JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Alexandre AKSENOV

Counting solutions without zeros or repetitions of a linear congruence and rarefaction in *b*-multiplicative sequences.

Tome 27, n° 3 (2015), p. 625-654.

<http://jtnb.cedram.org/item?id=JTNB_2015__27_3_625_0>

Journal de Théorie des Nombres
de Bordeaux **27** (2015), 625–654

Counting solutions without zeros or repetitions of a linear congruence and rarefaction in *b*-multiplicative sequences.

par Alexandre AKSENOV

Résumé. Pour une suite fortement b-multiplicative donnée et un nombre premier p fixé, l'étude de la p-raréfaction consiste à caractériser le comportement asymptotique des sommes des premiers termes d'indices multiples de p. Les valeurs entières du polynôme « norme » trivarié

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

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 les 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 $1{+}\zeta_p{-}\zeta_p^2$. Une méthode algorithmique de recherche des coefficients de $\mathcal{N}_{p,i_1,i_2}$ est développée.

Abstract. Consider a strongly b-multiplicative sequence and a prime p. Studying its p-rarefaction consists in characterizing the asymptotic behaviour of the sums of the first terms indexed by the multiples of p. The integer values of the "norm" 3-variate polynomial

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

Manuscrit reçu le 28 février 2014, révisé le 16 décembre 2014, accepté le 17 février 2015.
Mathematics Subject Classification. 05A10, 05A18, 11B39, 11R18.
Mots-clefs. Thue-Morse sequence, b-multiplicative sequences, rarefactions, cyclotomic extensions, Lucas numbers, binomial coefficients, set partitions.

where ζ_p is a primitive p-th root of unity, and $i_1, i_2 \in \{1, 2, \ldots, p-1\}$, 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 $i_1 = 1$ and $i_2 = 2, 3$. 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 polynomials of $1+\zeta_p-\zeta_p^2$ 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 strongly b-multiplicative sequence. The general definition of a strongly b-multiplicative sequence of complex numbers (see [2]) can be written as:

Definition 1.1. Let $(t_n)_{n\geqslant 0}$ be a sequence of complex numbers and $b \geqslant 2$ an integer. The sequence $(t_n)_{n\geqslant 0}$ is called
emphstrongly b-multiplicative if it satisfies, for each $n \in \mathbb{N}$, the equation

$$t_n = \prod_{i=0}^{l} t_{c_i},$$

where $n = \sum_{i=0}^{l} c_i b^i$ is the b-ary expansion of a natural integer n. Additionally, we ask that $t_0 = 1$ or t_n is identically zero.

This definition ensures that t_n does not depend on the choice of the b-ary expansion of n (for b-ary expansions which may or may not start with zeroes). If the values of a strongly b-multiplicative sequence are either 0 or roots of unity, it is b-automatic. An example of such sequence is the $\{1, -1\}$-valued Thue-Morse sequence defined by $b = 2, t_1 = -1$ (referred as $A106400$ in OEIS, cf [16]). Further in this text we are going to refer to this sequence as the *Thue-Morse sequence*. A survey on the strongly b-multiplicative sequences with values in an arbitrary compact group can be found in [6].

Rarified sums (or p-rarified sums, the term is due to [7]) of a sequence $(t_n)_{n\geqslant 0}$ are the sums of initial terms of the subsequence $(t_{pn})_{n\geqslant 0}$ (the *rarefaction step* p is supposed to be a prime number in this paper). The problem of estimating the speed of growth of these sums has been studied in [8],[5],[9],[10],[11]. The following result has been proved in a special case.

Proposition 1.2 (see [9], Theorem 5.1)**.** *Let $(t_n)_{n\geqslant 0}$ be the Thue-Morse sequence. Suppose that $b=2$ 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.

We are going to study this problem in a more general case. In Section 2 we generalize Proposition 1.2 to Proposition 2.2 valid for a large subclass of strongly b-multiplicative sequences (with different values of b). Proposition 2.2 describes the speed of growth of p-rarified sums of a strongly b-multiplicative sequence in a form

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

similar to (1.1). The more general formula (1.2) contains the quantity

$$\xi\left((t_n)_{n\geqslant 0}, p\right) := \mathbf{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\sum_{j=0}^{b-1} t_j \zeta_p^j\right). \tag{1.3}$$

The properties of this norm expression provide information about the speed of growth of rarified sums. In Sections 3, 4, 5 we develop a method to study these norms.

Denote by $d((t_n)_{n\geqslant 0})$ the number of nonzero terms among $t_1, \dots, t_{b-1}$. For technical reasons, the method described in this article concerns only the strongly b-multiplicative sequences such that $d((t_n)_{n\geqslant 0})\leqslant 2$; in general, if $d \geqslant 3$, it leads to too difficult computations. On the other hand, the case where $d((t_n)_{n\geqslant 0})=1$ (which concerns, for example, the Thue-Morse sequence) is relatively easy. In the short description of the method, which follows, we assume that $d((t_n)_{n\geqslant 0})=2$.

Our method consists in dealing with a strongly b-multiplicative sequence of monomials instead of the initial strongly b-multiplicative sequence of complex numbers. Let $i_1, i_2 \in \{1, \dots, b-1\}$ be the two indices such that $t_{i_1}\neq 0$ and $t_{i_2}\neq 0$. Then the strongly b-multiplicative sequence of monomials associated with the sequence $(t_n)_{n\geqslant 0}$ and the choice of the order of i_1, i_2 is

defined by

$$\begin{aligned} T_0 &= 1, \\ T_{i_1} &= Y_1, \\ T_{i_2} &= Y_2, \\ T_c &= 0 \text{ if } c \in \{1, \dots, b{-}1\} \setminus \{i_1, i_2\} \\ T_n &= \prod_{i=0}^{l} T_{c_i} \text{ otherwise,} \end{aligned}$$

where $n = \sum_{i=0}^{l} c_i b^i$ is the b-ary expansion of a natural integer n.

Clearly, $T_n{=}0$ if and only if $t_n{=}0$. For example, if $b{=}3$ and $i_1{=}1, i_2{=}2$ then the sequence $(T_n)_{n\geqslant 0}$ starts with

$$1, Y_1, Y_2, Y_1, Y_1^2, Y_1Y_2, Y_2, Y_1Y_2, Y_2^2, \dots$$

If $b{=}5$ and $i_1{=}1, i_2{=}2$, it starts with

$$1, Y_1, Y_2, 0, 0, Y_1, Y_1^2, Y_1Y_2, 0, 0, Y_2, \dots$$

One can define the p-rarefied sums of the sequence $(T_n)_{n\geqslant 0}$ and the formal object

$$\prod_{j=1}^{p-1} \left(\sum_{c=0}^{b-1} \zeta_p^{jc} T_c \right) \tag{1.4}$$

which plays the role of $\xi\left((T_n)_{n\geqslant 0}, p\right)$. One can write (1.4) explicitly as

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

and homogenize this polynomial, which defines

$$\mathcal{N}_{p,i_1,i_2}(Y_0, Y_1, Y_2) = \prod_{j=1}^{p-1} \left(Y_0 + \zeta_p^{i_1 j} Y_1 + \zeta_p^{i_2 j} Y_2\right). \tag{1.6}$$

The norm (1.3) is then recovered as the value $\mathcal{N}_{p,i_1,i_2}(1, t_{i_1}, t_{i_2})$. 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 [18].

