n_2,p).\end{aligned}$$

The identity (4.11) leads to

$$\begin{aligned}(4.17)\quad &\sigma_{p-1-\delta,(j=1,\dots,p-1)}\left(1+\zeta_p^j+\zeta_p^{2j}\right)\\ &=\binom{p-1}{\delta}+\sum_{n_2=1}^{\frac{p-1}{2}}\binom{n_2-1}{\delta}\left(\binom{p-n_2}{n_2}+\binom{p-n_2-1}{n_2-1}\right)\end{aligned}$$

and the discussion that follows the formula (4.11) identifies each number $(-1)^{n_2}f^{1,2}(n_1,n_2,p)$ as the number of ways to put n_2 disjoint dominoes on a discrete circle of length p. □

$$
\begin{array}{ccccccccccccccccccccc}
 & & & & & & & +1 & & & & & & & & & & & & & \\
 & & & & & & -1 & & -1 & & & & & & & & & & & & \\
 & & & & & +1 & & +2 & & +1 & & & & & & & & & & & \\
 & & & & -1 & & -3 & & -3 & & -1 & & & & & & & & & & \\
 & & & +1 & & +4 & & +6 & & +4 & & +1 & & & & & & & & & \\
 & & -1 & & -5 & & -10 & & +12_{\blacklozenge} & & -5 & & -1 & & & & & & & & \\
 & +1 & & +6 & & +15 & & -2 & & -7 & & +6 & & +1 & & & & & & & \\
 -1 & & -7 & & +12_{\blacklozenge} & & -13 & & +9 & & +1 & & -7 & & -1 & & & & & & \\
 & +1 & & +8 & & -5 & & +1 & & +4 & & -10 & & +6 & & -3_{\blacklozenge} & & +1 & & & \\
 & -1 & & +2_{\blacklozenge} & & -3 & & +4 & & -5 & & +6 & & +4 & & -3 & & +2 & & -1 & \\
+1 & & -1 & & +1 & & -1 & & +1 & & -1 & & +1_{\blacklozenge} & & -1 & & +1 & & -1 & & +1
\end{array}
$$

FIGURE 2. Coefficients of $\prod_{j=1}^{10}\left(X+\zeta_{11}^{j}Y+\zeta_{11}^{3j}Z\right)$

4.5. The case $i_1 = 1, i_2 = 3$. In this case the formula

$$\triangle^{1,3}(n_1,n_2,p) = \triangle^{2,3}(n_1, p-1-n_1-n_2, p) \tag{4.18}$$

is analogous to (4.8) and implies

$$\triangle^{1,3}(n_1,n_2,p) = \begin{cases} (-1)^{n_1+n_2}\binom{n_1+n_2}{n_1} & \text{if } n_1+3n_2 \leqslant p-1 \\ (-1)^{n_2}\binom{p-1-n_2}{n_1} & \text{if } n_1+3n_2 \geqslant 2p-2 \text{ or} \\ & \quad n_1+3n_2 = 2p-4, \end{cases} \tag{4.19}$$

therefore, in two regions, the coefficients of the triangle are identical to the previous case.

The coefficients in the middle region can be calculated using the general formula (4.7). Let us specify different quantities used there, namely the position of sources and the associated forces. The sources are the integer points situated on two lines: the *upper* line with equation $n_1+3n_2 = p$ and the *lower* line with equation $n_1+3n_2 = 2p$. One can see that the number of integer points on the upper line of sources is

$$\#\left\{\begin{array}{c} 0<n_1<p \\ 0<n_2<p \\ n_1+3n_2=p \end{array}\right\} = [\frac{p}{3}] \tag{4.20}$$

and the number of integer points on the lower line is

$$\#\left\{\begin{array}{c} 0<n_1<p \\ 0<n_2<p \\ n_1+3n_2=2p \end{array}\right\} = \mathrm{rnd}(\frac{p}{6}), \tag{4.21}$$

the closest integer to $\frac{p}{6}$.

