Sign-reductions, p-adic valuations, binomial coefficients modulo p^k and triangular symmetries

Mihai Prunescu *

Abstract

According to a classical result of E. Kummer, the p-adic valuation v_p applied to a binomial coefficient $\binom{a+b}{a}$ yields the number of carries occurring while adding a and b in basis p. We show that for all $m \in \mathbb{N}$ the numbers $v_p(\binom{a}{b})$ build a pattern with triangular symmetry for $0 \leq b \leq a \leq p^m - 1$. This fact will be compared with the triangular symmetry of the patterns $u_p(\binom{a}{b} \mod p)$ for $0 \leq b \leq a \leq p^m - 1$, where u_p is the sign-reduction: $u_p(x) = x$ if $0 \leq x \leq p/2$ and $u(x) = p - x$ if $p/2 < x < p$. It is shown that $n = 4$ is the only one composite number such that $u_n(\binom{a}{b} \mod n)$ has triangular symmetry. In this special case the two patterns coincide. It is also shown that the last non-zero digits of the binomial coefficients written in basis p build a pattern with triangular symmetry. A combined pattern unifies all proven features.

Key Words: binomial coefficient, p-adic valuation, triangular symmetry, Kummer's theorem about carries, Pascal's Triangle modulo p^k, automatic 2-dimensional sequence, Zaphod Beeblebrox.

A.M.S.-Classification: 11A07, 05E11, 28A80, 68Q45.

1 Introduction

Let p be a prime. According to a classical result of Ernst Kummer, if $p^c \mid \binom{a+b}{a}$ but $p^{c+1} \nmid \binom{a+b}{a}$, then the number of carries that occur during the digital addition of a with b in basis p is c. If $k \in \mathbb{Z}$ and $p^c \mid k$ but $p^{c+1} \nmid k$, one says that $v_p(k) = c$. The function v_p is called p-adic valuation. One takes by convention $v_p(0) = \infty$. Three general properties of the general notion of valuation will be used here. A valuation is a homomorphism, i. e. $v_p(ab) = v_p(a) + v_p(b)$, satisfying triangle's inequality for ultra-metrics, i.e. $v_p(a + b) \geq \min(v_p(a), v_p(b))$. Moreover, if $v_p(a) \neq v_p(b)$, then $v_p(a + b) = \min(v_p(a), v_p(b))$.

A direct consequence of Kummer's Theorem about carries is the following:

Corollary 1.1 *If $0 \leq v \leq u \leq p^m - 1$, then $0 \leq v_p(\binom{u}{v}) \leq m - 1$. Both bounds are taken as values over the given set.*

Kummer's Theorem can be seen as a result concerning the complexity of addition. It corresponds to the usual human experience that an instance of addition, that needs more carries produces the sensation of being more difficult. If the values $v_p(\binom{s}{a})$ are written down in a triangular lattice, in the same way as $\binom{s}{a}$, this lattice can be seen as a map of the difficulty to add numbers written in basis p. The numbers on row s express the difficulty to get the sum s from summands a and $s - a$.

The first goal of this note is to show that for all $m \in \mathbb{N}$, the first p^m rows of Pascal's Triangle, which are numbered from 0 to $p^m - 1$, build a pattern with triangular symmetry. This fact implies

*Brain Products, Freiburg, Germany and Simion Stoilow Institute of Mathematics of the Romanian Academy, Research unit 5, P. O. Box 1-764, RO-014700 Bucharest, Romania. mihai.prunescu@math.uni-freiburg.de.

that every Pascal's Triangle modulo p^k is the union of an ascendant chains of symmetric triangular blocks of edge p^m, where $m \in \mathbb{N}$. This is done in Section 3.

In Section 4 this symmetry is compared with another symmetry occurring when the binomial coefficients are projected onto a finite set in connection with a prime number. To reach the second symmetry, the binomial coefficients modulo p are projected onto the set $\{0, \ldots, (p-1)/2\}$ by a function u_p, defined such that $u_p(x) = x$ if $0 \leq x \leq (p-1)/2$ and $u(x) = p-x$ if $(p-1)/2 < x < p$. We call the function u_p sign-reduction and we observe that it is a kind of absolute value. From a philosophical point of view absolute values and valuations are related. Unhappily, for the moment we cannot give more deep evidence of a relation between the two symmetries.

In [9] the author described the square dihedral symmetry of the sequences $a(i,j) \mod p$ for $a(i,j) = (a(i,j-1) + ma(i-1,j-1) + a(i-1,j)) \mod p$ with constant initial conditions and $m \neq 0$. This symmetry was also bazed on sign-reduction. The reader will observe that Lemmas 5.3 and 5.4 in [9] are related with Lemma 4.2 in the present article. The triangular dihedral symmetry for the case $m = 0$ (i. e. $\binom{i+j}{i} \mod p$) was not noticed by the author because it did not match in the square grid used in [9]. In Section 4 this gap is filled. The triangular symmetry was empirically observed by other authors, at least for the fundamental block given by the first p rows - see [3], where some images and comments are displayed.

Section 5 contains a more or less coincidential interference between both symmetries in a limit case. It is shown that the number $n = 4$ is the only one composite number such that the triangle $u_n(\binom{u}{v} \mod n)$ consists of an ascendant chain of symmetric triangles of edge n^m, where $m \in \mathbb{N}$. This pattern has been also studied by A. Granville in [5] and [6]. A construction in Section 6 is possible only because one symmetric pattern is active where the other one is not. They are complementary.

Also, some natural connections with automatic sequences arise during the paper.

2 Prerequisites

Definition 2.1 A triangular lattice Θ is a set of double indexed points $P(u,v)$ of the plane, $u, v \in \mathbb{N}$, $0 \leq v \leq u$, such that all triangles in the set $\{P(u,v)P(u+1,v)P(u+1,v+1) \,|\, 0 \leq v \leq u\} \cup \{P(u,v)P(u+1,v+1)P(u,v+1) \,|\, 0 \leq v \leq u\}$ are disjoint and congruent equilateral triangles. Up to similarity there is only one triangular lattice, that will be called Θ.

Definition 2.2 Let S be a set. A triangle over S is an application $T : \Theta \to S$. For some $n \in \mathbb{N}$, let $\Theta(n)$ be the subset consisting of the first n rows of Θ, indexed from 0 to $n-1$. Let $T(n)$ be the restriction of T to the set $\Theta(n)$. The function $T(n)$ will be also called a triangle. The value $T(P(u,v))$ will be shortly written down as $T(u,v)$.

Pascal's Triangle and Pascal's Triangle modulo n are examples of triangles, with $T(u,v) = \binom{u}{v}$ and $T(u,v) = \binom{u}{v} \mod n$ respectively. Both triangles are uniquely determined by the initial conditions $T(u,0) = T(u,u) = 1$ and by the recurrence $T(u+1,v+1) = T(u,v) + T(u,v+1)$ for all $u, v \in \mathbb{N}$ with $0 \leq v \leq u$. The same recurrence must be considered once over $\mathbb{Z}$ and once over the finite cyclic group $\mathbb{Z}/n\mathbb{Z}$.

