

KATHOLIEKE
UNIVERSITEIT
LEUVEN

SUBSTITUTIONS GENERATING THE p-ADIC VALUATION OF THE BINOMIAL AND LEGENDRE-POLYNOMIAL COEFFICIENT MATRICES

André Barbé, Gencho Skordev

SCD/SISTA report nr. 08-182
Oktober 2008

INGENIEURSWETENSCHAPPEN
Departement Elektrotechniek (ESAT-SCD)
Kasteelpark Arenberg, 10
B3001 Leuven /Heverlee - Belgium

SUBSTITUTIONS GENERATING THE p-ADIC VALUATION OF THE BINOMIAL AND LEGENDRE-POLYNOMIAL COEFFICIENT MATRICES.

A. Barbé
Katholieke Universiteit Leuven
Department of Electrical Engineering ESAT, Division SCD
Kasteelpark Arenberg 10
3001 Leuven, Belgium
andre.barbe@esat.kuleuven.be

G. Skordev
Cevis-Universität Bremen
Universitätsallee 29
28359 Bremen, Germany
skordev@cevis.uni-bremen.de

Abstract

We consider the fractal matrix which describes the divisibility properties of the coefficients of the Legendre polynomials by prime powers, and derive a block matrix substitution system that generates it. Central in the development is a similar substitution for a particular matrix of binomial coefficients.

Keywords: Fractal Matrices, Pascal Triangle, Polynomial Sequences, p-adic Number Representations, Divisibility by Prime Powers, Kummer Lemma, Matrix Substitution, Tiling Substitutions

1 Introduction

In this paper, we will consider structural aspects of certain divisibility properties –by powers of a prime number $p > 2$– of the coefficient table (sequence, matrix) associated with the Legendre polynomials (see, e.g., Abramowitz and Stegun[1])

$$P_l(x) = \frac{1}{2^l} \sum_{v=0}^{\lfloor l/2 \rfloor} (-1)^v \binom{l}{v} \binom{2l-2v}{l} x^{l-2v} \qquad l \in \mathbb{N}. \tag{1}$$

Divisibility properties of the coefficients of Legendre polynomials have been considered by several authors, e.g., Holt[2], Wahab[3], Carlitz[4], Honda[5], Landweber[6], Yui[7], Brylinski[8], Robert[9], Zuber[10], Allouche and Skordev[11]. The Schur congruence for the Legendre polynomials is the most prominent example (Wahab[3], Carlitz[4]).

Under the variable transformation $k = l - 2v$ (or $v = \frac{l-k}{2}$, $v \in \mathbb{N}$), (1) can be rewritten as

$$P_l(x) = \frac{1}{2^l} \sum_{k=0}^{l} (-1)^{\frac{l-k}{2}} L(k,l) x^k, \tag{2}$$

with, for $l \in \mathbb{N}$, $0 \leq k \leq l$

$$L(k,l) = \binom{l}{\frac{l-k}{2}}\binom{l+k}{l} \quad \text{when } l-k \text{ is even} \tag{3}$$

$$= 0 \quad \text{when } l-k \text{ is odd.} \tag{4}$$

By extending the L-coefficients with $L(k,l) = 0$ for $l \in \mathbb{N}$ and $k > l$,we can consider $L = (L(k,l))_{(k,l)\in\mathbb{N}^2}$ as a (double) sequence on the integer lattice

$$\mathcal{L} = \{(k,l)|(k,l) \in \mathbb{N}^2\}.$$

Defining the "Legendre coefficient sequence" $P = (P(k,l))_{(k,l)\in\mathbb{N}^2}$: where

$$P(k,l) = \frac{1}{2^l}(-1)^{\frac{l-k}{2}}L(k,l). \tag{5}$$

then yields

$$P_l(x) = \sum_{k=0}^{\infty} P(k,l)x^k.$$

Just to give an idea, the first 9×9 elements of L are represented in the following matrix:

$$\begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \downarrow l \end{array} \begin{array}{c} \overset{k}{\rightarrow} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots \\ 2 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots \\ 0 & 12 & 0 & 20 & 0 & 0 & 0 & 0 & 0 & \cdots \\ 6 & 0 & 60 & 0 & 70 & 0 & 0 & 0 & 0 & \cdots \\ 0 & 60 & 0 & 280 & 0 & 252 & 0 & 0 & 0 & \cdots \\ 20 & 0 & 420 & 0 & 1260 & 0 & 924 & 0 & 0 & \cdots \\ 0 & 280 & 0 & 2520 & 0 & 5544 & 0 & 3432 & 0 & \cdots \\ 70 & 0 & 2520 & 0 & 13860 & 0 & 6435 & 0 & 12870 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \end{bmatrix} \tag{6}$$

Apart from sequences on $\mathcal{L}$, sequences on other integer lattices denoted $\widetilde{\mathcal{L}}$, $\widehat{\mathcal{L}}$ and $\widehat{\mathcal{L}}^*$ will be used as well. These lattices are defined and graphically represented in Fig. 1. Throughout this paper, graphical representations use a coordinate system (k,l), where k is displayed along the horizontal axis, and l along the vertical axis (positive directions respectively to the right and downwards).

A sequence $X = (X(k,l))_{(k,l)\in\mathcal{L}}$ will usually be considered as a double infinite matrix, and will then be denoted by boldface capitals $\mathbf{X}$ and $\mathbf{X}(k,l)$ for the matrix and the corresponding element with coordinates (k,l). Note that, for consistency reasons, and contrary to common practice, k refers to columns, l to rows. Ranking of columns/rows starts at 0. In general, $\mathbf{X}_m$, where $\mathbf{X}$ may be replaced by any bold capital letter, denotes a $\mathbb{Z}p^m \times p^m$-matrix. $\mathbf{X}_m$ is said to have *logsize* (logarithmic size) m.

We will associate a graphical representation with a sequence X (or matrix $\mathbf{X}$), by coloring cell $[k,k+1) \times [l,l+1) \in \mathbb{R}^2$ with a color specifically associated to the value $X(k,l)$ (or $\mathbf{X}(k,l)$. This is illustrated in Fig. 2 for part of the graphical representation of the Legendre matrix $(\mathbf{P}(k,l) \bmod 25)$. This representation has a striking regular fractal structure. Here p has to be an odd prime number, as the coefficients of P are rational numbers whose denominators are powers of two. The fractal structure of the Legendre matrix mod p was

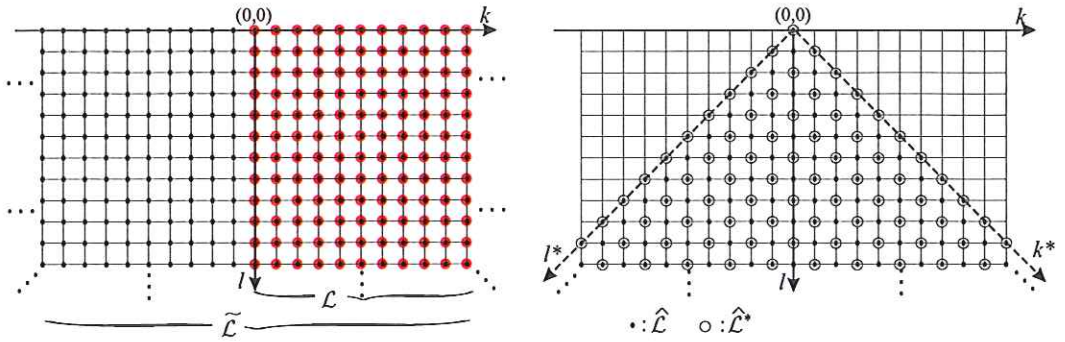

Figure 1: The integer lattices $\mathcal{L} = \{(k,l)|(k,l) \in \mathbb{N} \times \mathbb{N}\}$, $\widetilde{\mathcal{L}} = \{(k,l)|(k,l) \in \mathbb{Z} \times \mathbb{N}\}$ (left), $\widehat{\mathcal{L}} = \{(k,l)|(k,l) \in \mathbb{Z} \times \mathbb{N},\ |k| \leq l\}$, $\widehat{\mathcal{L}}^* = \{(k,l)|(k,l) \in \widehat{\mathcal{L}},\ |(l-k) \text{ is even}\}$(right).

studied in von Haeseler *et al.*[12], using matrix substitutions and iterated function systems derived from the so-called Carlitz-properties of these sequences (which in turn goes back to the Schur congruence, see Allouche and Skordev[11]).

The main topic of this paper is the more interesting and complicated fractal structure of the matrix $v_p\mathbf{P} = (v_p(\mathbf{P}(k,l))_{(k,l)\in\mathcal{L}}$ of p-adic valuations of the elements in the Legendre matrix $\mathbf{P}$, see Fig. 3 and Fig. 4. Remind that the p-adic valuation $v_p(a)$ of an integer $a \neq 0$ is the highest power of p which divides a, and $v_p(0) = \infty$ (see e.g., Allouche and Shallit[13], p. 39). Observe that, because p is an odd prime, the divisibility of $\mathbf{P}(k,l)$ by p^s for some $s \geq 1$ is the same as the divisibility by p^s of $\mathbf{L}(k,l)$, implying that $v_p(\mathbf{P}) = v_p(\mathbf{L})$. Our goal is to find an iterative description of the matrix $v_p(\mathbf{L})$. This will be done by showing that $\mathbf{L}$ is the elementwise product (so-called Hadamard or Schur product, see Horn and Johnson[14], Ch. 5) of two matrices $\mathbf{B}$ and $\mathbf{G}$, which are easier to deal with.

The first matrix is defined as

$$\mathbf{B}(k,l) \quad = \quad \binom{l+k}{l}. \tag{7}$$

It contains a particular display of the binomial coefficients, and hence will be called "binomial matrix":

$$\mathbf{B} = \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \downarrow l \end{matrix} \begin{matrix} \overset{k}{\rightarrow} \\ \end{matrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \cdots \\ 1 & 3 & 6 & 10 & 15 & 21 & 28 & 36 & 45 & \cdots \\ 1 & 4 & 10 & 20 & 35 & 56 & 84 & 120 & 165 & \cdots \\ 1 & 5 & 15 & 35 & 70 & 126 & 210 & 330 & 495 & \cdots \\ 1 & 6 & 21 & 56 & 126 & 252 & 462 & 792 & 1287 & \cdots \\ 1 & 7 & 28 & 84 & 210 & 462 & 924 & 1716 & 3003 & \cdots \\ 1 & 8 & 36 & 120 & 330 & 792 & 1716 & 3432 & 6435 & \cdots \\ 1 & 9 & 45 & 165 & 495 & 1287 & 3003 & 6435 & 12870 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix} \tag{8}$$

In order to construct the second matrix $\mathbf{G}$, we first need to define the sequence $\widetilde{G}$ on $\widetilde{\mathcal{L}}$,

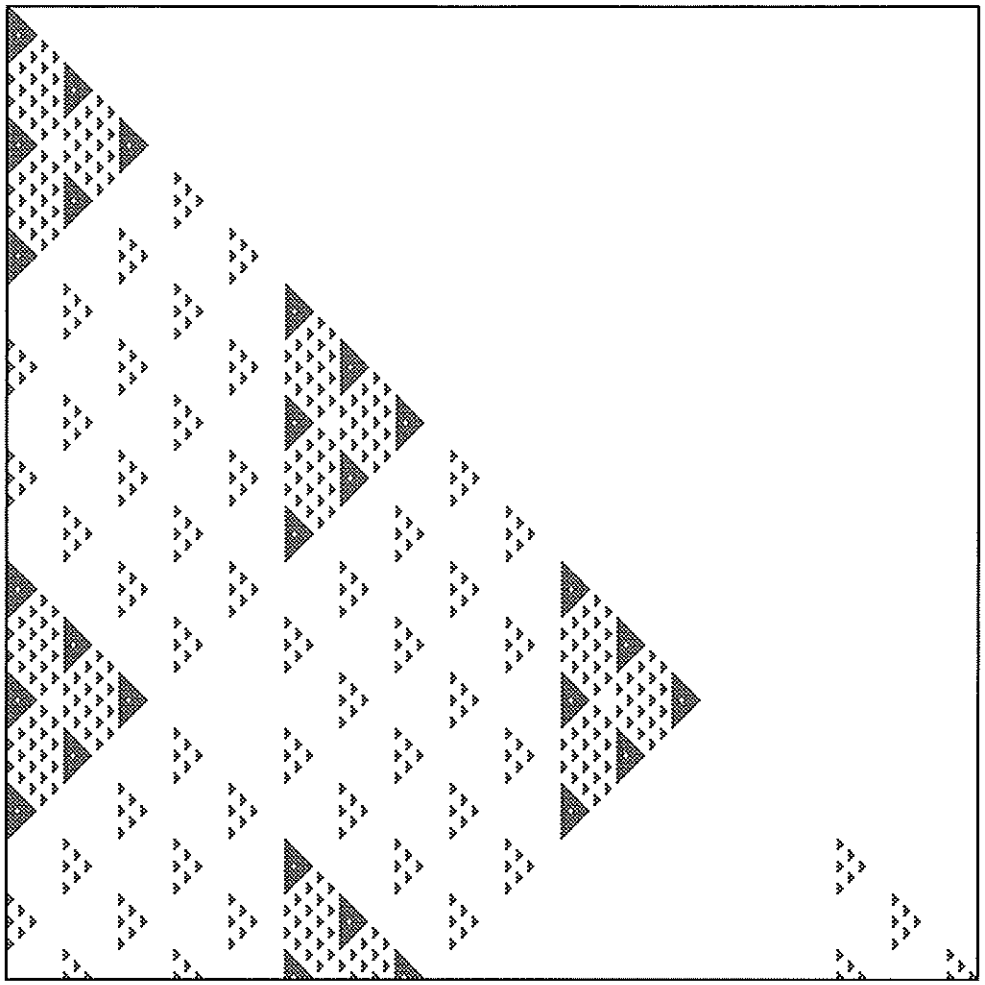

Figure 2: Graphical representation of the Legendre polynomial coefficient matrix modulo 25. White squares correspond to coefficients which are 0 in $\mathbb{Z}_{25}$, black squares to coefficients which are $\neq 0$ in $\mathbb{Z}_{25}$. (Domain: $(k,l) \in [0,437]^2$).