The form (1.6) of "norm" polynomial reveals to be common for the strongly b-multiplicative sequences which satisfy $d((t_n)_{n\geqslant 0}){=}2$ (as defined above). In order to retrieve a particular sequence from this form, one should set the formal variables Y_0, Y_1, Y_2 to special values, fix the two residue classes i_1, i_2 and take a base b (bigger than the smallest positive representatives of i_1, i_2, and such that the residue class of b modulo p is in $\mathbb{F}_p^\times$, and it

generates this multiplicative group). Since the form (1.6) inherits the properties of its coefficients, any functional relation between these coefficients can be considered as a key result.

In this context, Sections 3 and 4 enunciate a combinatorial interpretation of the coefficients of $\mathcal{N}_{p,i_1,i_2}$ in terms of the following counting problem.

Problem 1.3. *Let p be a prime number, let $\mathbf{f}$ be a vector of length $p-1$, all elements of which are residue classes modulo p among $0, i_1, i_2$ (i.e., $\mathbf{f}\in\{0,i_1,i_2\}^{p-1}\subset\mathbb{F}_p^{p-1}$). Let i be an element of $\mathbb{F}_p$. Find the number of vectors $\mathbf{x}\in\mathbb{F}_p^{p-1}$ which are permutations of $(1,2,\dots,p-1)$ and such that*

$$\mathbf{f}\cdot\mathbf{x}=i.$$

The equivalence of Problem 1.3 and the problem of determining the coefficients of $\mathcal{N}_{p,i_1,i_2}$ is made explicit in Proposition 4.2.

Our main result is the following.

Theorem 1.4 (equivalent to Theorem 4.5)**.** *Let p be an odd prime, and $i_1, i_2 \in \mathbb{F}_p^\times$ such that $i_1 \neq i_2$. Denote by $\triangle^{i_1,i_2}(n_1,n_2,p)$ the coefficient of the term $Y_0^{p-1-n_1-n_2}Y_1^{n_1}Y_2^{n_2}$ in $\mathcal{N}_{p,i_1,i_2}(Y_0,Y_1,Y_2)$. Fix exponents $n_1, n_2 \in \{1,\dots,p-2\}$ such that $n_1+n_2<p$. Then,*

$$\triangle^{i_1,i_2}(n_1,n_2,p)\equiv-\triangle^{i_1,i_2}(n_1-1,n_2,p)-\triangle^{i_1,i_2}(n_1,n_2-1,p) \bmod p \tag{1.7}$$

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

$$\triangle^{i_1,i_2}(n_1,n_2,p)=-\triangle^{i_1,i_2}(n_1-1,n_2,p)-\triangle^{i_1,i_2}(n_1,n_2-1,p) \tag{1.8}$$

holds.

The relation (1.8) (similar to the recurrence equation of the Pascal's triangle) 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 5 we describe an algorithm in $O(p^2)$ additions that calculates the coefficients of (1.6) using this relation. We study the case $i_1=1, i_2=2$ and re-prove the result

$$\prod_{j=1}^{p-1}\left(1+\zeta_p^j-\zeta_p^{2j}\right)=L_p, \tag{1.9}$$

the p-th Lucas number (i.e., the p-th term of the sequence referred as *A*000032 by OEIS, cf [16]). We 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.

The results of this article (except Theorem 3.5 and Subsection 5.5) are part of the Ph.D. thesis [1].

2. Partial sums of a stronly q-multiplicative sequence.

We are going to prove an asymptotic result about partial sums of a strongly q-multiplicative sequence used in the proof of Proposition 2.2.

Lemma 2.1. *Let $q\geqslant 2$ be an integer and consider a strongly q-multiplicative sequence $(\tau_n)_{n\geqslant 0}$ of complex numbers of absolute value smaller than or equal to 1. Denote the partial sums of $(\tau_n)_{n\geqslant 0}$ by*

$$\psi(N) := \sum_{n<N} \tau_n \ (N \in \mathbb{N}).$$

Then we have the following.

If $|\psi(q)| \leqslant 1$, then

$$\psi(N) = O(\log N). \tag{2.1}$$

If $|\psi(q)| > 1$, then

$$\psi(N) = O\left(N^{\frac{1}{\log q}\left(\log\left|\sum_{c=0}^{q-1}\tau_c\right|\right)}\right). \tag{2.2}$$

Proof. Denote, for any $N, Q \in \mathbb{N}$ $(Q > 0)$,

$$\eta(N,Q) := Q\left\lfloor \frac{N}{Q}\right\rfloor.$$

If $Q = q^m$, then the q-ary expansion of $\eta(N,Q)$ can be obtained from the q-ary expansion of N by replacing the last m digits by zeroes.

Suppose that N is a natural integer with q-ary expansion $N = \sum_{i=0}^{l} c_i q^i$. Then,

$$\begin{aligned}\psi(N) &= \sum_{n=0}^{\eta(N,q^l)-1}\tau_n + \sum_{n=\eta(N,q^l)}^{\eta(N,q^{l-1})-1}\tau_n + \ldots + \sum_{n=\eta(N,q)}^{N-1}\tau_n \\ &= \left(\sum_{c=0}^{c_l-1}\tau_c\right)\left(\sum_{c=0}^{q-1}\tau_c\right)^l + \tau_{c_l}\left(\sum_{c=0}^{c_{l-1}-1}\tau_c\right)\left(\sum_{c=0}^{q-1}\tau_c\right)^{l-1} + \ldots + \prod_{k=1}^{l}\tau_{c_k}\cdot\left(\sum_{c=0}^{c_0-1}\tau_c\right) \\ &= \sum_{i=0}^{l}\left(\prod_{k=i+1}^{l}\tau_{c_k}\right)\cdot\psi(c_i)\cdot\psi(q)^i. \end{aligned} \tag{2.3}$$

If $|\psi(q)| \leqslant 1$ then each term of the sum (2.3) is bounded (by the maximum of $|\psi(c)|, c = 1, \ldots, q-1$), therefore $\psi(N) = O(l) = O(\log N)$.

Suppose that $|\psi(q)| > 1$. Then we are going to extend the definition of the function $\psi(x)$ to all real $x \geqslant 0$ using the right-hand side of the formula (2.3). This requires to check that the result does not depend on the choice of the q-ary expansion of the argument.