There is also another way to define Pascal's Triangles, considering a square lattice $\mathbb{N} \times \mathbb{N}$ and a recurrent double sequence given by the initial conditions $a(i,0) = a(0,j) = 1$ and $a(i,j) = a(i,j-1) + a(i-1,j)$. In this case $a(i,j) = \binom{i+j}{i}$ or respectively $\binom{i+j}{i} \mod n$, see author's papers [9] and [11]. To change the coordinates fron the square lattice coordinates to the triangular lattice coordinates, observe that:

$$a(i,j) \quad = \quad T(i+j,i),$$

$$T(u,v) \quad = \quad a(v,u-v),$$

for all $0 \leq i,j$ and $0 \leq v \leq u$.

The square lattice representation of the binomial coefficients has some advantages. As proven in [9], if $m \in \mathbb{F}_p$, if the sequence $a(i,j)$ satisfies the conditions $a(i,0) = a(0,j) = 1$ and $a(i,j) = a(i,j-1) + ma(i-1,j-1) + a(i-1,j)$, and if for $m \in \mathbb{N}$ we define the matrix $A_m = \{a(i,j) \,|\, 0 \leq i,j < p^m\}$, then:

$$A_m = A_1 \otimes (A_1 \otimes \cdots \otimes A_1) = A_1^{\otimes n}.$$

Here $\otimes$ means the (Kronnecker-) tensor product of matrice. If S is some multiplicative monoid, $A \in M_{n,m}(S)$ and $B \in M_{s,t}(S)$, then the matrix $A \otimes B$ belongs to $M_{ns,mt}(S)$ and is the matrix with block-wise representation $(a(i,j)B)_{0 \leq i < n, 0 \leq j < m}$. The $\otimes$-monomial $A^{\otimes n}$ is defined as $A \otimes A^{\otimes(n-1)}$. A_1 was called fundamental block. If $m = 0$ the recurrent double sequence $a(i,j)$ is exactly the $\binom{i+j}{i}$ as remarked above. The tensor product representation of this double sequence follows also directly from the classical theorem of Lucas concerning the value of $\binom{a}{b} \mod p$ as a function of their digits in basis p.

At this point should be mentioned that Pascal's Triangle modulo p^k is not a limit of tensor powers of matrices if $k \geq 2$. However, Pascal's Triangles modulo p^k are p-automatic, and consequently can be produced by matrix substitution and are projections of double sequences produced by two-dimensional morphisms. See [1] and [2].

Definition 2.3 A triangle $T(n) : \Theta(n) \to S$ is called symmetric if for all $0 \leq v \leq u \leq n-1$, $T(u,v) = T(u,u-v)$ and $T(u,v) = T(n-1-u+v, n-u-1)$.

To understand this definition, consider the applications $S, R : \Theta(n) \to \Theta(n)$, given by $S(u,v) = (u,u-v)$ and $R(u,v) = (n-1-v,u-v)$ for all $u,v \in \mathbb{N}$ with $0 \leq v \leq u \leq n-1$. It is only pure computation to prove that $R^3 = S^2 = id$ and that $S^{-1}RS = R^{-1}$. In fact, S is a reflection of $\Theta(n)$ across a median, R is a rotation with $120°$ of $\Theta(n)$ around its center, and the group generated by S and R is the whole dihedral group D_6, the symmetry group of the equilateral triangle. This group has six elements. Under the action of D_6, $\Theta(n)$ splits in orbits of length 6, 3 or 1. If $n \neq 3k+1$ there is no central element, so no orbit of length 1 does occur. Instead of $T(u,v) = T(n-1-u+v, n-u-1)$, one can check that $T(u,v) = T(n-v-1, u-v)$. This is just the other rotation.

Using the correspondence between triangular and square lattice coordinates, one can adapt this definition for triangles presented in square lattice coordinates.

Definition 2.4 Let $A \in M_{n,n}(S)$ be a square matrix. The set $T_1(A) = \{a(i,j) \,|\, 0 \leq i,j < n \wedge 0 \leq i+j \leq n-1\}$ is called the first triangle of A. The complemetary set $T_2(A) = \{a(i,j) \,|\, 0 \leq i,j < n \wedge i+j > n-1\}$ is the second triangle of A. $T_1(A)$ is called symmetric if it satisfies the identities $a(i,j) = a(j,i)$ and $a(i,j) = a(j,n-1-i-j)$ for all $i,j \geq 0$ with $i+j \leq n-1$.

Instead of $a(i,j) = a(j,n-1-i-j)$ one can check that $a(i,j) = a(j,n-1-i-j)$. This is again the other rotation.

3 p-Adic valuation

Let p be a prime and $v_p : \mathbb{Z} \to \mathbb{N} \cup \{\infty\}$ the p-adic valuation.

Lemma 3.1 *For $1 \leq i \leq p^m$ and $0 \leq k \leq p^m - i$ the following holds:*

$$v_p[\binom{p^m - i}{k}] = v_p[\binom{i-1+k}{i-1}].$$

Proof: By definition,

$$\binom{p^m - i}{k} = \frac{(p^m - i - (k-1)) \cdots (p^m - i)}{k!} \quad \wedge \quad \binom{i-1+k}{i-1} = \frac{i \cdots (i + (k-1))}{k!}.$$

By the group homomorphism property of valuations, it must be shown that $v_p((p^m - i) \cdots (p^m - i - (k-1))) = v_p(i \cdots (i + (k-1)))$. For, it would be enough that for all $i \leq x \leq i + (k-1)$, $v_p(p^m - x) = v_p(x)$. Indeed, $x \leq i + (p^m - i) - 1 = p^m - 1 < p^m$, so $v_p(x) < v_p(p^m) = m$. Hence, $v_p(p^m - x) = \min(v_p(p^m), v_p(x)) = v_p(x)$. □

Theorem 3.2 *The patterns $\{v_p(\binom{u}{v}) \,|\, 0 \leq v \leq u < p^m\}$ have triangular symmetry for all $m \geq 0$.*

A possible name for the pattern built by the p-valuation applied to binomial coefficients, i. e. $\{v_p(\binom{u}{v}) \,|\, 0 \leq v \leq u\}$, could be the *Pascal - Kummer Triangle*. The set with $0 \leq v \leq u \leq p^m$ contains the values $\{0, \ldots, m-1\}$ according to Corollary 1.1. An example is displayed in Figure 1.

Proof: By Lemma 3.1, the pattern is preserved by a rotation with 120° around its center. By the identity $\binom{u}{v} = \binom{u}{u-v}$, it is preserved by a reflection across its median. According to the definition 2.3 and its consequences, the pattern has triangular symmetry. □

The next Lemma has been published by I. Tomescu as a problem proposed to the readers of Gazeta Matematică in [12].

Lemma 3.3 *Let p be a prime and $n = n_k p^k + \cdots + n_0$, with $n_k, \ldots, n_0 \in \{0, \ldots, p-1\}$. The number of binomial coefficients $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$ that are multiples of p is:*

$$n + 1 - (n_0 + 1) \cdots (n_k + 1).$$

Proof: Let $a = a_k p^k + \cdots + a_0$, with $a_k, \ldots, a_0 \in \{0, \ldots, p-1\}$. By Kummer's Theorem, $p \not| \binom{n}{a}$ if and only if for all i, $n_i \geq a_i$. So for all i, a_i can be chosen in $n_i + 1$ ways. □

The following Lemma provides supplementary information about this pattern and will be also applied in a later section. It has been given as a problem to be solved during a mathematical contest in Luxemburg, 1980. For both Lemmas 3.3 and 3.4 and other nice puzzles, see [8].