as follows:

$$\widetilde{G}(k,l) = \binom{l}{\frac{l-k}{2}} \text{ for } -l \leq k \leq l,\ (l-k) \text{ even} \tag{9}$$

$$= 0 \text{ for } |k| > l \text{ or } (l-k) \text{ odd} \tag{10}$$

We display the first 9 rows of $\widetilde{G}$:

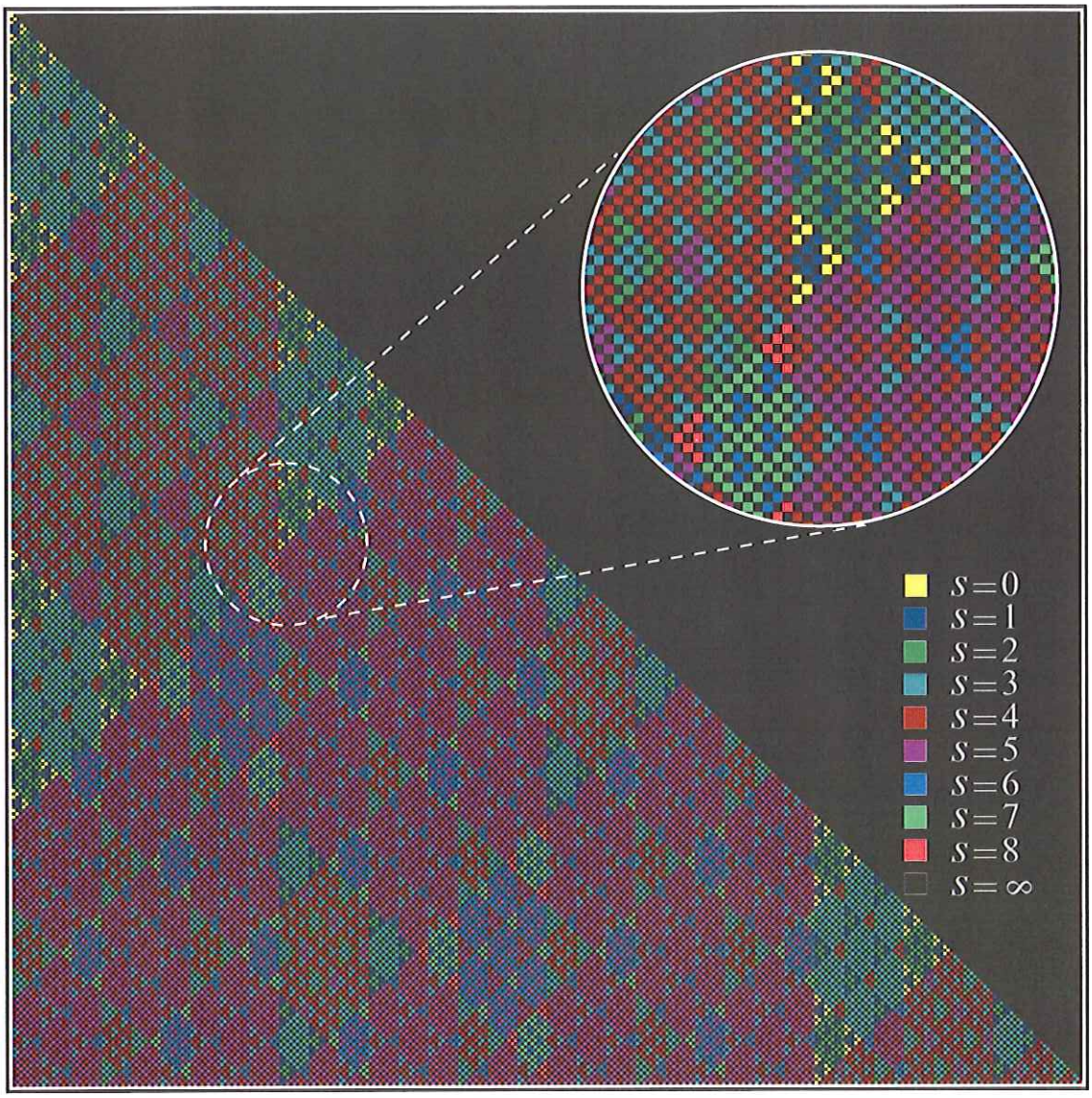

Figure 3: Graphical representation of the 3-adic valuations of the Legendre polynomial coefficient matrix $\mathbf{V} = v_3(\mathbf{P})$ in the domain $(k,l) \in [0,323]^2$. The color at a given position (k,l) corresponds to $s = v_3(\mathbf{P}(k,l))$, as indicated in the color code, meaning that $\mathbf{P}(k,l)$ is divisible by 3^sbut not by 3^{s+1}.

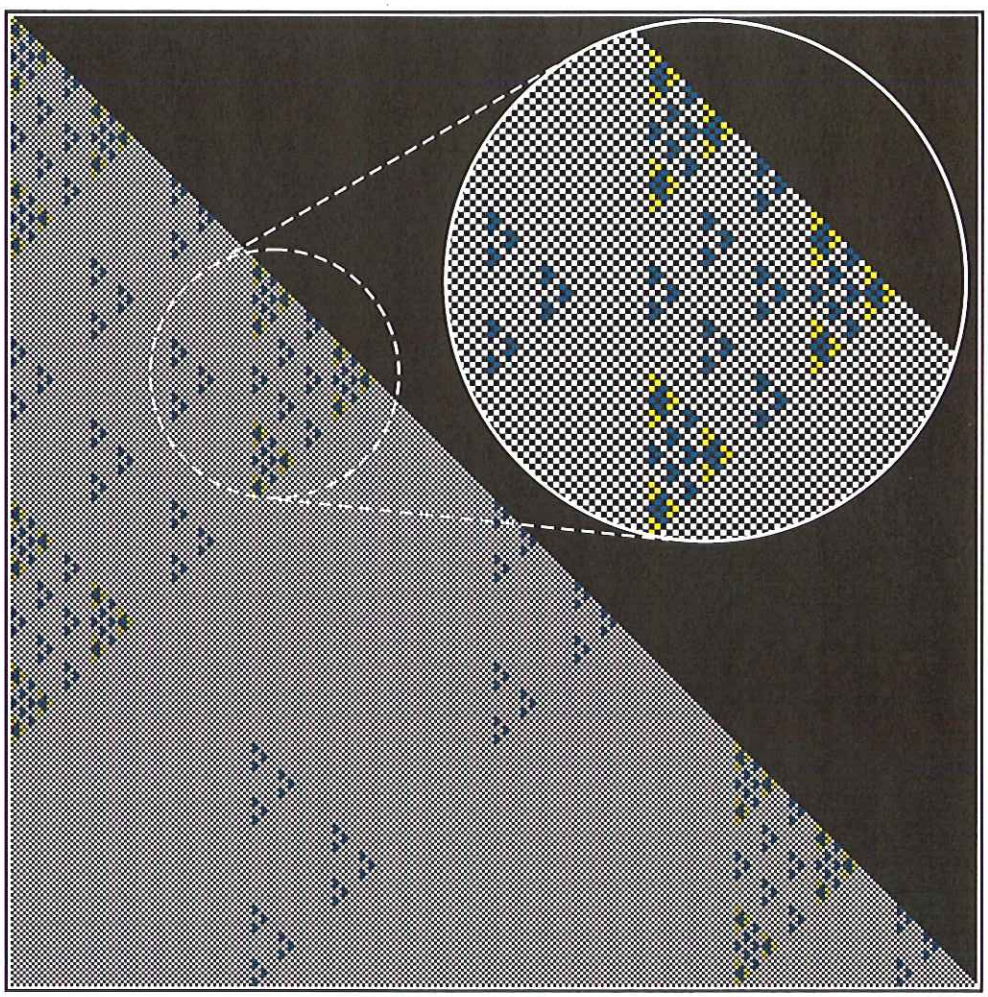

Figure 4: Graphical representation of the 3-adic valuations of the Legendre polynomial coefficient matrix $\mathbf{V}^{(2)}$ where all valuations ≥ 2 are identified and represented by white squares. Yellow corresponds to a 3-adic valuation value of 0, blue to 1, and black to ∞. (Domain $(k, l) \in [0, 323]^2$).

$$
\begin{array}{cccccccccccccccccccc}
 & & & & & & & & & & k & & & & & & & & & \\
 & & & & & & & & & & \rightarrow & & & & & & & & & \\
\cdots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots \\
\cdots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots \\
\cdots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots \\
\cdots & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 3 & 0 & 3 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \cdots \\
\cdots & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 4 & 0 & 6 & 0 & 4 & 0 & 1 & 0 & 0 & 0 & 0 & \cdots \\
\cdots & 0 & 0 & 0 & 0 & 1 & 0 & 5 & 0 & 10 & 0 & 10 & 0 & 5 & 0 & 1 & 0 & 0 & 0 & \cdots \\
\cdots & 0 & 0 & 0 & 1 & 0 & 6 & 0 & 15 & 0 & 20 & 0 & 15 & 0 & 6 & 0 & 1 & 0 & 0 & \cdots \\
\cdots & 0 & 0 & 1 & 0 & 7 & 0 & 21 & 0 & 35 & 0 & 35 & 0 & 21 & 0 & 7 & 0 & 1 & 0 & \cdots \\
\cdots & 0 & 1 & 0 & 8 & 0 & 28 & 0 & 56 & 0 & 70 & 0 & 56 & 0 & 28 & 0 & 8 & 0 & 1 & \cdots \\
\cdots & 1 & 0 & 9 & 0 & 36 & 0 & 84 & 0 & 126 & 0 & 126 & 0 & 84 & 0 & 36 & 0 & 9 & 0 & 1 & \cdots \\
\iddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
\quad \downarrow l \tag{11}
$$

(the 1 on the top row is located at position $(k,l) = (0,0)$).
Observe that the points in $\widehat{\mathcal{L}}$ where $\widetilde{G}(k,l) \neq 0$ form the lattice $\widehat{\mathcal{L}}^*$. In a later stage, we will consider the restriction $\widehat{G}$ of $\widetilde{G}$ on $\widehat{\mathcal{L}}$:

$$\widehat{G}(k,l) = \widetilde{G}(k,l)|_{\widehat{\mathcal{L}}}. \tag{12}$$

Even more important is the restriction of $\widetilde{G}$ to $\mathcal{L}$, yielding the matrix $\mathbf{G}$:

$$\mathbf{G}(k,l) \;=\; \widetilde{G}(k,l),\ (k,l) \in \mathcal{L} \tag{13}$$

(this matrix is formed by the rightmost elements with nonnegative coordinate k in table (11)).

From (3-4), (7) and (9-10-13) it is clear that $\mathbf{L}$ is the elementwise (Hadamard) product (denoted $\odot$) of $\mathbf{B}$ and $\mathbf{G}$:

$$\mathbf{L} = \mathbf{B} \odot \mathbf{G}. \tag{14}$$

As it holds that $v_p(a.b) = v_p(a) + v_p(b)$ for any integers a, b, this product property (14)is transformed into an ordinary sum of matrices for the p-adic valuations:

$$v_p(\mathbf{L}) = v_p(\mathbf{B}) + v_p(\mathbf{G}). \tag{15}$$

The binomial matrix $\mathbf{B}$, and even more its p-adic valuation $v_p(\mathbf{B})$, will play a central role, not only because it appears as such in the product $\mathbf{L} = \mathbf{B} \odot \mathbf{G}$, but also because the nonzero coefficients in $\widetilde{G}$ correspond in a natural way to the elements of $\mathbf{B}$ (and hence $v_p(\mathbf{B})$ also defines $v_p(\mathbf{G})$).

These nonzero coefficients of $\widetilde{G}$ are found on the sublattice $\widehat{\mathcal{L}}^*$. On the lattice $\widehat{\mathcal{L}}$, a new (skew) coordinate system (k^*, l^*) can be defined, where

$$k^* = \frac{k+l}{2},\ l^* = \frac{l-k}{2} \qquad (\text{or } l = k^* + l^*, k = k^* - l^*) \tag{16}$$

(see Fig. 1). Then we find, for $\widetilde{G}(k,l)$ on $\widehat{\mathcal{L}}^*$:

$$\widetilde{G}(k,l) = \binom{l}{\frac{l-k}{2}} = \binom{l^*+k^*}{l^*} = \mathbf{B}(k^*, l^*). \tag{17}$$

From here on, it will be more convenient to use shorthand notations for the p-adic valuations of $\mathbf{L}, \mathbf{B}, \mathbf{G}$:

$$\mathbf{V} = v_p(\mathbf{L}) \tag{18}$$
$$\mathbf{K} = v_p(\mathbf{B}) \tag{19}$$
$$\mathbf{R} = v_p(\mathbf{G}). \tag{20}$$

Hereby, even the prime p is no longer indicated: either the expressions in which $\mathbf{K}$ or $\mathbf{R}$ appear hold for any p, or any specific value of p will be explicitly mentioned in the context. Hence, we write (15) as

$$\mathbf{V} = \mathbf{K} + \mathbf{R}. \tag{21}$$

For example, for $p = 3$, one finds by taking the 3-adic valuations of the first 9×9 elements of $\mathbf{B}$, the logzise-2 part of $\mathbf{K}$

$$\mathbf{K}_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 2 & 1 & 1 & 2 \\ 0 & 1 & 1 & 0 & 2 & 2 & 1 & 2 & 2 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 & 1 & 2 & 1 & 1 & 2 \\ 0 & 2 & 2 & 1 & 2 & 2 & 1 & 2 & 2 \end{bmatrix}. \tag{22}$$

Our aim is first to derive a substitution for $\mathbf{K}$, i.e., a procedure which systematically grows $\mathbf{K}_{m+1}$ from $\mathbf{K}_m$, by replacing elements in $\mathbf{K}_m$ with a set of elements. Actually, as will be shown in Sec. 2, we will find a substitution which, in the example above for $p = 3$, replaces elementary 3×3-blocks by 3×3 blocks of size 3×3 (for arbitrary p, this will be a replacement of an elementary $p \times p$ block by $p \times p$ elementary blocks). In a second step, see Sec. 3, it will be shown how the substitution on $\mathbf{K}$ induces a substitution on $\mathbf{R}$. Section 4 constructs the substitution on $\mathbf{V}$ by combining the substitutions for $\mathbf{K}$ and $\mathbf{R}$ in a kind of substitution sum.