Take $x = q^{-m}X$ where $m \in \mathbb{Z}, X \in \mathbb{N}$, and the q-ary expansion of X is $X = \sum_{i=0}^{m+l} c_{i-m}q^i$. Then the two q-ary expansions of x are

$$x = \sum_{i=-m}^{l} c_i q^i = \sum_{i=-m+1}^{l} c_i q^i + (c_{-m} - 1)q^{-m} + \sum_{i=-\infty}^{-m-1} (q-1)q^i.$$

We have to prove the identity

$$\begin{aligned}(2.4)\quad \sum_{i=-m}^{l} \left(\prod_{k=i+1}^{l} \tau_{c_k}\right) \cdot \psi(c_i)d(q)^i \;=\; & \\ \sum_{i=-m+1}^{l} \left(\prod_{k=i+1}^{l} \tau_{c_k}\right) \cdot \psi(c_i)d(q)^i + \left(\prod_{k=-m+1}^{l} \tau_{c_k}\right) \cdot \psi(c_{-m}-1)\psi(q)^{-m} & \\ + \psi(q-1)\left(\sum_{i=-\infty}^{-m-1} \left(\prod_{k=i+1}^{l} \tau_{c_k}\right) \cdot \psi(q)^i\right). &\end{aligned}$$

where we denote $c_i = q - 1$ for $i < -m$.

Indeed, some sub-expressions of the right-hand side of (2.4) can be simplified. The last summand can be factored with one factor being

$$\begin{aligned}\psi(q-1)\left(\sum_{i=-\infty}^{-m-1} \left(\prod_{k=i+1}^{-m-1} \tau_{c_k}\right) \cdot \psi(q)^i\right) &= \psi(q-1)\sum_{i=-\infty}^{-m-1} \tau_{q-1}^{-m-i-1}\psi(q)^i \\ &= \psi(q-1)\tau_{q-1}^{-m-1}\left(\frac{\tau_{q-1}}{\psi(q)}\right)^m \frac{1}{\frac{\psi(q)}{\tau_{q-1}} - 1} \\ &= \psi(q-1)\frac{1}{\psi(q)^m(\psi(q) - \tau - q - 1)} \\ &= \psi(q)^{-m}.\end{aligned}$$

Next, the sum of the two last summands in (2.4) is

$$\begin{aligned}\left(\prod_{k=-m+1}^{l} \tau_{c_k}\right) \cdot \psi(c_{-m}-1)\psi(q)^{-m} + \left(\prod_{k=-m}^{l} \tau_{c_k}\right)\psi(q)^{-m} & \\ = \left(\prod_{k>-m} \tau_{c_k}\right)\psi(c_{-m})\psi(q^{-m}). &\end{aligned}$$

These transformations reduce the right-hand side of (2.4) to the form of the left-hand side, proving the identity. Therefore, $\psi(x)$ is a well-defined function of a real argument.

This function is continuous. Indeed, consider a sequence $(x_n)_n$ of positive real numbers which converges to $x > 0$. Suppose that either $x_n > x$ for all n or $x_n < x$ for all n. Let $x = \sum_{i=-\infty}^{l} c_i q^i$ be the q-ary expansion of x which has a property chosen depending on the choice above: if $x_n > x$, the expansion of x does not end by $q-1$'s, if $x_n < x$, it does not end by zeroes. In both cases, for each $m > 0$ there is a rang $\tilde{n}$ such that $n > \tilde{n}$ implies that any q-ary expansion of x_n (denote it by $x_n = \sum_{i=-\infty}^{l} \bar{c}_i q^i$) has all digits before radix point and m digits after radix point identical to those of x. This property implies:

$$|\psi(x) - \psi(x_n)| = \left| \sum_{i=-\infty}^{m-1} \prod_{k>i} \tau_{c_k} \cdot d(c_i) d(b)^i - \sum_{i=-\infty}^{m-1} \prod_{k>i} \tau(\bar{c}_k) \cdot d(\bar{c}_i) d(b)^i \right| \tag{2.5}$$

$$\leqslant 2 \max_{c \in \{0,\dots,b-1\}} \sum_{i<-m} |d(b)|^i \xrightarrow[m\to\infty]{} 0,$$

which proves that the sequence $(\psi(x_n))_n$ converges to $\psi(x)$.

By the definition (2.3), for any $x \geqslant 0$, $\psi(qx) = \psi(q)\psi(x)$. Therefore,

$$\psi(x) = \left(\frac{x}{q^l}\right) \psi(q)^l \text{ where } l = \lfloor \log_q x \rfloor, \text{ therefore}$$

$$|\psi(x)| \leqslant \left(\max_{x \in [1,q]} |\psi(x)| \right) |\psi(q)|^l = O(|\psi(q)|^l) = O(x^{\frac{\log|\psi(q)|}{\log q}}).$$

Lemma is proved. □

Remark that the second part of this Theorem (2.2) has been proved in the article [10] (formula (2.9)).

The previous Lemma leads to the following asymptotic result about the p-rarified sums.

Proposition 2.2. *Consider a strongly b-multiplicative sequence $(t_n)_{n\geqslant 0}$ with values in $\{-1, 0, 1\}$ and a prime number p such that $b < p$ is a generator of the multiplicative group $\mathbb{F}_p^\times$. Suppose that the following inequality holds:*

$$\left| \mathbf{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}} \left(\sum_{c=0}^{b-1} t_c \zeta_p^c \right) \right| > \max \left((\sum_{c=0}^{b-1} t_c)^{p-1}, 1 \right) \tag{2.6}$$

where ζ_p denotes a primitive p-th root of unity and $\mathbf{N}_{L/K}$ denotes the norm. Then we have the following estimation:

$$\sum_{n<N, p \,|\, n} t_n = O\left(N^{\frac{1}{(p-1)\log b} \log\left(\mathbf{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}} (\sum_{c=0}^{b-1} t_c \zeta_p^c) \right)} \right) \tag{2.7}$$

Proof. The norm in (2.7) is real and nonnegative because it is a product of $\frac{p-1}{2}$ complex-conjugate pairs. Furthermore, it is bigger than 1 by the hypothesis (2.6). This proves that the right-hand side of (2.7) has a meaning.

The p-rarefied sum in the left-hand side can be expanded as

$$\sum_{n<N} 1_{p|n} t_n = \sum_{n<N} \frac{1}{p}\left(1+\zeta_p^n+\zeta_p^{2n}+\ldots+\zeta_p^{(p-1)n}\right)t_n = \frac{1}{p}\left(\sum_{n<N} t_n + \sum_{n<N}\sum_{j\in\mathbb{F}_p^\times} \zeta_p^{jn} t_n\right). \tag{2.8}$$

Remark that the sequences $(t_n)_{n\geqslant 0}$ and $(\zeta_p^{jn}t_n)_{n\geqslant 0}$ ($j\in\{1,\ldots,p-1\}$), which appear in the previous formula, are strongly b^{p-1}-multiplicative.