Lemma 3.4 *$v_p(\binom{u}{v}) = 0$ for all $v \in \{0, \ldots, u\}$ iff $u = zp^m - 1$, $m \geq 0$ and $z \in \{1, \ldots, p-1\}$.*

Proof: By Lemma 3.3, if $u = zp^m - 1$, with $m \geq 0$ and $z \in \{1, \ldots, p-1\}$, then the number of binomial coefficients in row u that are not divisible with p is $zp^m - (z-1+1)(p-1+1) \cdots (p-1+1) = 0$. For the converse, if a number u contains a digit $n_i < p-1$ in its inner or at the end, one can produce a carry over in addition by choosing a number v with a bigger digit $v_i > n_i$ for this position. So only the first digit might be different from $p-1$. □

By Lemma 3.4 we know exactly which are the constant lines in the Pascal-Kummer Triangle.

The Pascal-Kummer Triangle is not automatic, because the values of $v_p(\binom{u}{v})$ are not bounded. To surpass this inconvenient, one has to adapt the notion of valuation for rings of classes of remainders, like $\mathbb{Z}/p^k\mathbb{Z}$. The resulting notion is not standard, because valuation theory has been developped for fields, and the rings $\mathbb{Z}/p^k\mathbb{Z}$ are not domains. However, this non-standard notion is very natural in the present context. We recall that all ideals in $\mathbb{Z}/p^k\mathbb{Z}$ have the form $p^i\mathbb{Z}/p^k\mathbb{Z}$ and that they build a descending finite chain of ideals:

$$\mathbb{Z}/p^k\mathbb{Z} = p^0\mathbb{Z}/p^k\mathbb{Z} > p\mathbb{Z}/p^k\mathbb{Z} > \cdots > p^{k-1}\mathbb{Z}/p^k\mathbb{Z} > p^k\mathbb{Z}/p^k\mathbb{Z} = 0.$$

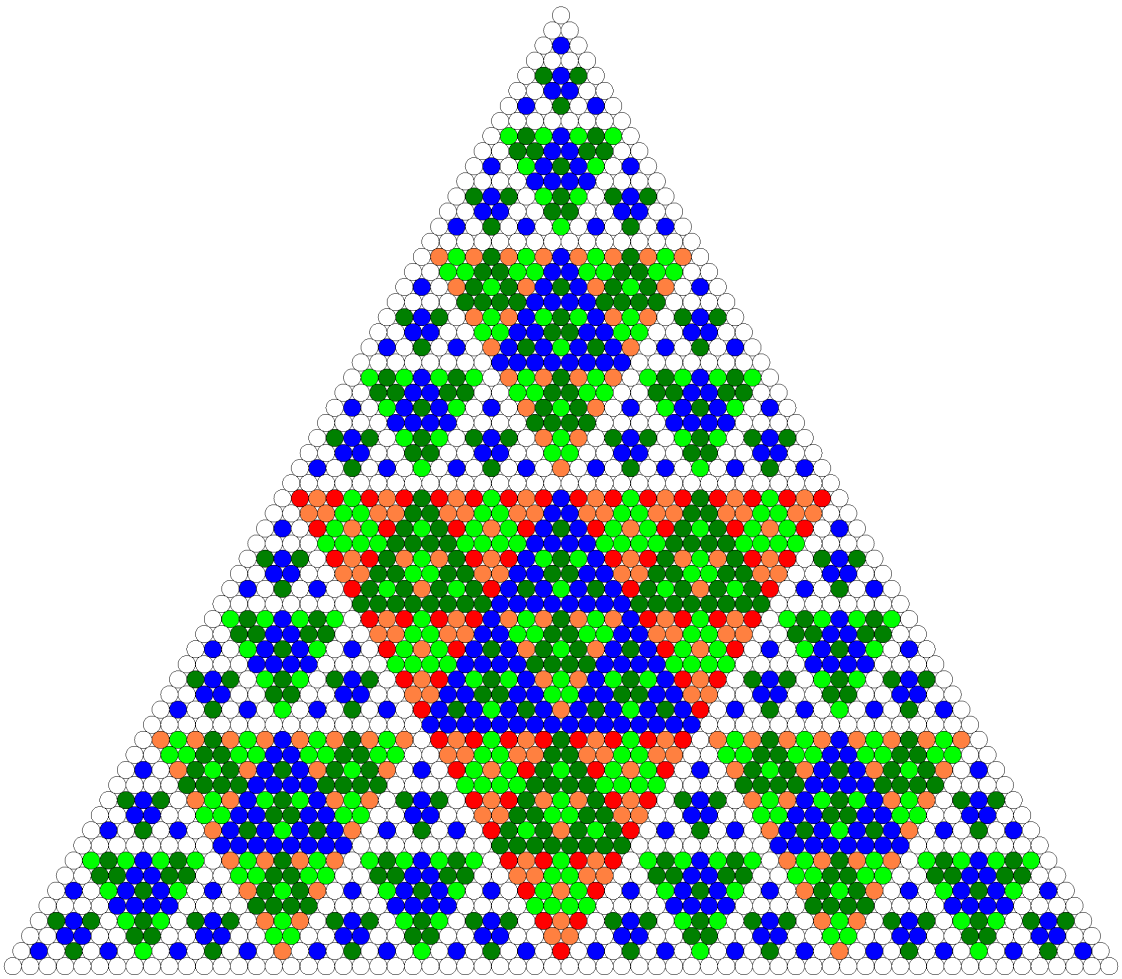

Figure 1: The first 64 rows of the Pascal-Kummer Triangle $v_2(\binom{u}{v})$.

Definition 3.5 For a prime p and for $k \geq 1$ we define $v_p : \mathbb{Z}/p^k\mathbb{Z} \to \{0, 1, \ldots, k\}$ as:

$$v_p(x) = \begin{cases} s & x \in p^s\mathbb{Z}/p^k\mathbb{Z} \wedge x \notin p^{s+1}\mathbb{Z}/p^k\mathbb{Z} \wedge s < k, \\ k & x = 0. \end{cases}$$

Corollary 3.6 *The patterns* $\{v_p(\binom{u}{v} \mod p^k) \,|\, 0 \leq v \leq u < p^m\}$ *have triangular symmetry for all* $m \geq 0$. *Moreover, the two-dimensional sequence* $\{v_p(\binom{u}{v} \mod p^k) \,|\, 0 \leq v \leq u\}$ *is* p*-automatic.*

Proof: The triangular symmetry of the patterns follows directly from Theorem 3.2. The 2-dimensional sequence is p-automatic because the 2-dimensional sequence $(\binom{u}{v} \mod p^k)$ is p-automatic, and that the p-automatic sequences are closed under projections. See the monograph [1] for both properties. However, using Kummer's Theorem, one can very easily construct an automaton generating the same sequence in square coordinates - i.e. $a(i, j) = \binom{i+j}{j} \mod p^k$. The input alphabet is $\Sigma = \{0, \ldots, p-1\} \times \{0, \ldots, p-1\}$. The set of states is $Z = \{z_0, z_1, \ldots, z_{k-1}\} \cup \{w_1, \ldots, w_{k-1}\} \cup \{f\}$. For $t < k$, z_t means that t many carries have been counted so far, but in the moment there is no carry to add. Similarly, w_t means that t many carries have been counted so far and the digit addition done in the last step produced a carry. In

state f a number of k carries have been already counted. In this case it is no more important whether in the last step a carry has been produced or not. The digits of the input (i, j) come in starting with the less significant pair (i_0, j_0). The output function ω assigns to each state the number of carries: $\omega(z_t) = \omega(w_t) = t$, $\omega(f) = k$. □

Corollary 3.7 *The patterns* $\{\binom{u}{v} \mod 2 \,|\, 0 \le v \le u < 2^m\}$ *have triangular symmetry for all* $m \ge 0$.