We should mention that the fractal structure of the graphical representation of the sequence $(\binom{n+k}{k} \bmod p^s)_{(n,k)\in\mathbb{N}^2} = \mathbf{B} \bmod p^s$ for p being a prime, and where entries in this sequence which are 0 are represented by a white square and the entries different from 0 are represented by a black square, has been deciphered in von Haeseler *et al.*[15] in the form of a so-called Hierarchical Iterated Functions Systems (HIFS). The main point there is the interpretation of Kummer's result (see below, Theorem 2.1) as a HIFS (see Peitgen *et al.*[16], Ch. 5, Ch. 8). The result from the next section, which provides a substitution for $\mathbf{K} = v_p(\mathbf{B})$, and which also exploits Kummer's result, is of another nature and also broader in scope.

The results and the proofs of this paper are in the spirit of so-called "Visible Structures in Number Theory", see Borwein and Jorgensen[17].

2 The substitution generating the valuation matrix K

We will first show how to generate $\mathbf{K}_{m+1}$ from $\mathbf{K}_m$. Then the substitution will be derived.

Use will be made of

Theorem 2.1 *(Kummer's Result, see Peitgen* et al.[16]*, p. 429).*
The p-adic valuation $v_p(\binom{k+l}{k})$ equals the number of carries in the p-adic addition of the p-adic representations of k and l.

2.1 A recursion for $\mathbf{K}_m$

We will need the following special matrices.
$\mathbf{O}_m = p^m \times p^m$-matrix whose elements are all 0.
$\mathbf{D}_m = p^m \times p^m$-matrix whose elements *on and above* the skew diagonal are all 0, and the elements below the skew diagonal are all 1.
$\mathbf{I}_m = p^m \times p^m$-matrix whose elements are all 1.

Also, it will be convenient to introduce the *bigsum* operation $\oplus$. Let $\mathbf{A}_{m+k}$ and $\mathbf{B}_m$ denote two matrices of logsize $m+k$ and m respectively, where $k \geq 0$. Then $\mathbf{A}_{m+k}$ can be partitioned in $p^k \times p^k$ blocks of logsize m, as follows (coordinates of blocks will be given as superscripts):

$$\mathbf{A}_{m+k} = \begin{bmatrix} \mathbf{A}_m^{(0,0)} & \cdots & \mathbf{A}_m^{(p^k-1,0)} \\ \vdots & \ddots & \vdots \\ \mathbf{A}_m^{(0,p^k-1)} & \cdots & \mathbf{A}_m^{(p^k-1,p^k-1)} \end{bmatrix} \tag{23}$$

Then define the bigsum operation of $\mathbf{A}_{m+k}$ and $\mathbf{B}_m$ as

$$\mathbf{A}_{m+k} \oplus \mathbf{B}_m = \begin{bmatrix} \mathbf{A}_m^{(0,0)} + \mathbf{B}_m & \cdots & \mathbf{A}_m^{(p^k-1,0)} + \mathbf{B}_m \\ \vdots & \ddots & \vdots \\ \mathbf{A}_m^{(0,p^k-1)} + \mathbf{B}_m & \cdots & \mathbf{A}_m^{(p^k-1,p^k-1)} + \mathbf{B}_m \end{bmatrix}. \tag{24}$$

When $k = 0$, it is clear that $\mathbf{A}_m \oplus \mathbf{B}_m = \mathbf{A}_m + \mathbf{B}_m$.

Notice that the bigsum operation is associative, i.e. with $l \geq k \geq 0$, it holds that $\mathbf{A}_{m+l} \oplus (\mathbf{B}_{m+k} \oplus \mathbf{C}_m) = (\mathbf{A}_{m+l} \oplus \mathbf{B}_{m+k}) \oplus \mathbf{C}_m = \mathbf{A}_{m+l} \oplus \mathbf{B}_{m+k} \oplus \mathbf{C}_m$. Although not quite the same, this bigsum operation shows similarities with the bigsum used in Barbé[18] and which is an additive counterpart of the Kronecker product.

Furthermore, many matrices will have a particular Hankel form, and it is convenient to represent this in a symbolic way. With $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ matrices of the same size, we denote by $[\mathbf{A}, \mathbf{B}, \mathbf{C}]$ the following block Hankel matrix consisting of $p \times p$ blocks:

$$[\mathbf{A}, \mathbf{B}, \mathbf{C}]_p = \begin{bmatrix} \mathbf{A} & \mathbf{A} & \cdots & \mathbf{A} & \mathbf{A} & \mathbf{B} \\ \mathbf{A} & \mathbf{A} & \cdots & \mathbf{A} & \mathbf{B} & \mathbf{C} \\ \mathbf{A} & \mathbf{A} & \cdots & \mathbf{B} & \mathbf{C} & \mathbf{C} \\ \vdots & \vdots & & & \vdots & \\ \mathbf{A} & \mathbf{B} & \cdots & \mathbf{C} & \mathbf{C} & \mathbf{C} \\ \mathbf{B} & \mathbf{C} & \cdots & \mathbf{C} & \mathbf{C} & \mathbf{C} \end{bmatrix}. \tag{25}$$

Mostly the odd-prime subscript p will be deleted as, although being arbitrary, it is constant within the context, and the formulas are generic. Sometimes, matrix (25) will also be symbolized by

$$\begin{bmatrix} \mathbf{A} & \rightarrow & \mathbf{B} \\ \downarrow & \nearrow & \uparrow \\ \mathbf{B} & \leftarrow & \mathbf{C} \end{bmatrix}. \tag{26}$$

Theorem 2.2 $\mathbf{K}_{m+1}$ *can be obtained from* $\mathbf{K}_m$ *as follows*

$$\mathbf{K}_{m+1} = [\mathbf{O}_m, \mathbf{D}_m, \mathbf{I}_m] \oplus \mathbf{K}_m \tag{27}$$
$$= [\mathbf{O}_m \oplus \mathbf{K}_m, \mathbf{D}_m \oplus \mathbf{K}_m, \mathbf{I}_m \oplus \mathbf{K}_m]. \tag{28}$$

The proof will be postponed for a while, as we first need to consider an auxiliary matrix $\mathbf{U}_m$.

$\mathbf{U}_m$ is the matrix of size $p^m \times p^m$ where element $\mathbf{U}_m(k,l)$ displays the p-adic representation of k and l with m digits (there may be leading 0's), respectively denoted

$$k_{(p),m} = (k_{m-1} \dots k_0)_p \tag{29}$$
$$l_{(p),m} = (l_{m-1} \dots l_0)_p, \tag{30}$$

as follows

$$\mathbf{U}_m(k,l) = \left\langle \begin{array}{c} k_{(p),m} \\ l_{(p),m} \end{array} \right\rangle. \tag{31}$$

Let $\left\langle \begin{array}{c} \alpha \\ \beta \end{array} \right\rangle \mathbf{U}_m$, $\alpha, \beta \in [p]$ denote the matrix obtained from $\mathbf{U}_m$ by augmenting all the p-adic representations $\left\langle \begin{array}{c} k_{m-1} \dots k_0 \\ l_{m-1} \dots l_0 \end{array} \right\rangle$ which appear as elements in $\mathbf{U}_m$ with one extra leading digit pair $\left\langle \begin{array}{c} \alpha \\ \beta \end{array} \right\rangle$, i.e.,

$$\left\langle \begin{array}{c} \alpha \\ \beta \end{array} \right\rangle \mathbf{U}_m = \left[\left\langle \begin{array}{c} \alpha k_{m-1} \dots k_0 \\ \beta l_{m-1} \dots l_0 \end{array} \right\rangle \right]_{(k,l) \in [p^{m-1}]}. \tag{32}$$

Then we can write

$$\mathbf{U}_{m+1} = \begin{bmatrix} \left\langle \begin{array}{c} 0 \\ 0 \end{array} \right\rangle \mathbf{U}_m & \left\langle \begin{array}{c} 1 \\ 0 \end{array} \right\rangle \mathbf{U}_m & \cdots & \left\langle \begin{array}{c} p-2 \\ 0 \end{array} \right\rangle \mathbf{U}_m & \left\langle \begin{array}{c} p-1 \\ 0 \end{array} \right\rangle \mathbf{U}_m \\ \left\langle \begin{array}{c} 0 \\ 1 \end{array} \right\rangle \mathbf{U}_m & \left\langle \begin{array}{c} 1 \\ 1 \end{array} \right\rangle \mathbf{U}_m & \cdots & \left\langle \begin{array}{c} p-2 \\ 1 \end{array} \right\rangle \mathbf{U}_m & \left\langle \begin{array}{c} p-1 \\ 1 \end{array} \right\rangle \mathbf{U}_m \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \left\langle \begin{array}{c} 0 \\ p-1 \end{array} \right\rangle \mathbf{U}_m & \left\langle \begin{array}{c} 1 \\ p-1 \end{array} \right\rangle \mathbf{U}_m & \cdots & \left\langle \begin{array}{c} p-2 \\ p-1 \end{array} \right\rangle \mathbf{U}_m & \left\langle \begin{array}{c} p-1 \\ p-1 \end{array} \right\rangle \mathbf{U}_m \end{bmatrix}. \tag{33}$$

Now consider the p-adic addition $k_{(p),m} + l_{(p),m}$ in element $\mathbf{U}_m(k,l)$. If no carry is generated in the addition at the leftmost digit pair $\left\langle \begin{array}{c} k_{m-1} \\ l_{m-1} \end{array} \right\rangle$ (taking into account possible carries on the non-leading digit pairs) , then the element is said to be of *type* 0, otherwise it is of *type* 1(notice that, when adding two p-adic numbers, the maximal carry that can be generated at any position is 1). It is clear that for

$$\mathbf{U}_1 = \begin{bmatrix} \left\langle \begin{array}{c} 0 \\ 0 \end{array} \right\rangle & \left\langle \begin{array}{c} 1 \\ 0 \end{array} \right\rangle & \cdots & \left\langle \begin{array}{c} p-2 \\ 0 \end{array} \right\rangle & \left\langle \begin{array}{c} p-1 \\ 0 \end{array} \right\rangle \\ \left\langle \begin{array}{c} 0 \\ 1 \end{array} \right\rangle & \left\langle \begin{array}{c} 1 \\ 1 \end{array} \right\rangle & \cdots & \left\langle \begin{array}{c} p-2 \\ 1 \end{array} \right\rangle & \left\langle \begin{array}{c} p-1 \\ 1 \end{array} \right\rangle \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \left\langle \begin{array}{c} 0 \\ p-1 \end{array} \right\rangle & \left\langle \begin{array}{c} 1 \\ p-1 \end{array} \right\rangle & \cdots & \left\langle \begin{array}{c} p-2 \\ p-1 \end{array} \right\rangle & \left\langle \begin{array}{c} p-1 \\ p-1 \end{array} \right\rangle \end{bmatrix}; \tag{34}$$

all elements in $\mathbf{U}_1$ on and above the skew diagonal are of type 0, the ones below the skew diagonal are of type 1. We say that $\mathbf{U}_1$ has the **split-property**.

Lemma 2.3 *All* $\mathbf{U}_m$ *have the split property.*

Proof. By induction. We show that when $\mathbf{U}_m$ has the split property, then so does $\mathbf{U}_{m+1}$. Referring to (33), we have to consider three cases.

1. The blocks $\left\langle \begin{smallmatrix} \alpha \\ \beta \end{smallmatrix} \right\rangle \mathbf{U}_m$ above the skew diagonal blocks. These have $\alpha+\beta \leq p-2$. As the maximal leftmost carry in any element of $\mathbf{U}_m$ is 1, the maximal leftmost carry in the elements of $\left\langle \begin{smallmatrix} \alpha \\ \beta \end{smallmatrix} \right\rangle \mathbf{U}_m$ is $\alpha+\beta+1$, which is $\leq p-1$. This means that no leftmost carry is generated in the elements of these blocks. Hence all elements in $\mathbf{U}_{m+1}$ above the skew diagonal are of type 0.

2. The blocks $\left\langle \begin{smallmatrix} \alpha \\ \beta \end{smallmatrix} \right\rangle \mathbf{U}_m$ below the skew diagonal blocks have $\alpha+\beta \geq p$. This means that a leftmost carry is generated for all elements in these blocks, hence these elements are of type 1.

3. The blocks $\left\langle \begin{smallmatrix} \alpha \\ \beta \end{smallmatrix} \right\rangle \mathbf{U}_m$ on the skew diagonal blocks have $\alpha+\beta = p-1$. This means that a leftmost carry will be generated for those elements in $\left\langle \begin{smallmatrix} \alpha \\ \beta \end{smallmatrix} \right\rangle \mathbf{U}_m$ which have a leftmost carry in $\mathbf{U}_m$. These are the ones below the diagonal in $\mathbf{U}_m$ (under the assumption that $\mathbf{U}_m$ has the split property). For the elements in $\left\langle \begin{smallmatrix} \alpha \\ \beta \end{smallmatrix} \right\rangle \mathbf{U}_m$ on and above the skew diagonal, no carry is generated in the leftmost position.

Combining items 1,2 and 3 shows that all elements in $\mathbf{U}_{m+1}$ on and above the skew diagonal are of type 0 and all elements below the diagonal are of type 1. Hence , when $\mathbf{U}_m$ has the split property, also $\mathbf{U}_{m+1}$ has the split property. And as $\mathbf{U}_1$ has the split property, the lemma is proven.