By Lemma 2.1 applied to the sequence $(t_n)_{n\geqslant 0}$, one has one of the two estimations

$$\sum_{n<N} t_n = O\left(N^{\frac{1}{\log b}\log\left|\sum_{c=0}^{b-1} t_c\right|}\right) \text{ or}$$
$$\sum_{n<N} t_n = O(\log N).$$

In both cases we get (using the hypothesis (2.6)),

$$\sum_{n<N} t_n = O\left(N^{\frac{1}{(p-1)\log b}\log\left(\mathbf{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\sum_{j=0}^{b-1} t_j\zeta_p^j\right)\right)}\right). \tag{2.9}$$

Lemma 2.1 applied to a sequence of the form $(\zeta_p^{jn}t_n)_{n\geqslant 0}$ states that

$$\sum_{n<N} \zeta_p^{jn} t_n = O\left(N^{\frac{1}{(p-1)\log b}\log\left|\sum_{c=0}^{b^{p-1}-1}\zeta_p^{jc}t_c\right|}\right) \text{ or} \tag{2.10}$$

$$\sum_{n<N} \zeta_p^{jn} t_n = O(\log N). \tag{2.11}$$

On the other hand, one can expand the norm of $(\sum_{c=0}^{b-1} t_c\zeta_p^c)$ as

$$\mathbf{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\sum_{c=0}^{b-1} t_c\zeta_p^c\right) = \prod_{i=0}^{p-2}\left(\sum_{c=0}^{b-1}\zeta_p^{b^i cj}t_c\right) = \sum_{c_0,\ldots,c_{p-2}\in\{0,\ldots,b-1\}} \zeta_p^{j(c_0+bc_1+\cdots+b^{p-2}c_{p-2})} t_{c_0}\ldots t_{c_{p-2}} \tag{2.12}$$

where the sequences $(c_0,\ldots,c_{p-2})$ are nothing else than all possible choices of the index c when the product is expanded. The change of variable $n :=$

$c_0 + bc_1 + \cdots + b^{p-2}c_{p-2}$ leads to a new variable which goes through all integers from 0 to $b^{p-1} - 1$. Therefore,

$$\mathbf{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\Big(\sum_{c=0}^{b-1} t_c\zeta_p^c\Big) = \sum_{n=0}^{b^{p-1}-1} \zeta_p^n t_n, \tag{2.13}$$

which is the sum involved in (2.10).

Therefore,

$$\sum_{n<N} \zeta_p^{jn} t_n = O\left(N^{\frac{1}{(p-1)\log b}\log\left(\mathbf{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\sum_{c=0}^{b-1} t_c\zeta_p^c\right)\right)}\right). \tag{2.14}$$

Equations (2.8), (2.9) and (2.14) lead to the conclusion of the Proposition. □

Proposition 2.2 generalizes the first part of Proposition 1.2 (the estimation (1.1)) as the Thue-Morse sequence satisfies the conditions of validity of Propoition 2.2 and we get the following:

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

Another situation where the norms

$$\mathbf{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\sum_{j=0}^{b-1} t_j\zeta_p^j\right) \tag{2.15}$$

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

$$\mathbf{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1 + \zeta_p - \zeta_p^2) = L_p \tag{2.16}$$

the p-th term of the Lucas sequence (referred as $A000032$ by OEIS, cf [16]) defined recursively by $L_0{=}2, L_1{=}1, L_{n+2} = L_n{+}L_{n+1}$. This result is proved in a different way in Section 5.2.

3. Combinatorics of partitions of a set.

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

$$\prod_{j=1}^{j=p-1} \Big(X - \zeta^j\Big) = 1 + X + \cdots + X^{p-1}, \tag{3.1}$$

and the methods of this proof will be re-used in the proof of the functional equation in Section 4. 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 [17]). We are going to prove the following statement, which is equivalent to (3.1).

Lemma 3.1. *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 $A_2(n,p)$, $A_3(n,p)$, ..., $A_{p-1}(n,p)$, 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 3.2. Denote by $E_x^{k_1,\ldots,k_n}(n,p)$ (where $x \in \mathbb{F}_p$ and $k_1,\ldots,k_n \in \mathbb{F}_p^\times$) 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 3.3. *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 3.1 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 $n = 4$:

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

which is 4!, therefore Lemma 3.1 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 3.1 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 [12]. 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 $B_1 \cup B_2 \cup \cdots \cup B_c = \{1, 2, \ldots, n\}$. 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:

$$\begin{cases} \mu(\hat{0}, x) = 1 & \text{if } x = \{\{1\}, \{2\}, \ldots, \{n\}\} = \hat{0}; \\ \mu(\hat{0}, x) = -\sum\limits_{\substack{y \in \Pi_n \\ y < x}} \mu(\hat{0}, y) & \text{if } x \text{ is bigger than } \hat{0}. \end{cases}$$

By the Corollary to the Proposition 3 section 7 of [15] and the first Theorem from the section 5.2.1 of [12], if x is a partition of type $(\lambda_1, \ldots, \lambda_n)$, then

$$\mu(\hat{0}, x) = \prod_{i=1}^{n} (-1)^{\lambda_i - 1} (\lambda_i - 1)! \tag{3.2}$$

This formula will be useful in Section 4.

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 3.4. *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 partition $x \in \Pi_n$, 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 partition y of $\{1, 2, \ldots, n\}$,

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

Then, by Proposition 3.3,

$$s(y, p) = (-1)^{c(y)} \tag{3.3}$$

where $c(y)$ is the number of blocks in the partition y. By the Möbius inversion formula (see [12]),

$$r(\hat{0}, p) = \sum_{y \in \Pi_n} \mu(\hat{0}, y) s(y, p) = \sum_{y \in \Pi_n} (-1)^{c(y)} \mu(\hat{0}, y). \tag{3.4}$$

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

$$\sum_{y \in \Pi_n} (-1)^{c(y)} \mu(\hat{0}, y) = (-1)^n n! \tag{3.5}$$

in a way that uses the equivalence with Lemma 3.1. This proof may seem to be artificial because it is no longer used in the Section 4, and a purely combinatorial and more general proof exists: see the final formula of Chapter 3.10.4 of [17].

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 3.1 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 3.4 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 3.1 for n to Lemma 3.1 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 3.5. *Let*

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

and

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

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

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

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

The function $R(n)$ satisfies the estimation

$$R(n) = O(\log \log n). \tag{3.6}$$

Proof. Denote $\theta = 0.525$. By Theorem 1 of [3], 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,

$$n \geqslant \bar{p} - \bar{p}^\theta. \tag{3.7}$$

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 (3.7), $\bar{p} \leqslant u^{-1}(n)$, therefore

$$\forall n > N_1 \ f(n) = \bar{p} - n \leqslant \bar{p}^\theta \leqslant (u^{-1}(n))^\theta < n^{\bar{\theta}} \tag{3.8}$$

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 [13]. 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. □

4. Pascal's equation.

We are going to prove the functional equation satisfied by the coefficients of the polynomial $\mathcal{N}_{p,i_1,i_2}(Y_0, Y_1, Y_2)$ (introduced in (1.6)). To do this, we are going to describe a combinatorial interpretation of these numbers.