Proof: Indeed, for $v_2 : \mathbb{Z}/2\mathbb{Z} \to \{0, 1\}$ hold $v_2(1) = 0$ and $v_2(0) = 1$. So up to a permutation of values, $v_2(\binom{u}{v} \mod 2)$ produces the same pattern as $\binom{u}{v} \mod 2$. □

4 Sign-reduction

In the next definition the elements of the ring $\mathbb{Z}/n\mathbb{Z}$ are intentionally identified with their canonical representatives from the set $\{0, 1, \ldots, n-1\}$. The order used in the definition is the order of natural numbers.

Definition 4.1 Let n be a natural number. The sign-reduction $u_n : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is defined as:

$$u_n(x) = \begin{cases} x & 0 \le x \le n/2, \\ n - x & n/2 < x \le n - 1. \end{cases}$$

Lemma 4.2 *Let p be a prime. For $1 \le i \le p$ and $0 \le k \le p - i$ the following congruence holds:*

$$\binom{p-i}{k} \equiv (-1)^k \binom{i-1+k}{i-1} \mod p.$$

Proof: For $i = 1$ this result is folklore - but maybe not the following proof. The $(p+1)$-th row of Pascal's Triangle consists of $\binom{p}{k}$ and they are multiples of p for $k = 1, \ldots, p-1$. The p-th and $(p+1)$-th rows start in the field $\mathbb{F}_p$ as follows:

$$\begin{array}{ccccccc} & 1 & & x & & y & & z & \ldots \\ 1 & & 0 & & 0 & & 0 & & \ldots \end{array}$$

We apply the recurrence $T(u+1, v+1) = T(u, v) + T(u, v+1)$ and get successively $x = -1$, $y = 1$, $z = -1$ and so on. So $\binom{p-1}{k} \equiv (-1)^k \equiv (-1)^k \binom{1-1+k}{1-1} \mod p$, as it was to prove.

Now we continue by induction. Suppose that we have already shown that the row $p - i$ consists of elements respectively congruent with $(-1)^k \binom{i-1+k}{i-1} \mod p$ for $0 \le k \le p - i$, and suppose that in the row $p - i - 1$ we have already shown that $\binom{p-i-1}{k} \equiv (-1)^k \binom{i+k}{i} \mod p$. The next binomial coefficient is $\binom{p-i-1}{k+1}$ and has the following position in Pascal's Triangle:

$$\begin{array}{ccc} \binom{p-i-1}{k} & & \binom{p-i-1}{k+1} \\ & \binom{p-i}{k+1} & \end{array}$$

Consequently:

$$\binom{p-i-1}{k+1} = \binom{p-i}{k+1} - \binom{p-i-1}{k} \equiv (-1)^{k+1} \binom{i-1+k+1}{i-1} - (-1)^k \binom{i+k}{i} =$$

$$= (-1)^{k+1} \left[\binom{i+1}{i-1} + \binom{i+k}{i} \right] = (-1)^{k+1} \binom{i+k+1}{i} = (-1)^{k+1} \binom{(i+1)-1+(k+1)}{(i+1)-1} \mod p.$$

□

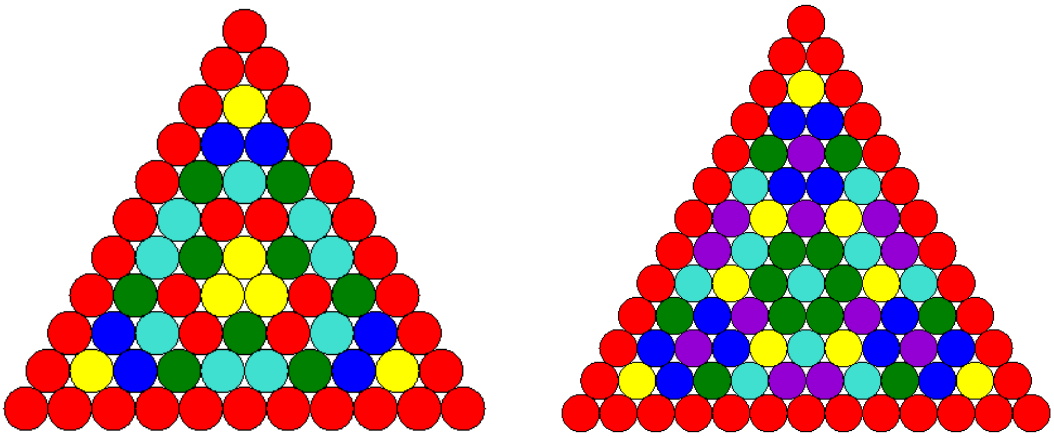

Figure 2: $u_{11}(\binom{u}{v} \mod 11)$ with $0 \le v \le u \le 10$ and $u_{13}(\binom{u}{v} \mod 13)$ with $0 \le v \le u \le 12$.

Lemma 4.3 *The pattern* $T_1(A_1) = \{u_p(\binom{u}{v} \mod p) \,|\, 0 \le v \le u < p\}$ *has triangular symmetry.*

Proof: Sign-reduction over the identity in Lemma 4.2 yields: $\binom{p-i}{k} \mod p = \binom{i-1+k}{i-1} \mod p$. This means that pattern is preserved by a rotation with 120° around its center. By the identity $\binom{u}{v} = \binom{u}{u-v}$, the pattern is preserved by a reflection across its median. According to the definition 2.3 and its consequences, the pattern has triangular symmetry. □

See Figure 2 for two examples.

Lemma 4.4 *In* $u_p(\binom{u}{v} \mod p)$ *the configuration:*

$$\begin{array}{ccc} & a & \\ a & & a \end{array}$$

is possible only if $p \le 3$ *or* $a = 0$. *Consequently, the central configurations in* T *for* $p \ge 5$ *are described below. Here always* $0 \ne a \ne b \ne 0$*:*

$$\begin{array}{ccccc} & a & & a & \\ a & & b & & a \\ & a & & a & \end{array} \qquad \text{if} \qquad p = 4k+1,$$

$$\begin{array}{ccccc} b & & a & & b \\ & a & & a & \\ & & b & & \end{array} \qquad \text{if} \qquad p = 4k+3.$$

Proof: Verify the eight possible relations $(\epsilon_1 p + (-1)^{1+\epsilon_1} a) + (\epsilon_2 p + (-1)^{1+\epsilon_2} a) = (\epsilon_3 p + (-1)^{1+\epsilon_3} a)$ for $\epsilon_1, \epsilon_2, \epsilon_3 \in \{0, 1\}$. The cases 100 and 011 lead to $3a = 0$, so $a = 0$ or $p = 3$. The cases 000 and 101 lead to $a = 0$. The other cases lead to $\pm p = \mp a$ or $2p = a$ possible only if $p \in \{2, 3\}$ and $a = 0$. The central configurations depend of the triangular symmetry, of the existence of a central element and of this condition. □

For the next steps we need the tensor product structure of Pascal's Triangle $\mod p$ as it has been recalled in the Introduction. Let $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ be the multiplicative group pf the field $\mathbb{F}_p$.