If (n_1, n_2) is a point on the upper line of sources, the value of $f^{1,3}(n_1, n_2, p)$ has a simple expression given by (4.6):

$$f^{1,3}(n_1, n_2, p) = \frac{(n_1 + n_2 - 1)!p}{n_1!n_2!} \tag{4.22}$$

because the sum consists of the single term associated to $X{=}\{1, \ldots, n_1{+}n_2\}$. Under the same hypotheses, (4.7) implies

$$\triangle^{1,3}(n_1, n_2, p) = \frac{(n_1 + n_2 - 1)!p}{n_1!n_2!} - \binom{n_1 + n_2}{n_1} = 2\binom{n_1{+}n_2{-}1}{n_1}. \tag{4.23}$$

In any point (n_1, n_2) such that $p \leqslant n_1 + 3n_2 < 2p$, the formula (4.7) takes the following form:

$$\begin{aligned}\triangle^{1,3}(n_1, n_2, p) &= (-1)^{n_1+n_2}\binom{n_1 + n_2}{n_1} \\ &+ \sum_{\substack{0<k\leqslant n_1 \\ 0<l\leqslant n_2 \\ p = i_1k+i_2l}} f^{1,3}(k, l, p)(-1)^{n_1+n_2-k-l}\binom{n_1{+}n_2{-}k{-}l}{n_1 - k}.\end{aligned} \tag{4.24}$$

We can also compute a simple expression for the forces of sources on the lower line. Suppose that $n_1, n_2 > 0$ and $n_1 + 3n_2 = 2p$. Then, by (4.5) and (4.18),

$$\begin{aligned}f^{1,3}(n_1, n_2, p) &= \triangle^{1,3}(n_1, n_2, p) + \triangle^{1,3}(n_1 - 1, n_2, p) + \triangle^{1,3}(n_1, n_2 - 1, p) \\ &= f^{2,3}(n_1, p - n_1 - n_2, p).\end{aligned} \tag{4.25}$$

By (4.6) (the sum, once again, consists of a single term because $2n_1 + 3(p{-}n_1{-}n_2){=}p$),

$$f^{2,3}(n_1, p - n_1 - n_2, p) = \frac{(-1)^{n_2}(p - n_2 - 1)!p}{n_1!(p - n_1 - n_2)!}. \tag{4.26}$$

For example, if $p = 11$, the numbers are those of Figure 2 (⧫ denotes a source).

References

[1] A.Aksenov, *Raréfaction dans les suites b-multiplicatives*. PhD thesis, University of Grenoble (2014).

[2] R.Baker, G.Harman and J.Pintz, *The difference between consecutive primes - II*. Proc. London Math. Soc., (3) **83** (2001), 532-562.

[3] A.T. Benjamin, J.J. Quinn, *The Fibonacci Numbers – Exposed More Discretely*, Mathematics Magazine vol **76** n°3 (June 2003), 182–192.

[4] M. Drmota and J.Morgenbesser, *Generalized Thue-Morse sequence of Squares*, Israel J. Math. **190** (2012), 157–193.

[5] M. DRMOTA and M.SKAŁBA, *Rarified sums of the Thue-Morse sequence*, Trans. Amer. Math. Soc. **352** (1999), 609–640.
[6] S.GOLDSTEIN, K.KELLY and E.SPEER, *The Fractal Structure of Rarefied Sums of the Thue-Morse Sequence*, J. Number Theory **42** (1992), 1–19.
[7] J.P.S.KUNG, G.-C.ROTA and C.-H.YAN, *Combinatorics: The Rota Way*, Cambridge University Press (2009).
[8] F.LUCA and R.THANGADURAI, *On an arithmetic function considered by Pillai*, J. Théor. Nombres Bordeaux, Tome 21, n°3 (2009), p. 695–701.
[9] M.PETKOVŠEK, H.S.WILF and D.ZEILBERGER, $A = B$, A K Peers, LTD., Wellesley, MA, 1996.
[10] G.-C.ROTA, *On the Foundations of Combinatorial Theory I. Theory of Möbius Functions*, Z. Wahrscheinlichkeitstheorie **2** (1964), 340–368.
[11] On-Line Encyclopedia of Integer Sequences, at `http://oeis.org`
[12] R.P.STANLEY, *Enumerative combinatorics*, Cambridge University Press (1997).
[13] B.M.TRAGER, *Algebraic Factoring and Rational Function Integration*, Proceeding of the 1976 ACM Symposium on Symbolic and Algebraic Computation.

Alexandre AKSENOV
Institut Fourier, UMR 5582
100, rue des Maths, BP 74
38402 St Martin d'Hères Cedex, France
E-mail : `Oleksandr.Aksenov@ujf-grenoble.fr`