Definition 4.1. 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

$$C_i^{i_1,i_2}(n_1,n_2,p) = \#\left\{ (x_1, \ldots, x_{n_1+n_2}) \in \mathbb{F}_p^{\times n_1+n_2} \;\middle|\; \begin{array}{c} x_k \neq x_l \text{ if } k \neq l, \\ i_1 \sum_{k=1}^{n_1} x_k + i_2 \sum_{k=n_1+1}^{n_1+n_2} x_k = i \end{array} \right\} \tag{4.1}$$

and

$$A_i^{i_1,i_2}(n_1,n_2,p) = \#\left\{(X_1,X_2)\in\mathcal{P}(\mathbb{F}_p^\times)^2 \,\middle|\, \begin{array}{c}|X_1|=n_1,|X_2|=n_2,\\ X_1\cap X_2=\emptyset,\\ i_1\sum X_1+i_2\sum X_2=i\end{array}\right\}. \tag{4.2}$$

Definition 4.1 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). One can also see that the answer to Problem 1.3 is $(p-1-n_1-n_2)!C_i^{i_1,i_2}(n_1,n_2,p)$ where n_1 (resp., n_2) is the number of coordinates of the vector $\mathbf{f}$ equal to i_1 (resp., i_2).

From this definition one can see that

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

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 (4.1) and (4.2). Proposition 4.2 below suggests to research the value of

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

We can express the symmetric polynomials of the quantities $(Y_0+\zeta_p^{i_1j}Y_1+\zeta_p^{i_2j}Y_2)$ in terms of the previously defined numbers via the following.

Proposition 4.2. *Let i_1,i_2 be two different elements of $\mathbb{F}_p^\times$ and denote by $\sigma_{v,(j=1,\dots,p-1)}$ 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:*

$$\sigma_{p-1-\delta,(j=1,\dots,p-1)}\left(Y_0+\zeta_p^{i_1j}Y_1+\zeta_p^{i_2j}Y_2\right) = \sum_{\substack{0\leqslant n_0,n_1,n_2\leqslant p-1\\ n_0+n_1+n_2=p-1\\ n_0\geqslant\delta}} \binom{n_0}{\delta}\triangle^{i_1,i_2}(n_1,n_2,p)Y_0^{n_0-\delta}Y_1^{n_1}Y_2^{n_2}. \tag{4.3}$$

In particular,

$$\mathcal{N}_{p,i_1,i_2}(Y_0,Y_1,Y_2) = \sum_{\substack{0\leqslant n_0,n_1,n_2\leqslant p-1\\ n_0+n_1+n_2=p-1}} \triangle^{i_1,i_2}(n_1,n_2,p)Y_0^{n_0}Y_1^{n_1}Y_2^{n_2}. \tag{4.4}$$

Proof. The symmetric polynomial develops as:

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

When we group the terms of this sum by sizes $n_0=|X_0'|, n_1=|X_1|, n_2=|X_2|$ we obtain (4.3). □

The method of proof of Lemma 3.4 can be generalized into the following conditional closed formula for the coefficients $\triangle^{i_1,i_2}(n_1,n_2,p)$:

Proposition 4.3. *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 $n_1+n_2<p$. Suppose that 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. Then,*

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

Proof. Define

$$f_k=\begin{cases} i_1 & \text{if } k\in\{1,\dots,n_1\}\\ i_2 & \text{if } k\in\{n_1+1,\dots,n_1+n_2\}\end{cases} \tag{4.6}$$

and $n:=n_1+n_2$.

Next, for each partition $x\in\Pi_n$ and each $i\in\mathbb{F}_p$ denote by $r_i^{i_1,i_2}(x,n_1,n_2,p)$ the number of sequences $(x_1,x_2,\dots,x_{n=n_1+n_2})$ of elements of $\mathbb{F}_p^\times$ of coimage x such that

$$i_1\sum_{k=1}^{n_1}x_k+i_2\sum_{k=n_1+1}^{n_1+n_2}x_k=i. \tag{4.7}$$

Let us also define $r^{i_1,i_2}(x,n_1,n_2,p) = r_0^{i_1,i_2}(x,n_1,n_2,p) - r_1^{i_1,i_2}(x,n_1,n_2,p)$ and

$$s_i^{i_1,i_2}(x,n_1,n_2,p) = \sum_{x' \geqslant x} r_i^{i_1,i_2}(x',n_1,n_2,p), \tag{4.8}$$

$$s^{i_1,i_2}(x,n_1,n_2,p) = s_0^{i_1,i_2}(x,n_1,n_2,p) - s_1^{i_1,i_2}(x,n_1,n_2,p). \tag{4.9}$$

By definition,

$$C_0^{i_1,i_2}(n_1,n_2,p) - C_1^{i_1,i_2}(n_1,n_2,p) = r^{i_1,i_2}(\hat{0},n_1,n_2,p). \tag{4.10}$$

Consider a partition $x \in \Pi_n$. The number $s_i^{i_1,i_2}(x,n_1,n_2,p)$ (defined by the formula (4.8)) admits an equivalent definition as the number of sequences $(x_1,x_2,\ldots,x_n)$ of elements of $\mathbb{F}_p^\times$ of coimage greater than or equal to x (in the sense of partitions) which satisfy (4.7). Denote by $B_1,\ldots,B_{c(x)}$ the blocks of x and

$$f_{B_j} = \sum_{k \in B_j} f_k (j = 1,\ldots,c(x)).$$

Then, $s_i^{i_1,i_2}(x,n_1,n_2,p)$ is the number of sequences $(x_{B_1},\ldots,x_{B_{c(x)}})$ of elements of $\mathbb{F}_p^\times$ (where the terms can be equal or distinct) such that

$$\sum_{j=1}^{c(x)} f_{B_j} x_{B_j} = i. \tag{4.11}$$

By the hypotheses of the Proposition, all f_{B_j} are nonzero in $\mathbb{F}_p$. Therefore, by Proposition 3.3,

$$s^{i_1,i_2}(x,n_1,n_2,p) = (-1)^{c(x)}. \tag{4.12}$$

By the Möbius inversion formula and the formula (3.5),

$$r(\hat{0},,n_1,n_2,p) = \sum_{y \in \Pi_n} (-1)^{c(y)} \mu(\hat{0},y) = (-1)^n n!.$$

Therefore,

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

which concludes the proof. □

The condition of Proposition 4.3 holds, for example, if the smallest positive representatives of i_1 and i_2 verify $n_1 i_1 + n_2 i_2 < p$.