We observe that the application:

$$u_p : \mathbb{F}_p^\times \to \{1, 2, \ldots, (p-1)/2\} := H_p,$$

has $\#u_p^{-1}(a) = 2$, for all $a \in H_p$, that $u_p^{-1}(1) = \{1, -1\}$ and that for all $a, b \in H_p$ and for all $x \in u_p^{-1}(a)$, $y \in u_p^{-1}(b)$, $u_p(xy)$ does not depend of the choice of the representatives x and y. Consequently one can define a new multiplication $\times$ over H_p by $a \times b = u_p(u_p^{-1}(a)u_p^{-1}(b))$. This operation induces a structure of group $(H_p, \times, 1)$ such that $u_p : \mathbb{F}_p^\times \to H_p$ is a homomorphism of groups with kernel $\{1, -1\} =< -1 >$. This yields:

$$H_p \cong \mathbb{F}_p^\times / < -1 > .$$

If we complete now this multiplication in a natural way with $a \times 0 = 0 \times a = 0$, we get:

Lemma 4.5 *If* $A_m = \{u_p(\binom{i+j}{i} \mod p) \,|\, 0 \leq i, j < p^m\} \in M_{p^m,p^m}(H_p \cup \{0\})$, *then:*

$$A_m = A_1 \otimes (A_1 \otimes \cdots \otimes A_1) = A_1^{\otimes n},$$

where the tensor product is defined according to the multiplication $\times$ *on* $H_p \cup \{0\}$ *and the tensor product monomial is inductively defined by* $A^{\otimes n} = A \otimes A^{\otimes(n-1)}$.

Lemma 4.6 *Let* $(J, \times)$ *be some associative monoid containing an element* 0 *with the property that for all* $x \in J$, $x \times 0 = 0 \times x = 0$. *Let* $A \in M_{m,m}(J)$ *and* $B \in M_{n,n}(J)$ *two matrices, such that* $T_1(A)$, $T_1(B)$ *have both triangular symmetry and* $T_2(A)$, $T_2(B)$ *consist both only of zeros. (Compare with Definition 2.4). Then for the matrix* $A \otimes B \in M_{mn,mn}(J)$ *holds:* $T_1(A \otimes B)$ *has triangular symmetry and* $T_2(A \otimes B)$ *consists only of zeros.*

Proof: Pure computation using Definition 2.4. □

More interesting than the proof is maybe the fact that if one tries to prove Lemma 4.6 in the form: *if both* $T_i(A)$ *have triangular symmetry and both* $T_i(B)$ *have triangular symmetry, then both* $T_i(A \otimes B)$ *have triangular symmetry*, it just does not work. Indeed, very easy counterexamples with $m = n = 2$ for T_2 and with $m = 3$ and $n = 2$ for both T_i can be constructed.

Theorem 4.7 *The patterns* $\{u_p(\binom{u}{v} \mod p) \,|\, 0 \leq v \leq u < p^m\}$ *have triangular symmetry for all* $m \geq 0$.

Proof: By induction in $m \geq 0$. The case $m = 0$ is trivial. For the case $m = 1$ we apply Lemma 4.3. Now we turn to square coordinates and we observe that $T_1(A_1)$ has triangular symmetry and that $T_2(A_1)$ consists only of zeros. Indeed, for $0 < i, j < p$ with $2p > i + j \geq p$, $p \,|\, \binom{i+j}{i}$. This means by Lemma 4.5 and by Lemma 4.7 that all $A_m = A_1^{\otimes n}$ are such that $T_1(A_m)$ has triangular symmetry and $T_2(A_m)$ consists only of zeros. But the patterns in question are exactly $T_1(A_m)$. □

For an example, see Figure 3.

We observe that the tensor product structure confirms Lemma 3.4. Another consequence of the tensor product structure is that the double sequence $u_p(\binom{u}{v} \mod p)$ is p-automatic. This follows again by the fact that the p-automatic sequence $\binom{u}{v} \mod p$ is projected onto the finite set $H_p \cup \{0\}$. In fact we know more: the sequnce is a 2-dimensional morphic sequence, with start-letter 1 and with substitutions $a \rightsquigarrow a \times A_1$ for all $a \in H_p \cup \{0\}$, where $\times$ is the appropriate multiplication. All elements of $H_p \cup \{0\}$ occur in the pattern, and can be found already in the second diagonal, near the edge.