■

Proof of Theorem 2.2

Let $c\left(\left\langle \begin{smallmatrix} k_{(p),m} \\ l_{(p),m} \end{smallmatrix} \right\rangle\right)$ denote the number of carries in the p-adic addition $k_{(p),m}+l_{(p),m}$. By extension, $c(\mathbf{U}_m)$ and $c\left(\left\langle \begin{smallmatrix} \alpha \\ \beta \end{smallmatrix} \right\rangle \mathbf{U}_m\right)$ are matrices whose elements are the number of carries in the corresponding elements of $\mathbf{U}_m$ and $\left\langle \begin{smallmatrix} \alpha \\ \beta \end{smallmatrix} \right\rangle \mathbf{U}_m$. Then it is clear by Kummer's Theorem, that

$$\mathbf{K}_m = c(\mathbf{U}_m), \tag{35}$$

and, with $\mathbf{M}_m^{(\alpha,\beta)} = c\left(\left\langle \begin{smallmatrix} \alpha \\ \beta \end{smallmatrix} \right\rangle \mathbf{U}_m\right)$, it follows from (33) that

$$\mathbf{K}_{m+1} = \begin{bmatrix} \mathbf{M}_m^{(0,0)} & \mathbf{M}_m^{(1,0)} & \cdots & \mathbf{M}_m^{(p-1,0)} \\ \mathbf{M}_m^{(0,1)} & \mathbf{M}_m^{(1,1)} & \cdots & \mathbf{M}_m^{(p-1,1)} \\ \vdots & \vdots & & \vdots \\ \mathbf{M}_m^{(0,p-1)} & \mathbf{M}_m^{(1,p-1)} & \cdots & \mathbf{M}_m^{(p-1,p-1)} \end{bmatrix}. \tag{36}$$

We show that it is possible to derive $\mathbf{M}_m^{(\alpha,\beta)} = c\left(\left\langle \begin{smallmatrix} \alpha \\ \beta \end{smallmatrix} \right\rangle \mathbf{U}_m\right)$ when we know $c(\mathbf{U}_m) = \mathbf{K}_m$. Three cases have to be considered.

1. $\mathbf{M}_m^{(\alpha,\beta)}$ is a block above the skew diagonal blocks in (36), i.e., $\alpha+\beta \leq p-2$. Then, as the leading carry in the elements of $\mathbf{U}_m$ is maximally 1, no extra leading carry is generated in any element of $\left\langle \begin{smallmatrix} \alpha \\ \beta \end{smallmatrix} \right\rangle \mathbf{U}_m$. This means that

$$\mathbf{M}_m^{(\alpha,\beta)} = c\left(\left\langle \begin{smallmatrix} \alpha \\ \beta \end{smallmatrix} \right\rangle \mathbf{U}_m\right) = c(\mathbf{U}_m) = \mathbf{K}_m = \mathbf{O}_m + \mathbf{K}_m. \tag{37}$$

2. $\mathbf{M}_m^{(\alpha,\beta)}$ is a block below the skew diagonal blocks in (36), i.e., $\alpha+\beta \geq p$. This means that $c\left(\left\langle \begin{smallmatrix} \alpha \\ \beta \end{smallmatrix} \right\rangle \mathbf{U}_m\right) = \mathbf{I}_m + c(\mathbf{U}_m)$, or

$$\mathbf{M}_m^{(\alpha,\beta)} = \mathbf{I}_m + \mathbf{K}_m. \tag{38}$$

3. $\mathbf{M}_m^{(\alpha,\beta)}$ is a block on the skew diagonal in (36), i.e., $\alpha+\beta \leq p-1$. Then, because of the split-property of $\mathbf{U}_m$,it holds that $c\left(\left\langle \begin{smallmatrix} \alpha \\ \beta \end{smallmatrix} \right\rangle \mathbf{U}_m(k,l)\right) = 1 + c(\mathbf{U}_m(k,l))$ for those elements $\mathbf{U}_m(k,l)$ which are of type 1, i.e. elements of $\mathbf{U}_m$ below the skew diagonal of $\mathbf{U}_m$ (i.e.,$k+l \geq p^m$). Otherwise $c\left(\left\langle \begin{smallmatrix} \alpha \\ \beta \end{smallmatrix} \right\rangle \mathbf{U}_m(k,l)\right) = c(\mathbf{U}_m(k,l))$. This yields

$$\mathbf{M}_m^{(\alpha,\beta)} = \mathbf{D}_m + \mathbf{K}_m. \tag{39}$$

Combining items 1,2 and 3 proves the theorem.

■

2.2 A block matrix substitution for K

2.2.1 Block matrix substitution

In this section, we define a block matrix substitution, which is an extension of a two-dimensional matrix substitution (Barbé[18]) or matrix-valued morphism (Allouche and Shallit[13], Ch. 14).

Consider a matrix $\mathbf{Q}_m$. This matrix can be partitioned in $p^{m-1} \times p^{m-1}$ blocks of size $p \times p$. These logsize-1 blocks are called *elementary block symbols*(or *elementary blocks*). A block substitution replaces each elementary block in $\mathbf{Q}_m$ by $p \times p$ elementary blocks, thus forming an enlarged matrix $\mathbf{Q}_{m+1}$. Hereby, it is essential that elementary blocks which are the same but appear at different places in $\mathbf{Q}_m$, are replaced by the same set of $p \times p$ elementary blocks. In a next step, each elementary block in $\mathbf{Q}_{m+1}$ is again replaced by $p \times p$ elementary blocks. In that way it is possible, when starting from an initial matrix $\mathbf{Q}_1$ which contains a single elementary block, to generate the sequence of growing matrices $\mathbf{Q}_1, \mathbf{Q}_2, \mathbf{Q}_3, \ldots$. Let $\mathcal{S}_\mathbf{Q}$ denote the set of all elementary blocks (may be finite or infinite), then a matrix block substitution is completely defined by determining how each elementary block $\mathcal{S}$ has to be replaced by $p \times p$ elementary blocks, and by fixing the initial elementary block. I.e., one needs to specify the tuple $(\sigma, \mathbf{Q}_1)$, where $\sigma_\mathbf{Q}$ defines the substitution map

$$\sigma_\mathbf{Q} : \mathcal{S}_\mathbf{Q} \to \mathcal{S}_\mathbf{Q}^{p\times p} : \sigma_\mathbf{Q}(\mathbf{S}) = \begin{matrix} \mathbf{S}^{(0,0)} & \mathbf{S}^{(1,0)} & \ldots \mathbf{S}^{(p-2,0)} & \mathbf{S}^{(p-1,0)} \\ \mathbf{S}^{(0,1)} & \mathbf{S}^{(1,1)} & \ldots \mathbf{S}^{(p-2,1)} & \mathbf{S}^{(p-1,1)} \\ \vdots & \vdots & \ldots \vdots & \vdots \\ \mathbf{S}^{(0,p-1)} & \mathbf{S}^{(1,p-1)} & \ldots \mathbf{S}^{(p-2,p-1)} & \mathbf{S}^{(p-1,p-1)} \end{matrix} \tag{40}$$

and $\mathbf{Q}_1 \in \mathcal{S}_\mathbf{Q}$ is the initial elementary block. One additional condition has to be added: $\sigma_\mathbf{Q}(\mathbf{Q}_1)$ has $\mathbf{Q}_1$ itself as its top-left elementary block (i,e, when $\mathbf{S} = \mathbf{Q}_1$, then $\mathbf{S}^{(0,0)} = \mathbf{Q}_1$). This implies that $\mathbf{Q}_m$ always appears as top-left part of $\mathbf{Q}_{m+1}$, which actually makes the substitution "grow" a bi-infinite matrix $\mathbf{Q}$ by an iterative expansion of $\mathbf{Q}_m$ to $\mathbf{Q}_{m+1}$ to the right and below, keeping $\mathbf{Q}_m$ at the top left.

2.2.2 Defining the substitution that generates $\mathbf{K}_m$

Theorem 2.4 *The substitution generating* $\mathbf{K}_m = v_p(\mathbf{B}_m)$ *is* $(\sigma_\mathbf{K}, \mathbf{K}_1)$, *with* $\mathbf{K}_1 = [0,0,1]$. *All elementary block symbols are of the type* $[a,a,b] = \begin{bmatrix} a & \rightarrow & a \\ \downarrow & \nearrow & \uparrow \\ a & \leftarrow & b \end{bmatrix}$, (a,b) *in some subset of* $\mathbb{N}^2$ *and the substitution map* $\sigma_\mathbf{K}$ *is defined by*

$$\sigma_K([a,a,b]) = [[a,a,a+1],[a,a,b+1],[b,b,b+1]] = \begin{bmatrix} [a,a,b] & \rightarrow & [a,a,b+1] \\ \downarrow & \nearrow & \uparrow \\ [a,a,b+1] & \leftarrow & [b,b,b+1] \end{bmatrix}. \quad (41)$$

Proof: Let

$$\mathbf{Z}_{m+1} = [\mathbf{O}_m, \mathbf{D}_m, \mathbf{I}_m]. \quad (42)$$

Theorem 2.2 then states that

$$\mathbf{K}_{m+1} = \mathbf{Z}_{m+1} \oplus \mathbf{K}_m. \quad (43)$$

Iterating this expression, starting from $\mathbf{K}_1$, gives

$$\mathbf{K}_m = \underbrace{\mathbf{Z}_m \oplus \mathbf{Z}_{m-1} \oplus \ldots \mathbf{Z}_{l+1}}_{\mathbf{W}_{m,l}} \oplus \underbrace{\mathbf{Z}_l \oplus \ldots \oplus \mathbf{Z}_2 \oplus \mathbf{K}_1}_{\mathbf{K}_l}. \quad (44)$$

We will now establish an isomorphism between the expressions

$$\begin{aligned} \mathbf{K}_m &= \mathbf{W}_{m,1} \oplus \mathbf{K}_1 && (45) \\ \text{with} \quad \mathbf{W}_{m,1} &= \mathbf{Z}_m \oplus \mathbf{Z}_{m-1} \oplus \ldots \oplus \mathbf{Z}_1 && (46) \end{aligned}$$

and

$$\begin{aligned} \mathbf{K}_{m+1} &= \mathbf{W}_{m+1,2} \oplus \mathbf{K}_2 && (47) \\ \text{with} \quad \mathbf{W}_{m+1,2} &= \mathbf{Z}_{m+1} \oplus \mathbf{Z}_m \oplus \ldots \oplus \mathbf{Z}_2. && (48) \end{aligned}$$

■

Observe that $\mathbf{Z}_m = \mathbf{D}_m$. By consequence, it follows from (42) that

$$\begin{array}{rcccl} \mathbf{O}_m + \mathbf{Z}_m & = & \mathbf{D}_m & = & [\mathbf{O}_{m-1}, \mathbf{D}_{m-1}, \mathbf{I}_{m-1}] \\ \mathbf{D}_m + \mathbf{Z}_m & = & 2\mathbf{D}_m & = & [\mathbf{O}_{m-1}, 2\mathbf{D}_{m-1}, 2\mathbf{I}_{m-1}] \\ \mathbf{I}_m + \mathbf{Z}_m & = & \mathbf{I}_m + \mathbf{D}_m & = & [\mathbf{I}_{m-1}, \mathbf{I}_{m-1} + \mathbf{D}_{m-1}, 2\mathbf{I}_{m-1}], \end{array} \quad (49)$$

and also

$$\mathbf{Z}_m + \mathbf{Z}_{m-1} = [[\mathbf{O}_{m-1}, \mathbf{D}_{m-1}, \mathbf{I}_{m-1}], [\mathbf{O}_{m-1}, 2\mathbf{D}_{m-1}, 2\mathbf{I}_{m-1}], [\mathbf{I}_{m-1}, \mathbf{I}_{m-1} + \mathbf{D}_{m-1}, 2\mathbf{I}_{m-1}]]. \quad (50)$$

Reiterating this in (46) shows that the elementary logsize-1 blocks in $\mathbf{W}_{m,1}$ are all of the form

$$\mathbf{O}_1 + x\mathbf{D}_1 + y\mathbf{I}_1, \ , x, y \in \mathbb{N} \quad (51)$$

and, from (45), that the corresponding elementary logsize-1 blocks in $\mathbf{K}_m$ are of the form

$$\mathbf{O}_1 + x\mathbf{D}_1 + y\mathbf{I}_1 + \mathbf{K}_1. \tag{52}$$

In a similar way, considering (47)and(48), it follows that all logsize-2 blocks in $\mathbf{K}_{m+1}$ are of the form

$$\mathbf{O}_1 + x\mathbf{D}_1 + y\mathbf{I}_1 + \mathbf{K}_2. \tag{53}$$

I.e., an isomorphism is established between the elementary logsize-1 blocks in $\mathbf{K}_m$ and the logsize-2 blocks in $\mathbf{K}_{m+1}$. Whenever there is a logsize-1 block of the particular form $\mathbf{O}_1 + \alpha\mathbf{D}_1 + \beta\mathbf{I}_1 + K_1$ at some logsize-1 block position in $\mathbf{K}_m$, there is a logsize-2 block of the particular form $\mathbf{O}_2 + \alpha\mathbf{D}_2 + \beta\mathbf{I}_2 + \mathbf{K}_2$ at the corresponding logsize-2 block position in $\mathbf{K}_{m+2}$. This means that, in going from $\mathbf{K}_m$ to $\mathbf{K}_{m+1}$, each elementary block in $\mathbf{K}_m$ of the form $\mathbf{O}_1 + \alpha\mathbf{D}_1 + \beta\mathbf{I}_1 + \mathbf{K}_1$, is replaced by a logsize-2 block of the form $\mathbf{O}_2 + \alpha\mathbf{D}_2 + \beta\mathbf{I}_2 + \mathbf{K}_2$. Working out this relationship more explicitly gives the following. With $\mathbf{K}_1 = [0,0,1]$ (from (34)), $\mathbf{O}_1 = [0,0,0]$, $\mathbf{D}_1 = [0,0,1]$, $\mathbf{I}_1 = [1,1,1]$, it follows that the elementary blocks in $\mathbf{K}_m$ are of the form

$$\mathbf{O}_1 + \alpha\mathbf{D}_1 + \beta\mathbf{I}_1 + K_1 = [\beta, \beta, \alpha + \beta + 1]. \tag{54}$$

This shows that the elementary blocks in $\mathbf{K}_m$ are of type $[a, a, b]$ (whatever m). This block is then replaced in $\mathbf{K}_{m+1}$ by the block $\mathbf{O}_2 + \alpha\mathbf{D}_2 + \beta\mathbf{I}_2 + \mathbf{K}_2$. With

$$\mathbf{K}_2 \overset{(43)}{=} [[0,0,1],[0,0,2],[1,1,2]], \tag{55}$$

and using (49), one gets the following expression which readily shows the logsize-1 partitioning of the logsize-2 blocks in $\mathbf{K}_{m+1}$:

$$\mathbf{O}_2 + \alpha\mathbf{D}_2 + \beta\mathbf{I}_2 + K_2 = [[\beta,\beta,\beta+1],[\beta,\beta,\alpha+\beta+2],[\alpha+\beta+1,\alpha+\beta+1,\alpha+\beta+2]]. \tag{56}$$

As this holds for any $m \geq 1$ and any $\alpha, \beta \in \mathbb{N}$, the isomorphism established above and made explicit in (54) and (56) induces the general block substitution function σ through which $\mathbf{K}_{m+1}$ is generated from $\mathbf{K}_m$:

$$\sigma : [\beta,\beta,\alpha+\beta+1] \mapsto [[\beta,\beta,\beta+1],[\beta,\beta,\alpha+\beta+2],[\alpha+\beta+1,\alpha+\beta+1,\alpha+\beta+2]]. \tag{57}$$

Introducing a change of variables: $\beta \to a$ and $\alpha + \beta + 1 \to b$, this transforms into the form given in the theorem.