Without the condition formulated in Proposition 4.3, (4.5) 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 4.4 ("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,*

$$\begin{aligned}(4.13)\quad C_0^{i_1,i_2}(n_1,n_2,p) - C_1^{i_1,i_2}(n_1,n_2,p) \equiv \\ n_1 C_1^{i_1,i_2}(n_1-1,n_2,p) + n_2 C_1^{i_1,i_2}(n_1,n_2-1,p) \\ - n_1 C_0^{i_1,i_2}(n_1-1,n_2,p) - n_2 C_0^{i_1,i_2}(n_1,n_2-1,p) \bmod p\end{aligned}$$

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

$$\begin{aligned}(4.14)\quad C_0^{i_1,i_2}(n_1,n_2,p) - C_1^{i_1,i_2}(n_1,n_2,p) = \\ n_1 C_1^{i_1,i_2}(n_1-1,n_2,p) + n_2 C_1^{i_1,i_2}(n_1,n_2-1,p) \\ - n_1 C_0^{i_1,i_2}(n_1-1,n_2,p) - n_2 C_0^{i_1,i_2}(n_1,n_2-1,p)\end{aligned}$$

holds.

Proof. We are going to use the notations of the beginning of the previous proof until the formula (4.11). We are also going to call a *hindrance* a subset X of $\{1, \dots, n_1 + n_2\}$ such that $\sum_{m \in X} f_m \equiv 0 \bmod p$. Proposition 4.3 corresponds to the case when there are no hindrances. Then

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

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

In general, the formula (4.12) should be replaced by:

$$(4.15)\qquad s^{i_1,i_2}(y,n_1,n_2,p) = (1-p)^{d(y)}(-1)^{c(y)}$$

if the partition y of $\{1, \dots, n_1 + n_2\}$ contains $d(y)$ blocks that are hindrances. We should, indeed, count the solutions of the congruences (4.11) for $i = 0, 1$ (in nonzero residues modulo p) and evaluate the difference. Proposition 3.3 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 (4.15).

The formula (4.15) can be rewritten as

$$s^{i_1,i_2}(y,n_1,n_2,p) = \sum_{l=0}^{d(y)} \sum_{\substack{X_1,X_2,\dots,X_l \\ \text{hindrances} \\ \text{contained in } y}} (-1)^{c(y)-l} p^l$$

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

$$C_0^{i_1,i_2}(n_1,n_2,p) - C_1^{i_1,i_2}(n_1,n_2,p) = \sum_{y\in\Pi_n} \mu(\hat{0},y) s^{i_1,i_2}(y,n_1,n_2,p) \tag{4.16}$$

$$= \sum_{\substack{X_1,X_2,\ldots,X_l \\ \text{disjoint hindrances}}} \sum_{\substack{y\in\Pi_n \\ y \text{ contains } X_1,\ldots,X_l \\ \text{as blocks}}} (-1)^{c(y)-l} \mu(\hat{0},y) p^l \tag{4.17}$$

$$\begin{aligned} = \sum_{X_1,\ldots,X_l} & (-1)^{|X_1|+|X_2|+\cdots+|X_l|-l} (|X_1|-1)! \\ & \times (|X_2|-1)! \ldots (|X_l|-1)! p^l \\ & \times \sum_{\substack{y\in\Pi_n \\ y \text{ contains } X_1,\ldots,X_l}} \mu(\hat{0}, y - X_1 - X_2 - \ldots - X_l) (-1)^{c(y-X_1-X_2-\cdots-X_l)} \end{aligned} \tag{4.18}$$

by factoring $\mu(\hat{0},y)$ according to the formula (3.2). In the last sum, $(y - X_1 - X_2 - \cdots - X_l)$ denotes the partition y, where the blocks $X_1, \ldots, X_l$ are removed (which is a partition of $(n_1+n_2-|X_1|-\cdots-|X_l|)$ elements). By applying (3.5) to the last sum of (4.18), we get

$$\begin{aligned} C_0^{i_1,i_2}(n_1,n_2,p) - C_1^{i_1,i_2}(n_1,n_2,p) = & \\ \sum_{X_1,\ldots,X_l} & (|X_1|-1)!(|X_2|-1)! \ldots (|X_l|-1)! (-1)^{n_1+n_2-l} \\ & p^l (n_1+n_2-|X_1|-\ldots-|X_l|)!. \end{aligned} \tag{4.19}$$

From (4.19),

$$C_0^{i_1,i_2}(n_1,n_2,p) - C_1^{i_1,i_2}(n_1,n_2,p) \equiv (-1)^{n_1+n_2}(n_1+n_2)! \bmod p, \tag{4.20}$$

which implies (4.13).

Suppose that $\{1, \ldots, n_1+n_2\}$ is not a hindrance. In order to prove (4.14), remark that the sum (4.19) can be split as

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

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 (4.19) with one of the arguments n_1 or n_2 decreased by 1, we get (4.14). □

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

Theorem 4.5 ("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,*

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

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

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

holds.

Proof. Division of both sides of (4.13) by $n_1!n_2!$ (which is not multiple of p) gives (4.21) and division by the same number of (4.14) gives (4.22). □

Theorem 1.4 follows directly from Proposition 4.2 and Theorem 4.5.

5. Some properties of finite Pascal's triangles.

5.1. 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 (4.22) is valid for any $n_1, n_2 \in \mathbb{N}^2$ such that $p \nmid n_1i_1+n_2i_2$. 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 (4.22) via Lemma 3.1. 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 (4.22) is valid, therefore, when $n_1+n_2 = p$.

We can now prove that the functional relation (4.22), 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 5.1. *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*

$$d(0,0) = 1, \tag{5.1}$$

$$d(n_1,n_2) = 0 \quad \textit{if} \quad n_1 = -1 \quad \textit{or} \quad n_2 = -1 \quad \textit{or} \quad n_1+n_2 \geqslant p, \tag{5.2}$$

$$d(n_1,n_2) + d(n_1-1,n_2) + d(n_1,n_2-1) = 0 \ \textit{if}\ p \nmid n_1 i_1 + n_2 i_2. \tag{5.3}$$

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 (5.2), (5.3) and $\delta(0,0) = 0$. In order to prove the theorem we should prove that $\delta = 0$.

By applying (5.3) successively to $n_2 = 0$ and $n_1 = 1,\dots,p-1$ one proves that $\delta(0,0) = -\delta(1,0) = \delta(2,0) = \cdots = \delta(p-1,0)$. By applying it to $n_1 = 0$ and $n_2 = 1,\dots,p-1$ one proves that $\delta(0,0) = -\delta(0,1) = \cdots = \delta(0,p-1)$.

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 (5.2).