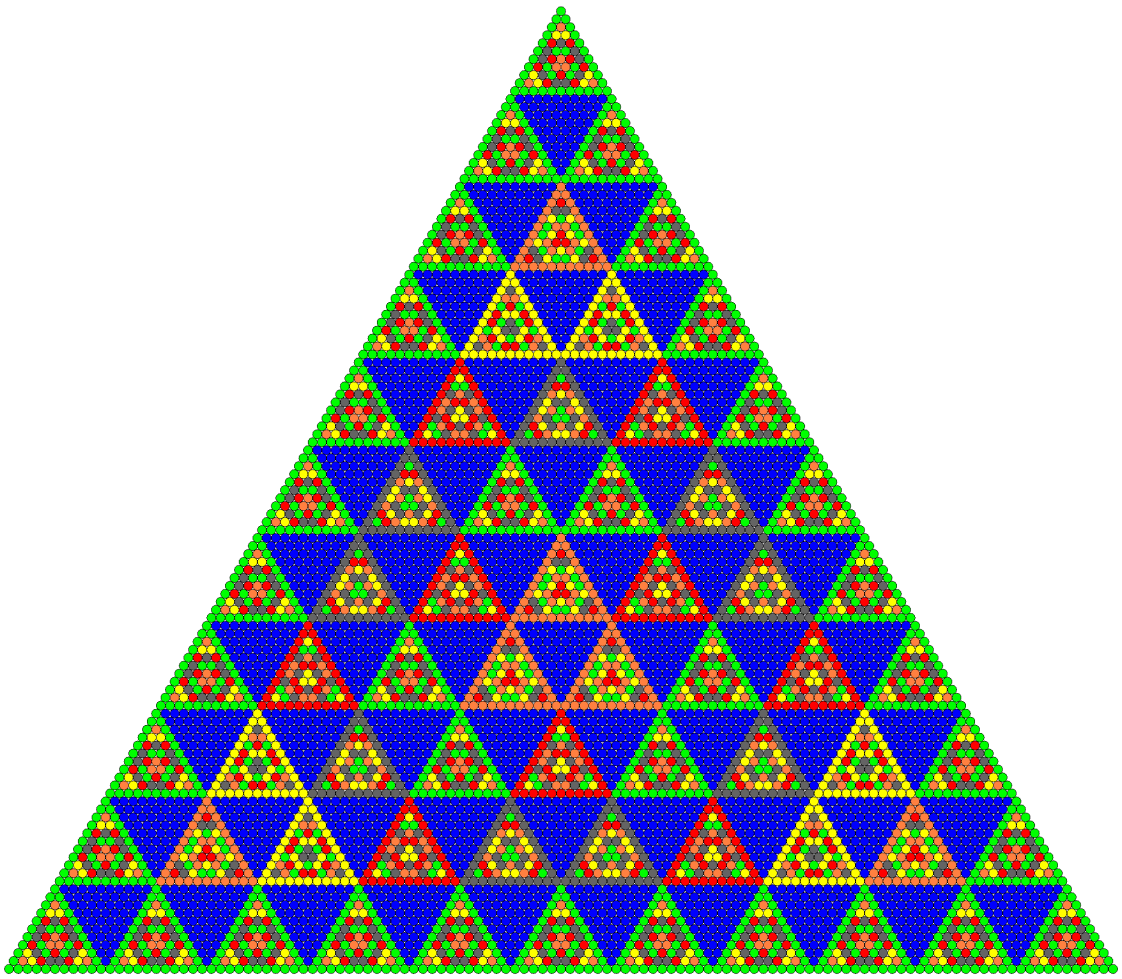

Figure 3: The first 121 rows of $u_{11}(\binom{u}{v} \mod 11)$, building $T_1(A_1 \otimes A_1)$. $T_1(A_1)$ multiplied with different group elements from H_{11} yields new blocks with permuted colors.

5 A property of the number 4

In this section we show that the number $n = 4$ is the only one composite number with the property that the triangles $\{u_n(\binom{u}{v} \mod n) \,|\, 0 \le v \le u \le n^m\}$ have triangular symmetry for all $m \ge 0$.

Lemma 5.1 is folklore. It can be found e.g. in the preprint [7], whose author has got the statement during a night-dream. For statements like Lemma 5.1 and much stronger, see Granville's remarkable article [4]. This Lemma is strong enough for our needs.

Lemma 5.1 *For all $m, n \in \mathbb{N}$ and prime p, $\binom{np}{mp} \equiv \binom{m}{n} \mod p^2$.*

Proof: (from [7]) In $(1+X)^{np} = [(1+X)^p]^n$ the coefficient of X^{mp} is:

$$\binom{np}{mp} = \sum_{\substack{0 \le k_i \le p \\ k_1 + \cdots + k_n = mp}} \prod_i \binom{p}{k_i}.$$

Modulo p^2 contribute only those terms with at least $n-1$ many k_i equal 0 or p. The sum of k_i being multiple of p, all of them must be 0 or p. So m of n many k_i must be p, and the number of possible choices is $\binom{n}{m}$. □

Theorem 5.2 *The unique composite $n \in \mathbb{N}$ such that the patterns $\{u_n(\binom{u}{v} \mod n) \mid 0 \le v \le u \le n^m\}$ have triangular symmetry for all $m \in \mathbb{N}$ is $n = 4$. In its case all patterns $\{u_4(\binom{u}{v} \mod 4) \mid 0 \le v \le u \le 2^m\}$ have triangular symmetry, and the patterns are the same as those given by $\{v_2(\binom{u}{v} \mod 4) \mid 0 \le v \le u \le 2^m\}$.*

Proof: The proof is structured in a sequence of Claims.

Claim: 1. *If all patterns $\{u_n(\binom{u}{v} \mod n) \mid 0 \le v \le u < n^m\}$ have triangular symmetry, then n must be a prime-power.*

Let $n = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$ be the prime factor decomposition of n. By the Chinese Remainder Theorem the following rings are isomorphic:

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \mathbb{Z}/p_2^{n_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{n_s}\mathbb{Z},$$

by $x \mod n \rightsquigarrow (x \mod p_1^{k_1} \cdots p_s^{k_s})$ and by this isomorphism $1 \in \mathbb{Z}/n\mathbb{Z}$ corresponds to $(1, 1, \ldots, 1)$. Suppose that the given sets have triangular symmetry. This implies that all $\binom{n^m-1}{k} = \pm 1$ for $m \in \mathbb{N}$ and $0 \le k \le n^m$. In particular, $v_p(\binom{n^m}{k}) = 0$ for all $0 \le k \le n^m$. If we focus on p_1 and apply Lemma 3.4, it follows that there is a sequence (x_m) taking values in $\{1, \ldots, p_1 - 1\}$ and an increasing sequence (k_m) of natural numbers such that for all $m \in \mathbb{N}$, $x_m p_1^{k_m} = p_1^{mn_1} p_2^{mn_2} \cdots p_s^{mn_s}$. The sequence (x_m) has a constant subsequence; let x be its constant value. It turns out that x has not a unique prime factor decomposition, unless $p_2 = \cdots = p_s = 1$.

Claim: 2. *If $n = p^k$ such that all patterns $\{u_n(\binom{u}{v} \mod n) \mid 0 \le v \le u < n^m\}$ have triangular symmetry and $k \ge 2$, then p cannot be an odd prime.*

Suppose that $n = p^k$, $k \ge 2$ and p is an odd prime. By Lemma 5.1,

$$\binom{p^k}{p^{k-1}} \equiv \binom{p}{1} = p \mod p^2,$$

so $\binom{p^k}{p^{k-1}} \equiv ap^2 + p \mod p^k$. If the row $p^k - 1$ consists only of $\pm 1 \mod p^k$, then $ap^2 + p \mod p^k$ must belong to the set $\{\pm 2, 0\}$, which is the set of possible sums of two elements of row $p^k - 1$. This is impossible, because $p \mod p^2$ must be then ± 2, which implies $p = 2$.

Claim: 3. *If $n = 2^k$ such that all patterns $\{u_n(\binom{u}{v} \mod n) \mid 0 \le v \le u < n^m\}$ have triangular symmetry, then $k \le 2$.*

Suppose $n = 2^k$ and $k \ge 3$. It follows:

$$\binom{2^k - 1}{2} = \frac{(2^k - 1)(2^k - 2)}{2} = 2^{2k-1} - 2^k - 2^{k-1} + 1 \equiv -2^{k-1} \mod 2^k.$$

For $k \ge 3$, $-2^{k-1} \mod 2^k$ cannot be $\pm 1 \mod 2^k$.