■

Figure 5 displays $\mathbf{K}_4$, $p = 3$.

From Theorem 2.4, it follows that each substitution step which brings $\mathbf{K}_m$ to $\mathbf{K}_{m+1}$ creates new elementary block symbols.

Notice that the elements of $\mathbf{K}_m$ range from 0 to m. Concerning the number of distinct elementary blocks in $\mathbf{K}_m$ it is easy to prove, by induction, the following

Lemma 2.5 *In $\mathbf{K}_m$, the set of distinct elementary block symbols is*

$$\mathcal{S}_{\mathbf{K},m} = \{[a,a,b] | a \in \{0,1,\ldots,m-1\}, b \in \{1,2,\ldots,m\}, a < b\}. \tag{58}$$

The cardinality of this set is $\frac{m(m+1)}{2}$.

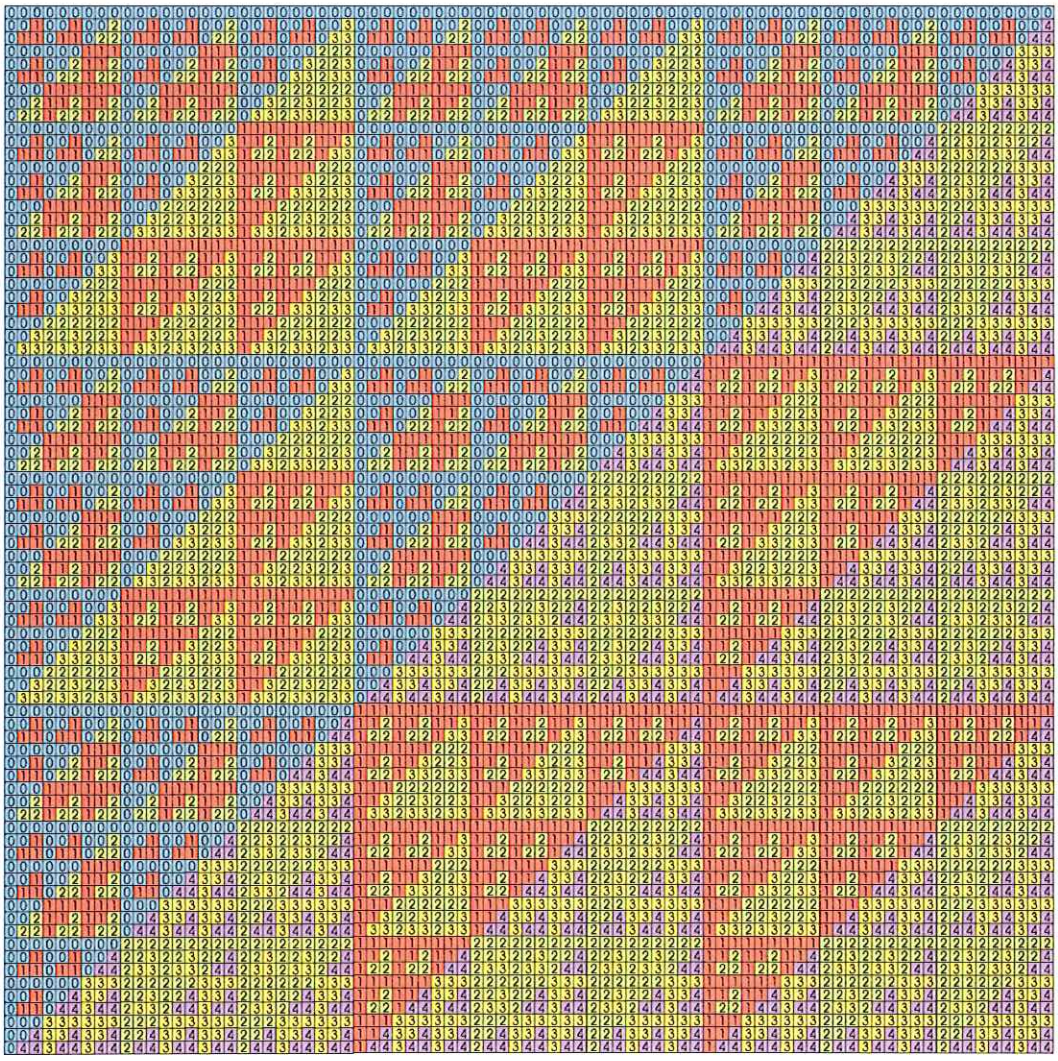

Figure 5: The $\mathbf{K}_4$-matrix for $p = 3$: numbers as well as graphical representation, where each element of $\mathbf{K}_4$ is represented by a colored square. The colors are in bijection with the numbers. The $\begin{bmatrix} \mathbf{A} & \rightarrow & \mathbf{B} \\ \downarrow & \nearrow & \uparrow \\ \mathbf{B} & \leftarrow & \mathbf{C} \end{bmatrix}$-structure on all $\mathbf{K}_m$, $m = 1, 2, 3, \ldots$ is visually clear.

This is represented in Fig. 6.

Thus the number of symbols involved in the substitution generating $\mathbf{K}$ is unbounded. This is no longer the case when we consider the so-called *s-reduction* of $\mathbf{K}$. This is defined for some integer $s \geq 1$, by

$$\mathbf{K}^{(s)}(k,l) = \mathbf{K}(k,l) \text{ if } \mathbf{K}(k,l) < s \tag{59}$$

$$= \overline{s} \text{ if } \mathbf{K}(k,l) \geq s, \tag{60}$$

where $\overline{s}$ is a symbol meaning "larger or equal then s" (and actually referring to elements in the binomial matrix $\mathbf{B}$ which are divisible by p^t, $t \geq s$. So it is meaningful to state $a < \overline{s}$, meaning that $a \in \{0, 1, \ldots, s-1\}$. Also $\overline{s} + n = \overline{s}$ for any $n \in \mathbb{N}$.

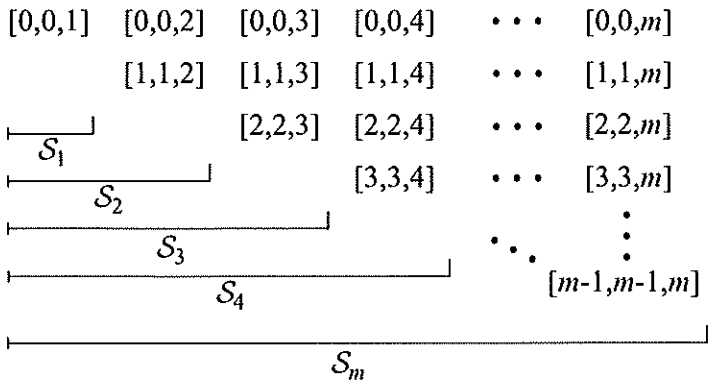

Figure 6: The structure in the sequence of symbol sets $\mathcal{S}_{\mathbf{K},1}, \mathcal{S}_{\mathbf{K},2}$, ...The symbols in each column result from the substitution (41) on the symbols in the previous column.

Clearly, the number of elements in $\mathbf{K}^{(s)}$ is s. The substitution for $\mathbf{K}^{(s)}$ can readily be derived from the substitution for $\mathbf{K}$ (see(41)), by replacing all entries in this formula which are $\geq s$ by $\overline{s}$. As a consequence of the definition of $\mathbf{K}^{(s)}$ and of Lemma 2.5, we obtain

Lemma 2.6 *In* $\mathbf{K}_m^{(s)}$, *the set* $\mathcal{S}_{\mathbf{K},m}^{(s)}$ *of elementary block symbols is*

1. *when* $m < s$: $\mathcal{S}_{\mathbf{K},m}^{(s)} = \{[a,a,b] | a \in \{0,1,\ldots,s-1\}, b \in \{1,2,\ldots,\overline{s}\}, a < b\}$.
   The cardinality of this set is $\frac{m(m+1)}{2}$.
2. *when* $m = s$: $\mathcal{S}_{\mathbf{K},m}^{(s)} = \{[a,a,b] | a \in \{0,1,\ldots,s-1\}, b \in \{1,2,\ldots,\overline{s}\}, a < b\}$.
   The cardinality of this set is $\frac{s(s+1)}{2}$.
3. *when* $m > s$: $\mathcal{S}_{\mathbf{K},m}^{(s)} = \{[a,a,b] | a \in \{0,1,\ldots,s-1\}, b \in \{1,2,\ldots,\overline{s}\}, a < b\} \cup \{[\overline{s},\overline{s},\overline{s}]\}$.
   The cardinality of this set is $\frac{s(s+1)}{2} + 1$.

It is clear that the result under item 2 in this Lemma also holds for the infinite matrix $\mathbf{K}^{(s)}$.

3 Substitution for the matrix R

When considering the graphical representation of $\mathbf{K}$ or $\mathbf{K}^{(s)}$, the substitution based on elementary block symbols that generates these matrices actually becomes a substitution based on tiles of the $\mathbb{R}_+^2$-plane. A tile corresponds to an elementary block $[a,a,b]$, as illustrated in Fig. 7 (for p=3), together with the corresponding substitution. In this section, it will be convenient to consider tiling substitutions. Before deriving the substitution for $\mathbf{R}$, an intermediate step which develops a substitution for the sequence $\widehat{K}$ is necessary.

3.1 Substitution for the sequence $\widehat{K}$

Consider first the p-adic valuation of the sequence $\widehat{K}$ (defined over $\widehat{\mathcal{L}}$, see (12))

$$\widehat{K} = v_p(\widehat{G}), \tag{61}$$

Figure 8 shows $\widehat{K}_2$, the logsize-2 part of the graphical representation of $\widehat{K}$, for $p = 3$. It has the shape of a diamond, and the squares containing a finite number correspond to the elements of $\mathbf{K}_2$ (see(22)), as if $\mathbf{K}_2$ has been rotated over $-45°$. The other squares contain the value ∞, as being the p-adic valuation of 0. Logsize-m graphical representations

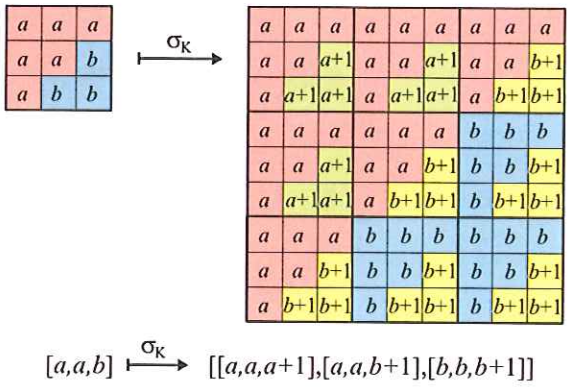

Figure 7: Illustration of the tile substitution corresponding to the symbolic block matrix substitution $[a, a, b] \mapsto [[a, a, a+1], [a, a, b+1], [b, b, b+1]]$ for $p = 3$. This extends in an obvious way to other values of the prime p according to the symbol definition (25).

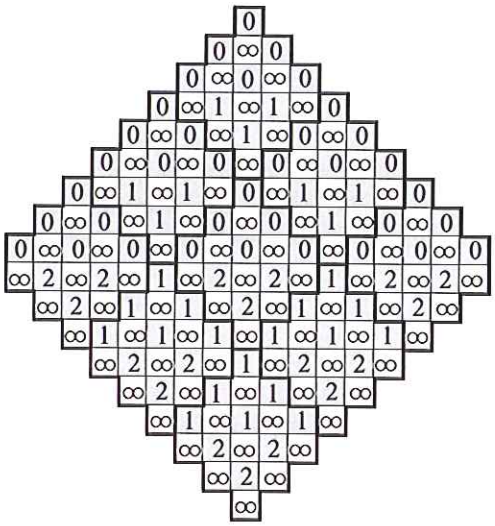

Figure 8: Graphical representation of $\widehat{K}_2$ (p=3). It consists of $p \times p$ elementary tiles. Compare to the $\mathbf{K}_2$-matrix (22).