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 (5.3) 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

$$\delta(n_1 - 1, p - \tilde{n} - n_1) + \delta(n_1, p - \tilde{n} - n_1 - 1) = 0. \tag{5.4}$$

By applying (5.4) successively to $n_1 = 1,\dots,n_1^S - 1$, we prove $\delta(n_1, p - \tilde{n} - n_1 - 1) = 0$ for n_1 in the same range $1,\dots,n_1^S - 1$. If $n_1^S \geqslant p - \tilde{n} - 1$, this concludes the step of induction. Otherwise, by applying (5.4) successively to $n_1 = p - \tilde{n} - 1,\dots,n_1^S + 1$ (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 $p - \tilde{n},\dots,n_1^S$.

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

$$f^{i_1,i_2}(n_1,n_2,p) = \triangle^{i_1,i_2}(n_1,n_2,p) + \triangle^{i_1,i_2}(n_1-1,n_2,p) + \triangle^{i_1,i_2}(n_1,n_2-1,p). \tag{5.5}$$

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 (4.19) combined with the end of the proof of Theorem 4.4:

$$n_1!n_2!f^{i_1,i_2}(n_1,n_2,p) = \sum_{\substack{X_1,X_2,\dots,X_l \\ \text{partition of } \{1,\dots,n_1+n_2\}, \\ \forall j\ p \mid \sum_{m\in X_j} f_m}} (|X_1|-1)!(|X_2|-1)!\dots(|X_l|-1)! \\ (-1)^{n_1+n_2-l}p^l(n_1+n_2-|X_1|-\dots-|X_l|)!\,. \tag{5.6}$$

This formula uses the notation (4.6) in order to describe the fact that summation goes through all partitions of $\{1,\dots,n_1+n_2\}$ into hindrances.

The definition (5.5) implies, by linearity of the Pascal's equation:

$$\triangle^{i_1,i_2}(n_1,n_2,p) = \sum_{\substack{0\leqslant k\leqslant n_1 \\ 0\leqslant l\leqslant n_2 \\ p\,|\,i_1k+i_2l}} f^{i_1,i_2}(k,l,p)(-1)^{n_1+n_2-k-l}\binom{n_1+n_2-k-l}{n_1-k}. \tag{5.7}$$

5.2. 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

$$\triangle^{1,2}(n_1,n_2,p) = \triangle^{1,2}(n_1,p-1-n_1-n_2,p). \tag{5.8}$$

It follows indeed from the fact that for each disjoint couple $X_1, X_2 \subset \mathbb{F}_p^\times$, as in the definition (4.2),

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

Formula (4.5) applies to at least one side of (5.8) for each (n_1,n_2) (and to both sides of (5.8) if $n_1+2n_2 = p-1$), leading to

$$\triangle^{1,2}(n_1,n_2,p) = \begin{cases} (-1)^{n_1+n_2}\binom{n_1+n_2}{n_1} & \text{if } n_1+2n_2 \leqslant p-1 \\ (-1)^{n_2}\binom{p-1-n_2}{n_1} & \text{if } n_1+2n_2 \geqslant p-1. \end{cases} \tag{5.9}$$

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

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

One can deduce (2.16) from (5.9) in the following way: by (4.4),

$$
\begin{aligned}
(5.10)\quad \prod_{j=1}^{j=p-1}\left(1+\zeta_p-\zeta_p^2\right) &= \sum_{n_1,n_2\in\mathbb{N}}(-1)^{n_2}\triangle^{1,2}(n_1,n_2,p)\\
&= \sum_{n_1,n_2\in\mathbb{N}}(-1)^{n_2-1}(\triangle^{1,2}(n_1-1,n_2,p)+\triangle^{1,2}(n_1,n_2-1,p)\\
&\qquad -f^{1,2}(n_1,n_2,p))\\
&= \sum_{n_1,n_2\in\mathbb{N}}((-1)^{n_2-1}\triangle^{1,2}(n_1,n_2-1,p)-(-1)^{n_2}\triangle^{1,2}(n_1-1,n_2,p)\\
&\qquad +(-1)^{n_2}f^{1,2}(n_1,n_2,p))\\
&= \sum_{n_1,n_2\in\mathbb{N}}(-1)^{n_2}f^{1,2}(n_1,n_2,p)
\end{aligned}
$$

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

$$
\begin{aligned}
(5.11)\quad f^{1,2}(n_1,n_2,p) &= \triangle^{1,2}(n_1-1,n_2,p)+\triangle^{1,2}(n_1,n_2-1,p)+\triangle^{1,2}(n_1,n_2,p)\\
&= (-1)^{n_2}\binom{n_1+n_2-1}{n_1-1}+2(-1)^{n_2}\binom{n_1+n_2-1}{n_1}\\
&= (-1)^{n_2}\left(\binom{n_1+n_2}{n_1}+\binom{n_1+n_2-1}{n_1}\right)\\
&= (-1)^{n_2}\left(\binom{p-n_2}{n_2}+\binom{p-n_2-1}{n_2-1}\right).
\end{aligned}
$$

The absolute value of (5.11) 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 [4]), for any $k \leqslant \frac{p-1}{2}$

$$\begin{aligned}(5.12)\quad &\#\{k \text{ disjoint dominoes on a circle of length } p\}\\ &= \#\{k \text{ disjoint dominoes on a line segment of length } p\}\\ &\quad + \#\{k-1 \text{ disjoint dominoes on a line segment of length } p-2\}\\ &= \binom{p-k}{k} + \binom{p-k-1}{k-1}.\end{aligned}$$

The sum (5.10) contains three terms not covered by the hypotheses of (5.11): 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 (5.10) 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 [4] to be L_p.

For example, if $p = 11$, the numbers are those of Figure 5.1 (⧫ denotes a source).

5.3. Application: an identity for binomial coefficients. The formulas (4.4) and (5.10) 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 (5.10):

$$\begin{aligned}(5.13)\qquad 1 = \prod_{j=1}^{j=p-1}\left(1-\zeta_p+\zeta_p^2\right) &= \sum_{n_1,n_2\in\mathbb{N}} (-1)^{n_1}\triangle^{1,2}(n_1,n_2,p)\\ &= \sum_{n_1,n_2\in\mathbb{N}} (-1)^{n_1} f^{1,2}(n_1,n_2,p).\end{aligned}$$

We further get:

$$(5.14)\quad 1 = 1+\sum_{n_1,n_2\in\mathbb{N}^*} (-1)^{n_1} f^{1,2}(n_1,n_2,p) = 1-\sum_{n_1,n_2\in\mathbb{N}^*} f^{1,2}(n_1,n_2,p).$$

The formula (5.11) leads to the following combinatorial identity[1]:

$$(5.15)\qquad \sum_{k=1}^{\frac{p-1}{2}}(-1)^k\left(\binom{p-k}{k}+\binom{p-k-1}{k-1}\right) = 0.$$

[1]The previous proof implies (5.15) in the case of prime $p\geqslant 5$. The Zeilberger's algorithm (implemented in Maple 17, see also Chapter 6 of the book [14]) generalizes it for any $p\geqslant 5$ congruent to 1 or 5 modulo 6

5.4. 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 5.2. *Let $p \geqslant 5$ be prime and $\delta \in \{0,\dots,p-2\}$ an integer. Then $\sigma_{p-1-\delta,(j=1,\dots,p-1)}(1+\zeta_p^j-\zeta_p^{2j})$ (see the notation of Proposition 4.2) 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 $\sigma_{p-1-\delta}(1+\zeta-\zeta^2) \equiv \binom{p-1}{\delta} \bmod p$.