Claim: 4. *All patterns $\{u_4(\binom{u}{v} \mod 4) \mid 0 \le v \le u \le 2^m\}$ have triangular symmetry, and are the same as those given by $\{v_2(\binom{u}{v} \mod 4) \mid 0 \le v \le u \le 2^m\}$.*

If we compare the functions $v_2 : \mathbb{Z}/4\mathbb{Z} \to \{0, 1, 2\}$ with $u_4 : \mathbb{Z}/4\mathbb{Z} \to \{0, 1, 2\}$ we see that:

$$v_2(x) = \begin{cases} 2 & x = 0, \\ 0 & x = 1 \vee x = 3, \\ 1 & x = 2, \end{cases} \qquad u_4(x) = \begin{cases} 0 & x = 0, \\ 1 & x = 1 \vee x = 3, \\ 2 & x = 2. \end{cases}$$

So up to a permutation of values, v_2 and u_4 are equal and produce the same pattern. This pattern is symmetric by the Theorem 3.2. □

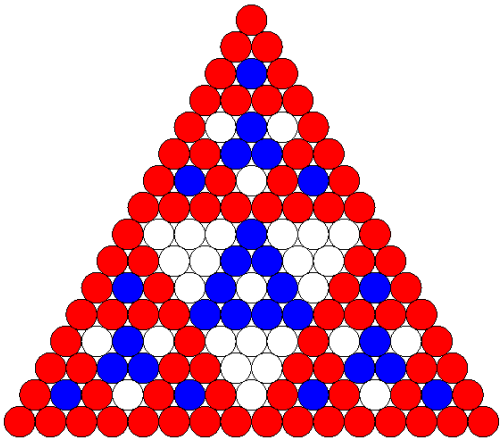

Figure 4: The first 16 rows of $u_4(\binom{u}{v} \mod 4)$ or of $v_2(\binom{u}{v} \mod 4)$.

First 16 lines of this pattern can be seen in Figure 4. The function u_4 has been also considered by Zaphod Beeblebrox in the nice papers [4] and [5] by A. Granville. A little bit in this spirit, we show now a complete description of the pattern.

Corollary 5.3 *The double sequence* $u_4(\binom{i+j}{i} \mod 4)$ *consists of the minors:*

$$A_1 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix}, \quad A_4 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Moreover, the whole double sequence can be generated starting with A_1 *and successively applying the following substitution rules:*

$$A_1 \rightsquigarrow \begin{pmatrix} A_1 & A_2 \\ A_2 & A_3 \end{pmatrix}, \quad A_2 \rightsquigarrow \begin{pmatrix} A_1 & A_2 \\ A_2 & A_3 \end{pmatrix}, \quad A_3 \rightsquigarrow \begin{pmatrix} A_3 & A_3 \\ A_3 & A_4 \end{pmatrix}, \quad A_4 \rightsquigarrow \begin{pmatrix} A_4 & A_4 \\ A_4 & A_4 \end{pmatrix}.$$

Proof: The author displayed a substitution with eight minors generating the pattern $(\binom{u}{v} \mod 4)$ in [10]. If we apply the function u_4 on these eight minors element-wise, two of them yield the minors called here A_3 and A_4 (which starting with A_3 would generate alone a pattern isomorphic with $\binom{u}{v} \mod 2$), other two of them reduce to A_1 and four of them reduce to A_2. The big surprise comes when one applies u_4 also on the rules of substitution. Without any contradiction, they fall together onto the rules given here, exactly like the minors: one, one, two and four at a time. □

6 The last non-zero digit symmetry

The functions v_p and u_p are complementary in the sense that one of them is active exactly over the places where the other one is constant. We can glue them together by considering their values as natural numbers and building the sum $u_p(x) + v_p(x)$. This function generate symmetric patterns if applied over $\binom{u}{v}$ with $0 \leq v \leq u < p^m$ for all $m \in \mathbb{N}$, but has the disadvantage, that values $0, 1, \ldots, \min(m-1, (p-1)/2)$ have not a unique interpretation anymore. Another idea is to fix the value of m and to consider the function $f(u,v) = m - 1 - v_p(\binom{u}{v}) + u_p(\binom{u}{v} \mod p)$. Now the two complementary patterns glue well and values have a unique interpretation. Unhappily, u_p is not too creative for $p \leq 5$ and v_p becomes interesting when $m \geq 4$.

But one can get much more if one applies u_p on the last non-zero digit of $\binom{u}{v}$ written in basis p.

Definition 6.1 Let $w_p : \mathbb{Z} \setminus \{0\} \to \mathbb{Z}$, given by $w_p(x) = x/p^{v_p(x)}$, the p-free part of x.

Lemma 6.2 *(Anton - Stickelberger - Hensel) Let p be prime, and $m, n \in \mathbb{N}$ with $n \geq m$. Let $r = n - m$. Let $n = n_0 + n_1 p + \cdots + n_d p^d$ with $0 \leq n_i < p$, and similarly for m and n with digits m_i and r_i respectively. Finally, let $v_p(\binom{n}{m}) = k$. Then:*

$$w_p(\binom{n}{m}) \equiv (-1)^k \left(\frac{n_0!}{m_0! r_0!}\right)\left(\frac{n_1!}{m_1! r_1!}\right) \cdots \left(\frac{n_d!}{m_d! r_d!}\right) \mod p.$$