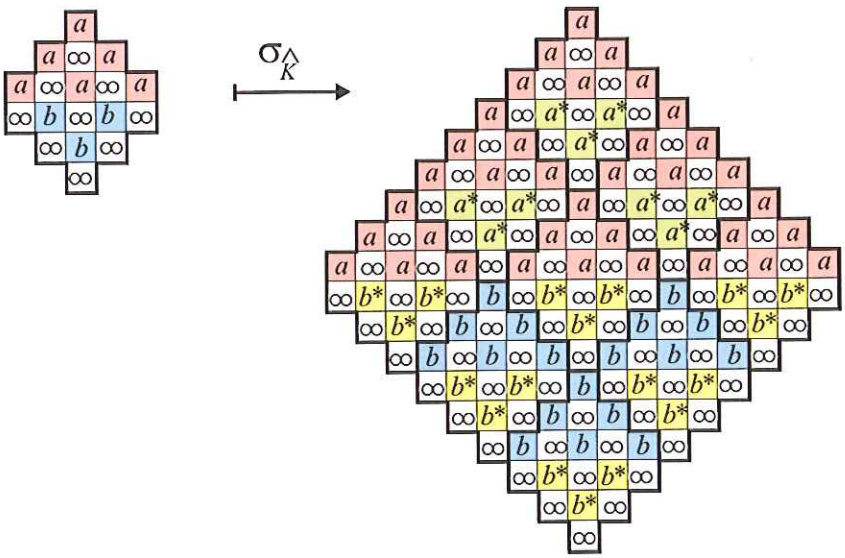

Figure 9: An elementary tile from $\widehat{K}$ and the corresponding tile substitution (for $p = 3$). Note that $a^* = a + 1, b^* = b + 1$. Compare to Fig. 7.

of $\widehat{K}$ relate in a similar way to $\mathbf{K}_m$. It is clear that with an elementary logsize-1 tile in the graphical representation of $\mathbf{K}$ (all of type $[a, a, b]$), there corresponds a logsize-1 tile $\hat{}[a, a, b]$ in the graphical representation of $\widehat{K}$, as shown in Fig.9. The substitution $[a, a, b] \mapsto [[a, a, a + 1], [a, a, b + 1], [b, b, b + 1]]$ defining $\mathbf{K}$ then transfers to a corresponding substitution

$$\hat{}[a, a, b] \mapsto \hat{}[\hat{}[a, a, a + 1], \hat{}[a, a, b + 1], \hat{}[b, b, b + 1]]. \tag{62}$$

$\widehat{K}$ is grown using this substitution, starting with the elementary tile $\widehat{K}_1 = \hat{} [0, 0, 1]$. This establishes an isomorphism between the substitutions for $\mathbf{K}$ and $\widehat{K}$ (or between $\mathbf{K}^{(s)}$ and $\widehat{K}^{(s)}$), and all properties concerning $\mathbf{K}$ can be easily transferred to $\widehat{K}$.

3.2 Substitution for R

In order to be able to turn expression

$$\mathbf{V} = \mathbf{K} + \mathbf{R}$$

(see (21)) into a substitution scheme, we need a substitution on $\mathbf{R}$ which is of the same type as for $\mathbf{K}$: an elementary square symbol block of logsize 1 ("square tile" of size $p \times p$) is replaced by $p \times p$ elementary square symbol blocks (square tiles). We will show here how this substitution can be derived from the substitution on $\widehat{K}$.

Figure 10 shows, for $p = 3$, how $\mathbf{R}$ and $\widehat{K}$ are related, and shows the distinct tilings for both. Observe that there are four types of elementary block symbols (elementary tiles) for $\mathbf{R}$:

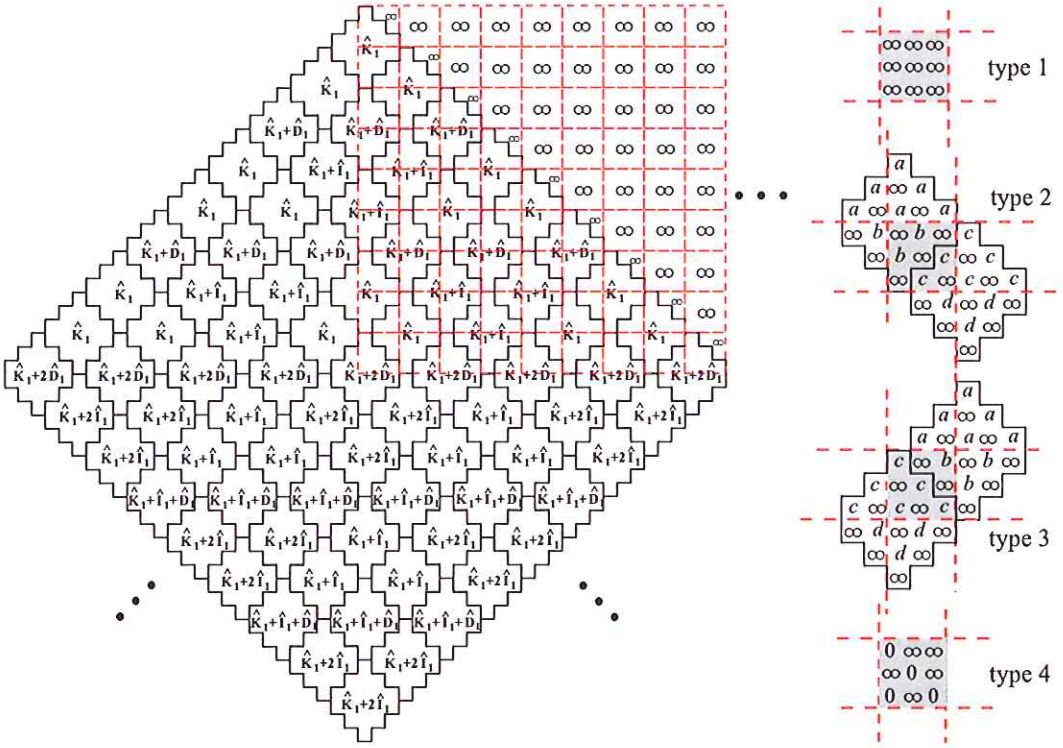

Figure 10: Left: The relationship between the tilings of $\widehat{K}$ (diamond-shaped tile with black outline) and $\mathbf{R}$ (square tiles with red outline), for $p = 3$ and logsize 3. $\widehat{K}_1 = {}^\wedge[0,0,1]$, $\widehat{D}_1 = {}^\wedge[0,0,1]$, $\widehat{I}_1 = {}^\wedge[1,1,1]$.The extension to greater sizes is trivially similar. Right: the four types of elementary symbol blocks (tiles) in $\mathbf{R}$, based on the fact that all tiles in $\widehat{K}$ are of general type ${}^\wedge[a,a,b]$.

Type 1: this concerns the blocks indicated with ∞ in the figure. The corresponding elementary block will be denoted $[\infty]$ and has all its elements equal to ∞ $(= v_p(0))$:

$$[\infty] = \begin{bmatrix} \infty & \infty & \infty \\ \infty & \infty & \infty \\ \infty & \infty & \infty \end{bmatrix}. \tag{63}$$

Types 2 and 3: occur at the nondiagonal elementary blocks in $\mathbf{R}$, and their content comes from two adjacent elementary blocks in $\widehat{K}$, in two possible ways, as illustrated in Figure10.

Type 2 is denoted $[b, c]$, and has the structure

$$[b, c] = \begin{bmatrix} \infty & b & \infty \\ b & \infty & c \\ \infty & c & \infty \end{bmatrix}. \tag{64}$$

Type 3 is denoted $< b, c >$:

$$< b, c >= \begin{bmatrix} c & \infty & b \\ \infty & c & \infty \\ c & \infty & c \end{bmatrix}. \tag{65}$$

Type 4: occurs on the diagonal blocks in $\mathbf{R}$, and is a specific instance of type 3:

$$< \infty, 0 >= \begin{bmatrix} 0 & \infty & \infty \\ \infty & 0 & \infty \\ 0 & \infty & 0 \end{bmatrix}. \tag{66}$$

(although these diagonal blocks involve distinct elementary $\widehat{K}$-blocks, all of type $\widehat{K}_1 + n\widehat{D}_1$, $n = 0, 1, 2, \ldots$ the six top right elements of these which form the left lower part of the diagonal blocks in $\mathbf{R}$ are all the same).

Now, assume that a substitution $\sigma_{\mathbf{R}}$ exists for $\mathbf{R}$. Then we know where to find the $p \times p$ elementary blocks which result from the substitution of any elementary block in $\mathbf{R}$: the elementary logsize-1 block $\mathbf{R}_1^{(k,l)}$ (recall that the superscript (k, l) refers to the block-coordinate) is substituted by a corresponding logsize-2 block, as follows

$$\sigma_{\mathbf{R}}(\mathbf{R}_1^{(k,l)}) = \mathbf{R}_2^{(k,l)} = \begin{bmatrix} \mathbf{R}_1^{(kp,lp)} & \mathbf{R}_1^{(kp+1,lp)} & \cdots & \mathbf{R}_1^{((k+1)p-1,lp)} \\ \mathbf{R}_1^{(kp,lp+1)} & \mathbf{R}_1^{(kp+1,lp+1)} & \cdots & \mathbf{R}_1^{((k+1)p-1,lp+1)} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{R}_1^{(kp,(l+1)p-1)} & \mathbf{R}_1^{(kp+1,(l+1)p-1)} & \cdots & \mathbf{R}_1^{((k+1)p-1,(l+1)p-1)} \end{bmatrix}. \tag{67}$$

We will now show, for the case $p = 3$, that identical elementary blocks in $\mathbf{R}$ map into identical logsize-2 blocks, from which we may conclude that the substitution $\sigma_{\mathbf{R}}$ actually exists.

First consider the type 1 blocks $[\infty]$. It is clear from Fig. 10, that all these blocks map into the same logsize-2 block:

$$[\infty] \mapsto \begin{bmatrix} [\infty] & [\infty] & [\infty] \\ [\infty] & [\infty] & [\infty] \\ [\infty] & [\infty] & [\infty] \end{bmatrix}. \tag{68}$$

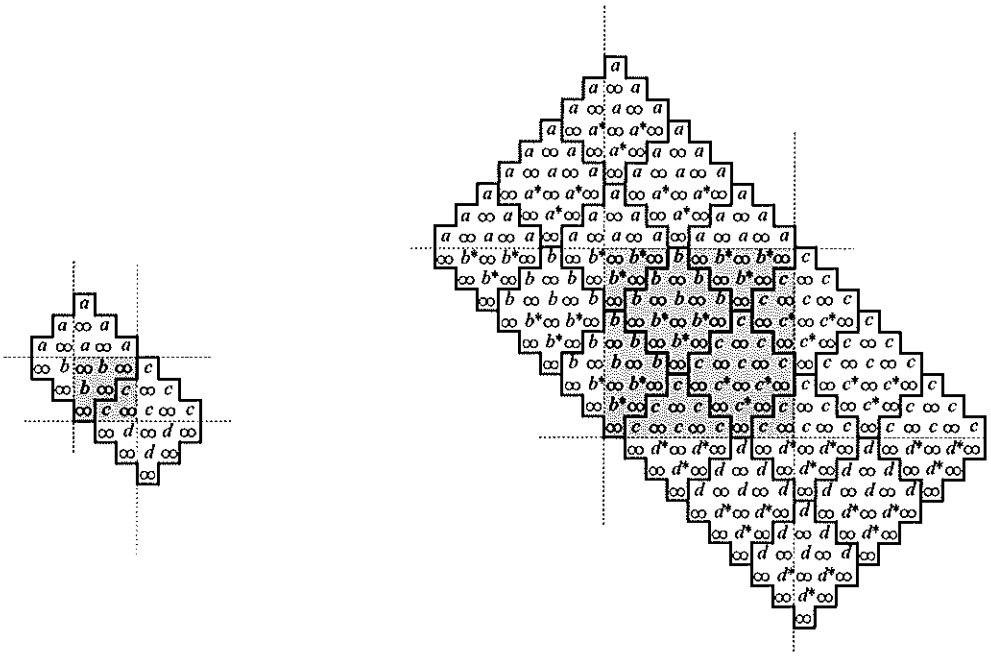

Figure 11: Finding the substitution for elementary block $[b, c]$ in $\mathbf{R}$.

Figure 11 shows how type 2 block $[b, c]$ in $\mathbf{R}$, which is obtained by joining parts of adjacent blocks $^\wedge[a, a, b]$ and $^\wedge[c, c, d]$ in $\widehat{K}$, maps into a logsize-2 block which is also obtained by the joining parts of the proper substitutions $\sigma_{\widehat{K}}(^\wedge[a, a, b])$ and $\sigma_{\widehat{K}}(^\wedge[c, c, d])$. We read from the figure that this gives

$$[b, c] \mapsto \begin{bmatrix} [b+1, b] & < b+1, b > & [b+1, c] \\ < b+1, b > & [b+1, c] & < c+1, c > \\ [b+1, c] & < c+1, c > & [c+1, c] \end{bmatrix}. \tag{69}$$

A similar result is obtained from Fig. 12 for type 3 blocks

$$< b, c > \mapsto \begin{bmatrix} < b+1, c > & [b+1, b] & < b+1, b > \\ [c+1, c] & < b+1, c > & [b+1, b] \\ < c+1, c > & [c+1, c] & < b+1, c > \end{bmatrix}. \tag{70}$$

Observe that the maps of $[b, c]$ and $< b, c >$ do not depend on the elements a, d which appear in the elementary blocks $^\wedge[a, a, b]$ and $^\wedge[c, c, d]$ from which $[b, c]$ originates. This is exactly why these mappings constitute a substitution in the strict sense for the symbols $[b, c]$ and $< b, c >$. The only mapping that still needs a check is the type 4 elementary diagonal block $< \infty, 0 >$ in $\mathbf{R}$. From Fig. 10, it can be seen that this block, when at position (n, n), maps into a logsize-2 block which contains parts of $\widehat{K}_1$ and $\widehat{K}_1 + n\widehat{D}_1$. Fortunately, the parts involved do not depend on n:

$$< \infty, 0 > \mapsto \begin{bmatrix} < \infty, 0 > & [\infty] & [\infty] \\ [1, 0] & < \infty, 0 > & [\infty] \\ < 1, 0 > & [1, 0] & < \infty, 0 > \end{bmatrix}. \tag{71}$$

Thus we conclude that $\mathbf{R}$ can be generated by a genuine substitution. This substitution is essentially defined by the mappings (69) and (70), as (68)and (71) are just special instances

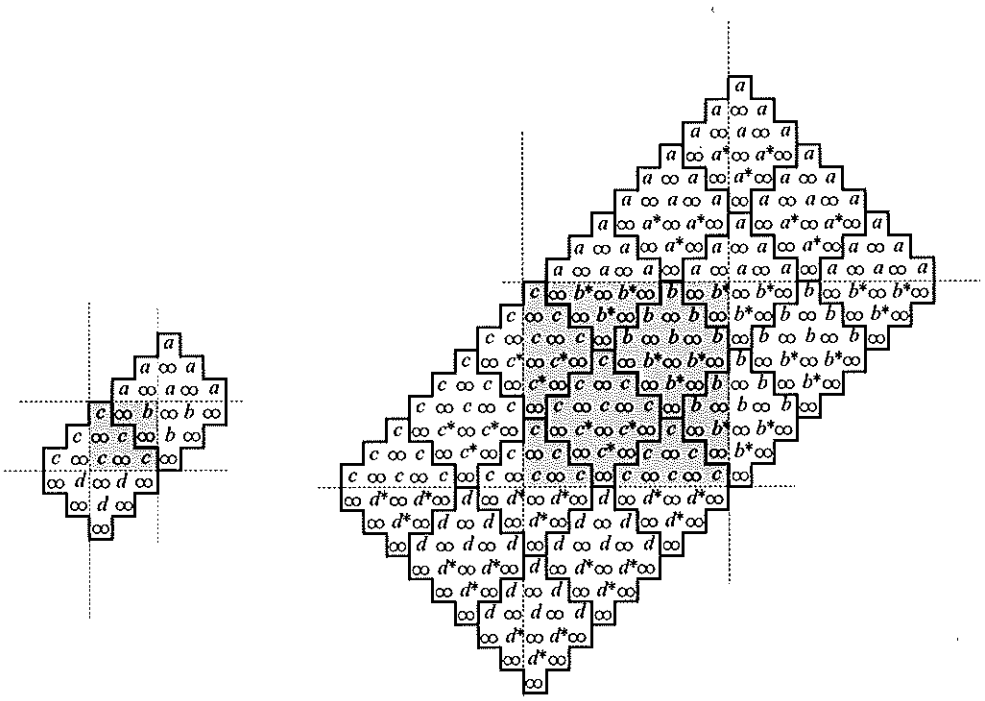

Figure 12: Finding the substitution for elementary block $< b, c >$ in $\mathbf{R}$.

of these when replacing b, c properly by ∞, thereby using the obvious relationship $[\infty] = [\infty, \infty] =< \infty, \infty >$. The substitution is completely determined by specifying the initial elementary block symbol, which is $\mathbf{R}_1 = \mathbf{R}_1^{(0,0)} =< \infty, 0 >$.