Proof. By Proposition 4.2, we get a similar expression to (5.10)

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

The identity (5.11) leads to

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

and the discussion that follows the formula (5.11) 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 5.2. Coefficients of $\prod_{j=1}^{10}\left(X+\zeta_{11}^{j}Y+\zeta_{11}^{3j}Z\right)$

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

$$\triangle^{1,3}(n_1,n_2,p)=\triangle^{2,3}(n_1,p-1-n_1-n_2,p) \tag{5.18}$$

is analogous to (5.8) and implies

$$\triangle^{1,3}(n_1,n_2,p)=\begin{cases}(-1)^{n_1+n_2}\binom{n_1+n_2}{n_1} & \text{if } n_1+3n_2\leqslant p-1\\ (-1)^{n_2}\binom{p-1-n_2}{n_1} & \text{if } n_1+3n_2\geqslant 2p-2 \text{ or}\\ & \quad n_1+3n_2=2p-4,\end{cases} \tag{5.19}$$

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 (5.7). 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

$$\#\left\{\begin{array}{c}0<n_1<p\\ 0<n_2<p\\ n_1+3n_2=p\end{array}\right\}=\left\lfloor\frac{p}{3}\right\rfloor \tag{5.20}$$

and the number of integer points on the lower line is

$$\#\left\{\begin{array}{c}0<n_1<p\\ 0<n_2<p\\ n_1+3n_2=2p\end{array}\right\}=\mathrm{rnd}(\frac{p}{6}), \tag{5.21}$$

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 (5.6):

$$f^{1,3}(n_1, n_2, p) = \frac{(n_1 + n_2 - 1)!p}{n_1!n_2!} \tag{5.22}$$

because the sum consists of the single term associated to $X=\{1, \dots, n_1+n_2\}$. Under the same hypotheses, (5.7) implies

$$\triangle^{1,3}(n_1, n_2, p) = \frac{(n_1 + n_2 - 1)!p}{n_1!n_2!} - \binom{n_1 + n_2}{n_1} = 2\binom{n_1+n_2-1}{n_1}. \tag{5.23}$$

In any point (n_1, n_2) such that $p \leqslant n_1 + 3n_2 < 2p$, the formula (5.7) takes the following form:

$$\begin{aligned}\triangle^{1,3}(n_1, n_2, p) &= (-1)^{n_1+n_2}\binom{n_1 + n_2}{n_1} \\ &\quad + \sum_{\substack{0<k\leqslant n_1 \\ 0<l\leqslant n_2 \\ p=i_1k+i_2l}} f^{1,3}(k, l, p)(-1)^{n_1+n_2-k-l}\binom{n_1+n_2-k-l}{n_1 - k}.\end{aligned} \tag{5.24}$$

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 (5.5) and (5.18),

(5.25)

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

By (5.6) (the sum, once again, consists of a single term because $2n_1 + 3(p-n_1-n_2) = p$),

$$f^{2,3}(n_1, p - n_1 - n_2, p) = \frac{(-1)^{n_2}(p - n_2 - 1)!p}{n_1!(p - n_1 - n_2)!}. \tag{5.26}$$

For example, if $p = 11$, the numbers are those of Figure 5.2 (⧫ denotes a source).

References

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

[2] G. Alkauskas, "Dirichlet series associated with strongly *q*-multiplicative functions", *Ramanujan J.* **8** (2004), no. 1, p. 13-21.

[3] R. C. Baker, G. Harman & J. Pintz, "The difference between consecutive primes. II", *Proc. London Math. Soc. (3)* **83** (2001), no. 3, p. 532-562.

[4] A. T. Benjamin & J. J. Quinn, "The Fibonacci numbers—exposed more discretely", *Math. Mag.* **76** (2003), no. 3, p. 182-192.

[5] F. M. Dekking, "On the distribution of digits in arithmetic sequences", in *Seminar on number theory, 1982–1983 (Talence, 1982/1983)*, Univ. Bordeaux I, Talence, 1983, p. Exp. No. 32, 12.
[6] M. Drmota & J. F. Morgenbesser, "Generalized Thue-Morse sequences of squares", *Israel J. Math.* **190** (2012), p. 157-193.
[7] M. Drmota & M. Skałba, "Rarified sums of the Thue-Morse sequence", *Trans. Amer. Math. Soc.* **352** (2000), no. 2, p. 609-642.
[8] A. O. Gel′fond, "Sur les nombres qui ont des propriétés additives et multiplicatives données", *Acta Arith.* **13** (1967/1968), p. 259-265.
[9] S. Goldstein, K. A. Kelly & E. R. Speer, "The fractal structure of rarefied sums of the Thue-Morse sequence", *J. Number Theory* **42** (1992), no. 1, p. 1-19.
[10] P. J. Grabner, "Completely q-multiplicative functions: the Mellin transform approach", *Acta Arith.* **65** (1993), no. 1, p. 85-96.
[11] R. Hofer, "Coquet-type formulas for the rarefied weighted Thue-Morse sequence", *Discrete Math.* **311** (2011), no. 16, p. 1724-1734.
[12] J. P. S. Kung, G.-C. Rota & C. H. Yan, *Combinatorics: the Rota way*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 2009, xii+396 pages.
[13] F. Luca & R. Thangadurai, "On an arithmetic function considered by Pillai", *J. Théor. Nombres Bordeaux* **21** (2009), no. 3, p. 693-699.
[14] M. Petkovšek, H. S. Wilf & D. Zeilberger, $A = B$, A K Peters, Ltd., Wellesley, MA, 1996, With a foreword by Donald E. Knuth, With a separately available computer disk, xii+212 pages.
[15] G.-C. Rota, "On the foundations of combinatorial theory. I. Theory of Möbius functions", *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete* **2** (1964), p. 340-368 (1964).
[16] J. A. Sloane, "On-Line Encyclopedia of Integer Sequences", `http://oeis.org`.
[17] R. P. Stanley, *Enumerative combinatorics. Vol. 1*, Cambridge Studies in Advanced Mathematics, vol. 49, Cambridge University Press, Cambridge, 1997, With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original, xii+325 pages.
[18] B. M. Trager, "Algebraic factoring and rational function integration.", Symbolic and algebraic computation, Proc. 1976 ACM Symp., Yorktown Heights/N.Y., 219-226 (1976)., 1976.

Alexandre Aksenov
Institut Fourier, UMR 5582
100, rue des Maths, BP 74
38402 St Martin d'Hères Cedex
FRANCE
E-mail: `alexander1aksenov@gmail.com`