Proof: See [4] for the proof of a stronger identity, modulo p^k. □

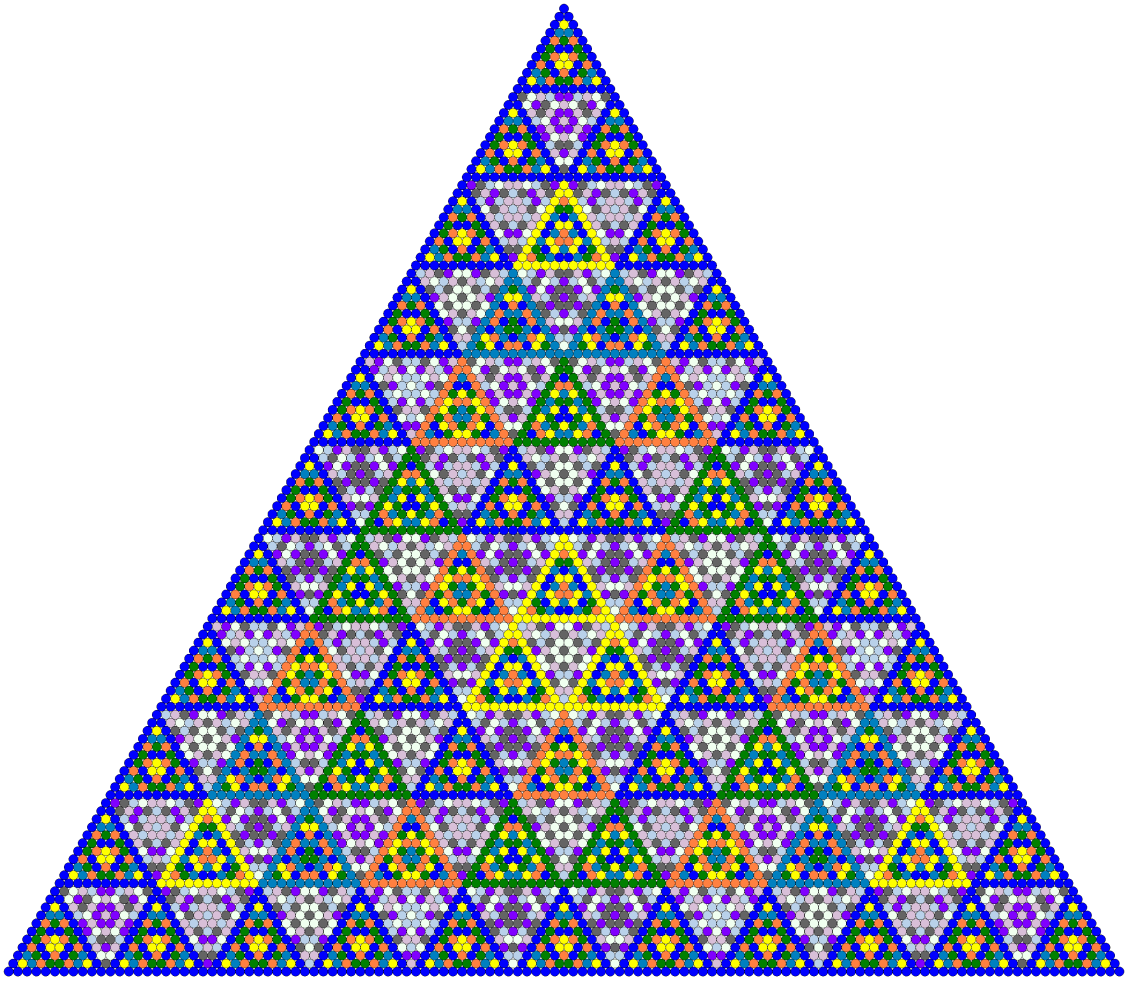

Figure 5: $u_{11}(w_{11}(\binom{u}{v}) \mod 11) + 5v_{11}(\binom{u}{v})$ with $0 \leq v \leq u \leq 121$.

Theorem 6.3 *Let p be a prime. The patterns $\{u_p(w_p(\binom{u}{v}) \mod p) \,|\, 0 \leq v \leq u \leq p^m\}$ have triangular symmetry for all $m \in \mathbb{N}$.*

Proof: Fix some $m \in \mathbb{N}$. Like before, it is enough to prove that one rotation conserve the pattern. We use this time the rotation $(u, v) \rightsquigarrow (n - 1 - v, u - v)$. It is to show that:

$$u_p\big(w_p(\binom{n}{s}) \mod p\big) = u_p\big(w_p(\binom{p^m - 1 - s}{n - s}) \mod p\big).$$

In order to use Lemma 6.2, let $r = n - s$, and n_i, r_i, s_i their digits in basis p, with $0 \leq i \leq m-1$. We observe that $p^m - 1$ in basis p consists of the repeated digit $p-1$ only, and that $p^m - 1 - s$ consists of the digits $p - 1 - s_i$. Moreover $(p^m - 1 - s) - (n - s) = p^m - 1 - n$, that consists of the digits $p-1-n_i$. Also recall that u_p and the projection $\mod p$ are multiplicative homomorphisms. One has to show that:

$$u_p\big(\frac{n_0!}{r_0!s_0!} \mod p\big) \cdots u_p\big(\frac{n_{m-1}!}{r_{m-1}!s_{m-1}!} \mod p\big) =$$
$$= u_p\big(\frac{(p-1-s_0)!}{r_0!(p-1-n_0)!} \mod p\big) \cdots u_p\big(\frac{(p-1-s_{m-1})!}{r_{m-1}!(p-1-n_{m-1})!} \mod p\big).$$

Now we focus on some factor $u_p(\frac{(p-1-s_i)!}{r_i!(p-1-n_i)!} \mod p)$.

$$u_p\big(\frac{(p-1-s_i)!}{(p-1-n_i)!} \mod p\big) = u_p\big(\frac{1 \cdot 2 \cdots (p-s_i-2)(p-s_i-1)}{1 \cdot 2 \cdots (p-n_i-2)(p-n_i-1)} \mod p\big).$$

Recall that by definition $u_p(x) = u_p(p-x)$. We apply this identity on every factor. One gets:

$$u_p\big(\frac{(p-1) \cdot (p-2) \cdots (s_i+2)(s_i+1)}{(p-1) \cdot (p-2) \cdots (n_i+2)(n_i+1)} \mod p\big).$$

But according to Wilson's Theorem, $(p-1)! \equiv -1 \mod p$, so the last term displayed is equal with:

$$u_p\big(\frac{(-1)/s_i!}{(-1)/n_i!} \mod p\big) = u_p\big(\frac{n_i!}{s_i!} \mod p\big).$$

Now the equality to show follows by equality factor-wise. □

Corollary 6.4 *The patterns* $\{u_p(w_p(\binom{u}{v}) \mod p) + v_p(\binom{u}{v})(p-1)/2 \,|\, 0 \leq v \leq u \leq p^m\}$ *have triangular symmetry for all* $m \in \mathbb{N}$.

Proof: This follows directly from Theorem 3.2 and Theorem 6.3. □

An application of the Corollary 6.4 can be seen in Figure 5. The advantage of this function is that it does not represent only the last non-zero digit, but also the p-adic valuation. Those patterns suggest that all sets $v_p(\binom{u}{v}) = k$ have a structure of tensor product of matrices, exactly like the set $v_p(\binom{u}{v}) = 0$. This is a question to study.

References

[1] **Jean-Paul Allouche, Jeffrey Shallit**: *Automatic sequences - theory, applications, generalizations.* Cambridge University Press, 2003.

[2] **J.-P. Allouche, F. von Haeseler, H.-O. Peitgen, A. Petersen, G. Skordev**: *Automaticity of double sequences generated by one-dimensional linear cellular automata.* Theoretical Computer Science, 188, 195 - 209, 1997.

[3] **Mike Bardzell, Jennifer Bergner, Kathleen Shannon, Don Spickler, Tyler Evans**: *PascGalois Abstract Algebra Classroom Resources.* Math DL - The MAA Mathematical Sciences Digital Library, http://mathdl.maa.org/mathDL/47/?pa=content&sa=viewDocument&nodeId=2636, 2008.

[4] **Andrew Granville**: *Arithmetic Properties of Binomial Coefficients I: Binomial coefficients modulo prime powers.* Canadian Mathematical Society Conference Proceedings 20, 253 - 275, 1997.

[5] **Andrew Granville**: *Zaphod Beeblebrox brain and the fifty-ninth row of Pascal's triangle.* American Mathematical Monthly, 99, 4, 318 - 331, 1992.

[6] **Andrew Granville**: *Correction to: Zaphod Beeblebrox brain and the fifty-ninth row of Pascal's triangle.* American Mathematical Monthly, 104, 9, 1997.

[7] **Mike Swarbrick Jones**: *A binomial congruence.* Preprint 2010.

[8] **Dorel Miheţ**: *Legendre's and Kummer's theorems again.* Resonance, 15, 12, 1111 - 1121, 2010.

[9] **Mihai Prunescu**: *Self-similar carpets over finite fields.* European Journal of Combinatorics, 30, 4, 866 - 878, 2009.

[10] **Mihai Prunescu**: *Recurrent two-dimensional sequences generated by homomorphisms of finite abelian p-groups with periodic initial conditions.* Fractals, 19, 4, 431 - 442, 2011.

[11] **Mihai Prunescu**: *$\mathbb{F}_p$-affine recurrent n-dimensional sequences over $\mathbb{F}_q$ are p-automatic.* To appear in European Journal of Combinatorics, 34, 260 - 284, 2013. See also http://home.mathematik.uni-freiburg.de/prunescu/fpaffine.pdf.

[12] **Ioan Tomescu**: *Problem proposed to the readers.* Gazeta Matematică, XCIV, 1983.