In the derivation of the substitution for $\mathbf{R}$ above, it was convenient to restrict ourselves to the particular case $p = 3$. A completely similar analysis is possible for other values of the prime p, taking into account the general structure $[a, a, b]$, as defined in Theorem 2.4, and the general validity of the substitutions (41), (62) for any p. This leads to the following general result:

Theorem 3.1 *The substitution generating* $\mathbf{R}$ *is* $(\sigma_{\mathbf{R}}, \mathbf{R}_1)$. *All elementary block symbols are* $p \times p$ *blocks of the following form (with* $b, c \in N(\subset \mathbb{N}) \cup \{\infty\}$*)*

$$[b, c] = \begin{bmatrix} \infty & b & \infty & b & \cdots & \infty & b & \infty \\ b & \infty & b & \infty & \cdots & b & \infty & c \\ \infty & b & \infty & b & \cdots & \infty & c & \infty \\ b & \infty & b & \infty & \cdots & c & \infty & c \\ \vdots & \vdots & & \ddots & & \vdots & & \\ \infty & b & \infty & c & \cdots & \infty & c & \infty \\ b & \infty & c & \infty & \cdots & c & \infty & c \\ \infty & c & \infty & c & \cdots & \infty & c & \infty \end{bmatrix} \tag{72}$$

or

$$< b,c >= \begin{bmatrix} c & \infty & b & \infty & \cdots & b & \infty & b \\ \infty & c & \infty & b & \cdots & \infty & b & \infty \\ c & \infty & c & \infty & \cdots & b & \infty & b \\ \infty & c & \infty & c & \cdots & \infty & b & \infty \\ \vdots & \vdots & & \iddots & & \vdots & & \\ c & \infty & c & \infty & \cdots & c & \infty & b \\ \infty & c & \infty & c & \cdots & \infty & c & \infty \\ c & \infty & c & \infty & \cdots & c & \infty & c \end{bmatrix}. \tag{73}$$

The substitution replaces the elementary symbol blocks b, c and $< b,c >$ by $p \times p$ new elementary blocks, as follows:

$\sigma_{\mathbf{R}}([b,c]) =$

$$\begin{bmatrix} [b+1,b] & < b+1,b > & [b+1,b] & \cdots & [b+1,b] & < b+1,b > & [b+1,c] \\ < b+1,b > & [b+1,b] & < b+1,b > & \cdots & < b+1,b > & [b+1,c] & < c+1,c > \\ [b+1,b] & < b+1,b > & [b+1,b] & \cdots & [b+1,c] & < c+1,c > & [c+1,c] \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ [b+1,b] & < b+1,b > & [b+1,c] & \cdots & [c+1,c] & < c+1,c > & [c+1,c] \\ < b+1,b > & [b+1,c] & < c+1,c > & \cdots & < c+1,c > & [c+1,c] & < c+1,c > \\ [b+1,c] & < c+1,c > & [c+1,c] & \cdots & [c+1,c] & < c+1,c > & [c+1,c] \end{bmatrix} \tag{74}$$

and

$\sigma_{\mathbf{R}}(< b,c >) =$

$$\begin{bmatrix} < b+1,c > & [b+1,b] & < b+1,b > & \cdots & < b+1,b > & [b+1,b] & < b+1,b > \\ [c+1,c] & < b+1,c > & [b+1,b] & \cdots & [b+1,b] & < b+1,b > & [b+1,b] \\ < c+1,c > & [c+1,c] & < b+1,c > & \cdots & < b+1,b > & [b+1,b] & < b+1,b > \\ \vdots & \vdots & \vdots & \iddots & \vdots & \vdots & \vdots \\ < c+1,c > & [c+1,c] & < c+1,c > & \cdots & < b+1,c > & [b+1,b] & < b+1,b > \\ [c+1,c] & < c+1,c > & [c+1,c] & \cdots & [c+1,c] & < b+1,c > & [b+1,b] \\ < c+1,c > & [c+1,c] & < c+1,c > & \cdots & < c+1,c > & [c+1,c] & < b+1,c > \end{bmatrix}. \tag{75}$$

The initial symbol from which to start the substitution is $\mathbf{R}_1 =< \infty, 0 >$.

Observe the symmetries in the matrices above. All are either Hankel or Toeplitz matrices. In $[b,c]$ and $< b,c >$ the non-infinite elements and the ∞-elements alternate in a checkerboard pattern. All non-infinite elements in $[b,c]$ equal b above the skew diagonal, and c below the skew diagonal. In $< b,c >$, all elements on and below the main diagonal equal c, the ones above the main diagonal equal b. At positions where there is a finite element in $< b,c >$, there is ∞ in $[b,c]$ and vice versa. The elementary blocks in the substitution matrices alternate between the $[*,*]$- and $< *,* >$-type in a checkerboard pattern. At positions where there is a $[*,*]$-type in one matrix, there is a $< *,* >$-type in the other, and vice versa. In the first substitution matrix, all blocks on the skew diagonal equal $[b+1,c]$, all blocks below the skew diagonal display the pair$(c+1,c)$, all blocks above this diagonal display the pair $(b+1,b)$. In the second substitution matrix, something similar occurs, but now along the main diagonal.

Also here, the number of distinct symbols which appear in $\mathbf{R}_m$, the logsize-m part of $\mathbf{R}$, can be determined. And this can be done as well for the s-reduction of $\mathbf{R}$. We summarize the results in

Lemma 3.2 *In* $\mathbf{R}_m$, *the set of distinct elementary block symbols is*

$$\mathcal{S}_m^{\mathbf{R}} = \{< \infty, 0 >, [\infty]\} \cup \{[a,b], < a,b > | a \in \{0,1,\ldots,m-1\}, b \in \{1,2,\ldots,m-2\}, b < a\}. \tag{76}$$

The cardinality of this set is $2 + (m-1)m$.

Lemma 3.3 *In* $\mathbf{R}_m^{(s)}$, *the set* $\mathcal{S}_{\mathbf{R}(s),m}$ *of elementary block symbols is*
1. *when* $m \leq s$: $\mathcal{S}_{\mathbf{R}(s),m} = \{< \infty, 0 >, [\infty]\} \cup \{[a,b], < a,b > | a \in \{0,1,\ldots,m-1\}, b \in \{1,2,\ldots,m-2\}, b < a\}$.
   The cardinality of this set is $2 + (m-1)m$.
2. *when* $m = s+1$: $\mathcal{S}_{\mathbf{R}(s),m} = \{< \infty, 0 >, [\infty]\} \cup \{[a,b], < a,b > | a \in \{0,1,\ldots,s\}, b \in \{1,2,\ldots,s-1\}, b < a\}$.
   The cardinality of this set is $2 + s(s+1)$.
3. *when* $m > s+1$: $\mathcal{S}_{\mathbf{R}(s),m} = \{< \infty, 0 >, [\infty]\} \cup \{[a,b], < a,b > | a \in \{0,1,\ldots,\overline{s}\}, b \in \{1,2,\ldots,s-1\}, b < a\} \cup \{[\overline{s},\overline{s}], < \overline{s},\overline{s} >\}$.
   The cardinality of this set is $4 + s(s+1)$.

4 The substitution for the p-adic valuation V of the Legendre coefficient matrix

We will now exploit the relationship $\mathbf{V} = \mathbf{K} + \mathbf{R}$ to determine the substitution for $\mathbf{V}$. Having similar substitutions for $\mathbf{K}$ and $\mathbf{R}$, it is clear that the substitution $\sigma_{\mathbf{V}}$ for $\mathbf{V}$, if it exists, must satisfy the following (recall that $\mathbf{V}_1^{(k,l)}$ refers to the elementary logsize-1 $(p \times p)$ block in $\mathbf{V}$ with coordinates (k,l), and that , in view of the summation above, it equals $\mathbf{K}_1^{(k,l)} + \mathbf{R}_1^{(k,l)}$

$$\sigma_{\mathbf{V}}(\mathbf{V}_1^{(k,l)}) = \sigma_{\mathbf{V}}(\mathbf{K}_1^{(k,l)} + \mathbf{R}_1^{(k,l)}) = \sigma_{\mathbf{K}}(\mathbf{K}_1^{(k,l)}) + \sigma_{\mathbf{R}}(\mathbf{R}_1^{(k,l)}). \tag{77}$$

The initial elementary block is $\mathbf{V}_1 = \mathbf{K}_1 + \mathbf{R}_1$.

Condition (77) actually allows to find the substitutions for the elementary blocks in $\mathbf{V}$. The only thing that needs to be checked in order to be able to conclude that the results induce a genuine substitution, is that identical elementary blocks should map into the same structure: i.e., if $\mathbf{V}_1^{(k,l)} = \mathbf{V}_1^{(i,j)}$ for some $((k,l) \neq (i,j)$, i.e., $\mathbf{K}_1^{(k,l)} + \mathbf{R}_1^{(k,l)} = \mathbf{K}_1^{(i,j)} + \mathbf{R}_1^{(i,j)}$ while $\mathbf{K}_1^{(k,l)} \neq \mathbf{K}_1^{(i,j)}$ and $\mathbf{R}_1^{(k,l)} \neq \mathbf{R}_1^{(i,j)}$, it must hold that $\sigma_{\mathbf{K}}(\mathbf{K}_1^{(k,l)}) + \sigma_{\mathbf{R}}(\mathbf{R}_1^{(k,l)}) = \sigma_{\mathbf{K}}(\mathbf{K}_1^{(i,j)}) + \sigma_{\mathbf{R}}(\mathbf{R}_1^{(k,l)})$. Or: $\sigma_{\mathbf{V}}(\mathbf{V}_1^{(k,l)})$ should only depend on the content of $\mathbf{V}_1^{(*,*)}$, not on its position, and thus not on the content of the underlying specific $\mathbf{K}_1^{(*,*)}$ or $\mathbf{R}_1^{(*,*)}$.

We will now demonstrate that this is the case. Recall that the elementary blocks in $\mathbf{K}$ are all of the type $[a,a,b]$, and those of $\mathbf{R}$ are either of type $< c,d >$ or $[c,d]$. Thus $\mathbf{V}_1^{(k,l)} = \mathbf{K}_1^{(k,l)+\mathbf{R}_1^{(k,l)}}$ is either of type $[a,a,b] + < c,d >$, or of type $[a,a,b] + [c,d]$.

Let us first have a look at the structure of the possible elementary $\mathbf{V}$-blocks.

i. Elementary $\mathbf{V}$-block of type $[a,a,b] + < c,d >$

From (41) and (65), it follows that (all matrices have size $p \times p$)

$$[a,a,b]+<c,d> = \begin{bmatrix} a & a & a & \cdots & a & a & b \\ a & a & a & \cdots & a & a & b \\ a & a & a & \cdots & a & b & b \\ \vdots & \vdots & \vdots & \iddots & \vdots & \vdots & \vdots \\ a & a & a & \cdots & b & b & b \\ a & a & b & \cdots & b & b & b \\ a & b & b & \cdots & b & b & b \end{bmatrix} \tag{78}$$

$$+ \begin{bmatrix} d & \infty & c & \cdots & c & \infty & c \\ \infty & d & \infty & \cdots & \infty & c & \infty \\ d & \infty & d & \cdots & c & \infty & c \\ \vdots & \vdots & \vdots & \iddots & \vdots & \vdots & \vdots \\ d & \infty & d & \cdots & d & \infty & c \\ \infty & d & \infty & \cdots & \infty & d & \infty \\ d & \infty & d & \cdots & d & \infty & d \end{bmatrix} \tag{79}$$

$$= \begin{bmatrix} a+d & \infty & a+c & \cdots & a+c & \infty & a+c \\ \infty & a+d & \infty & \cdots & \infty & a+c & \infty \\ a+d & \infty & a+d & \cdots & a+c & \infty & b+c \\ \infty & a+d & \infty & \cdots & \infty & b+c & \infty \\ \vdots & \vdots & \vdots & \iddots & \vdots & \vdots & \vdots \\ \infty & a+d & \infty & \cdots & \infty & b+c & \infty \\ a+d & \infty & a+d & \cdots & b+d & \infty & b+c \\ \infty & a+d & \infty & \cdots & \infty & b+d & \infty \\ a+d & \infty & b+d & \cdots & b+d & \infty & b+d \end{bmatrix} \tag{80}$$

$$\overset{\text{shorthand}}{=} ||[a+c, b+d, a+d]||, \tag{81}$$

where

$$||[u,v,w]|| = \begin{bmatrix} w & \infty & u & \infty & \cdots & \infty & \cdots & \infty & u & \infty & u \\ \infty & w & \infty & u & \cdots & u & \cdots & u & \infty & u & \infty \\ w & \infty & w & \infty & \cdots & \infty & \cdots & \infty & u & \infty & t \\ \infty & w & \infty & w & \cdots & u & \cdots & u & \infty & t & \infty \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \iddots & \vdots & \vdots & \vdots & \vdots \\ \infty & w & \infty & w & \cdots & w & \cdots & t & \infty & t & \infty \\ \vdots & \vdots & \vdots & \vdots & \iddots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ \infty & w & \infty & w & \cdots & v & \cdots & v & \infty & t & \infty \\ w & \infty & w & \infty & \cdots & \infty & \cdots & \infty & v & \infty & t \\ \infty & w & \infty & v & \cdots & v & \cdots & v & \infty & v & \infty \\ w & \infty & v & \infty & \cdots & \infty & \cdots & \infty & v & \infty & v \end{bmatrix}, \tag{82}$$

with $t = u + v - w$ (thus $||[u,v,w]||$ mentions only independent parameters). Notice the clear division of matrix $||[u,v,w]||$ into a left-, upper-, right- and bottom quarter, which respectively display w, u, t, v.

ii. Elementary V-block of type $[a,a,b] + [c,d]$

From (41) and (69), it follows by a straightforward matrix summation that

$$[a,a,b] + [c,d] = [a+c, b+d]. \tag{83}$$

Now consider the result of applying (77) on these two types of elementary blocks in $\mathbf{V}$.

i.

$$\sigma_{\mathbf{V}}([a,a,b]+<c,d>)=\sigma_{\mathbf{V}}(|[a+c,b+d,a+d]|)=\sigma_{\mathbf{K}}([a,a,b])+\sigma_{\mathbf{R}}(<c,d>). \quad (84)$$

I.e., (84) corresponds to the summation of (41) and (75).
Using

$$\alpha=a+c,\beta=b+d,\gamma=a+d,$$

and the following shorthand notations

$$\begin{aligned}
\mathsf{A} &= |[\alpha+1,\gamma+1,\gamma]| && (85)\\
\mathsf{B} &= |[\gamma+1,\beta+1,\gamma]| && (86)\\
\mathsf{C} &= |[\alpha+1,\alpha+\beta-\gamma+1,\alpha]| && (87)\\
\mathsf{D} &= |[\alpha+\beta-\gamma+1,\beta+1,\beta]| && (88)\\
\mathsf{E} &= [\alpha+1,\alpha+1] && (89)\\
\mathsf{F} &= |[\alpha+1,\alpha+1,\alpha]| && (90)\\
\mathsf{G} &= [\gamma+1,\gamma+1] && (91)\\
\mathsf{H} &= |[\gamma+1,\gamma+1,\gamma]| && (92)\\
\mathsf{K} &= [\beta+1,\beta+1] && (93)\\
\mathsf{L} &= |[\beta+1,\beta+1,\beta]| && (94)\\
\mathsf{P} &= [\alpha+\beta-\gamma+1,\alpha+\beta-\gamma+1] && (95)\\
\mathsf{Q} &= |[\alpha+\beta-\gamma+1,\alpha+\beta-\gamma+1,\alpha+\beta-\gamma]| && (96)\\
\mathsf{X} &= |[\alpha+1,\beta+1,\gamma]| && (97)
\end{aligned}$$

this gives

$$\sigma_{\mathbf{V}}(|[\alpha,\beta,\gamma]|)=\begin{bmatrix}
\mathsf{A} & \mathsf{E} & \mathsf{F} & \mathsf{E} & \cdots & \mathsf{E} & \cdots & \mathsf{E} & \mathsf{F} & \mathsf{E} & \mathsf{C}\\
\mathsf{G} & \mathsf{A} & \mathsf{E} & \mathsf{F} & \cdots & \mathsf{F} & \cdots & \mathsf{F} & \mathsf{E} & \mathsf{C} & \mathsf{P}\\
\mathsf{H} & \mathsf{G} & \mathsf{A} & \mathsf{E} & \cdots & \mathsf{E} & \cdots & \mathsf{E} & \mathsf{C} & \mathsf{P} & \mathsf{Q}\\
\mathsf{G} & \mathsf{H} & \mathsf{G} & \mathsf{A} & \cdots & \mathsf{F} & \cdots & \mathsf{C} & \mathsf{P} & \mathsf{Q} & \mathsf{P}\\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \iddots & \vdots & \vdots & \vdots & \vdots\\
\mathsf{G} & \mathsf{H} & \mathsf{G} & \mathsf{H} & \cdots & \mathsf{X} & \cdots & \mathsf{Q} & \mathsf{P} & \mathsf{Q} & \mathsf{P}\\
\vdots & \vdots & \vdots & \vdots & \iddots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots\\
\mathsf{G} & \mathsf{H} & \mathsf{G} & \mathsf{B} & \cdots & \mathsf{L} & \cdots & \mathsf{D} & \mathsf{P} & \mathsf{Q} & \mathsf{P}\\
\mathsf{H} & \mathsf{G} & \mathsf{B} & \mathsf{K} & \cdots & \mathsf{K} & \cdots & \mathsf{K} & \mathsf{D} & \mathsf{P} & \mathsf{Q}\\
\mathsf{G} & \mathsf{B} & \mathsf{K} & \mathsf{L} & \cdots & \mathsf{L} & \cdots & \mathsf{L} & \mathsf{K} & \mathsf{D} & \mathsf{P}\\
\mathsf{B} & \mathsf{K} & \mathsf{L} & \mathsf{K} & \cdots & \mathsf{K} & \cdots & \mathsf{K} & \mathsf{L} & \mathsf{K} & \mathsf{D}
\end{bmatrix}. \quad (98)$$

Observe that the result of the substitution only depends on $\alpha=a+c,\beta=b+d,\gamma=a+d$. This means that, no matter which elementary blocks $[a,a,b]$ in $\mathbf{K}$ and $<c,d>$ in $\mathbf{R}$ add up to the symbol $|[\alpha,\beta,\gamma]|$ in $\mathbf{V}$, the image under the mapping (98) is unique and independent of these constituents.

ii.

$$\sigma_{\mathbf{V}}([a,a,b]+[c,d])=\sigma_{\mathbf{V}}([a+c,b+d])=\sigma_{\mathbf{K}}([a,a,b])+\sigma_{\mathbf{R}}([c,d]). \quad (99)$$

I.e., (99) corresponds to the summation of (41) and (74). The result is a Hankel block matrix ($p\times p$ blocks), featuring the blocks $\mathsf{E},\mathsf{F},\mathsf{K},\mathsf{L}$ as defined above , and also

$$\mathsf{Z}=[\alpha+1,\beta+1]\ :$$

$$\sigma_{\mathbf{V}}([\alpha,\beta]) = \begin{bmatrix} \mathsf{E} & \mathsf{F} & \mathsf{E} & \cdots & \mathsf{E} & \mathsf{F} & \mathsf{Z} \\ \mathsf{F} & \mathsf{E} & \mathsf{F} & \cdots & \mathsf{F} & \mathsf{Z} & \mathsf{L} \\ \mathsf{E} & \mathsf{F} & \mathsf{E} & \cdots & \mathsf{Z} & \mathsf{L} & \mathsf{K} \\ \vdots & \vdots & \vdots & \iddots & \vdots & \vdots & \vdots \\ \mathsf{E} & \mathsf{F} & \mathsf{Z} & \cdots & \mathsf{K} & \mathsf{L} & \mathsf{K} \\ \mathsf{F} & \mathsf{Z} & \mathsf{L} & \cdots & \mathsf{L} & \mathsf{K} & \mathsf{L} \\ \mathsf{Z} & \mathsf{L} & \mathsf{K} & \cdots & \mathsf{K} & \mathsf{L} & \mathsf{K} \end{bmatrix} \tag{100}$$

Again, this mapping only depends on the specific elements in an elementary block of type $[\alpha,\beta]$ in $\mathbf{V}$, and not on the particular underlying constituents in $\mathbf{K}$ and $\mathbf{R}$.

All this leads to the conclusion that the substitution defined by the mappings (98) and (100) is genuine. The initial elementary block symbol from which to start the substitution is $\mathbf{V}_1 = \mathbf{K}_1 + \mathbf{R}_1 = [0,0,1] + < \infty, 0 >= |[\infty,1,0]|$. We conclude with the formal

Theorem 4.1 *The substitution generating the $\mathbf{V}$-matrix (i.e., the p-adic valuation of the Legendre coefficient matrix) is defined by $(\sigma_{\mathbf{V}}, \mathbf{V}_1)$, whereby the initial elementary symbol block matrix $\mathbf{V}_1 = |[\infty,1,0]|$, and whereby the substitution $\sigma_{\mathbf{V}}$ is defined by the expressions (98) and (100).*

For $\mathbf{V}_m$, it is not as easy as for $\mathbf{K}_m$ and $\mathbf{R}_m$ to give an explicit description of the elementary block symbol set and its cardinality (see Lemmas 2.5, 3.2). But it is clear that this symbol set generates itself by applying the substitution $\sigma_{\mathbf{V}}$ iteratively, starting from $|[\infty,1,0]|$.

A similar substitution exists for the s-reduced matrix $\mathbf{V}^{(s)}$. Just replace the non-infinite elements in the elementary symbol blocks which are $\geq s$ by $\overline{s}$. Or, as an alternative, one could consider the sum of the substitutions for $\mathbf{K}^{(s)}$ and $\mathbf{R}^{(s)}$, thereby taking into account that the sum of any two finite elements which is $\geq s$, should be reduced to $\overline{s}$.

Example 1 Consider the case $p = 3$. Figure 13 displays $\mathbf{V}_1$, $\mathbf{V}_2$, $\mathbf{V}_3$ resulting from applying the substitution $(\sigma_{\mathbf{V}}, \mathbf{V}_1)$, and Fig. 14 displays $\mathbf{V}_1^{(2)}$, $\mathbf{V}_2^{(2)}$, $\mathbf{V}_3^{(2)}$. These results correspond to the left-top part of the graphical representation of $\mathbf{V}$ and $\mathbf{V}^{(2)}$ as displayed in Figs. 3 and 4, which were calculated independently using (2).

Acknowledgements The authors thank Fritz von Haeseler and Jean-Paul Allouche for stimulating discussions, and Heinz-Otto Peitgen for his support. AB thanks the University of Bremen and GS the University of Leuven for their hospitality. This research was supported by the FWO research community ICCoS, and the Belgian Federal Science Policy Office (IUAP P6/04 (DYSCO)).

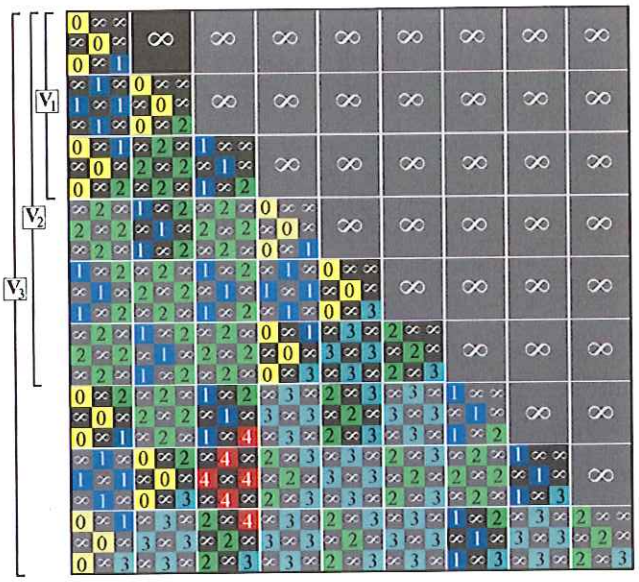

Figure 13: $\mathbf{V}_1$,$\mathbf{V}_2$,$\mathbf{V}_3$ as generated by the substitution $(\sigma_{\mathbf{V}}, \mathbf{V}_1)$. The distinct elementary block symbols (i.e. elementary blocks with distinct patterns) are highlighted by saturated coloring. $\mathbf{V}_1$ has 1 elementary block, it is the initial symbol from which the substitution $\sigma_{\mathbf{V}}$ starts, $\mathbf{V}_2$ has 7 distinct elementary blocks, $\mathbf{V}_3$ has 20. The number of distinct elementary blocks will keep growing in $\mathbf{V}_m$ as m grows.

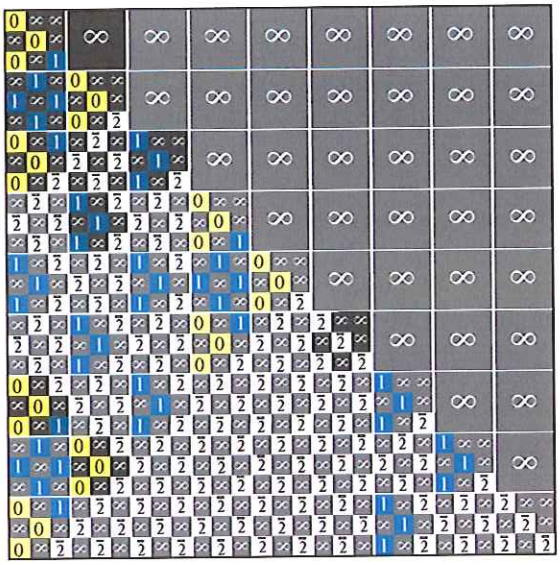

Figure 14: Generating the s = 2-restrictions $\mathbf{V}_1^{(2)}$, $\mathbf{V}_2^{(2)}$, $\mathbf{V}_3^{(2)}$ by substitution. Distinct elementary blocks are highlighted by saturated coloring. $\mathbf{V}_1^{(2)}$ has 1 elementary block, $\mathbf{V}_2^{(2)}$ has 7 elementary blocks. All distinct elementary blocks for the bi-infinite matrix $\mathbf{V}^{(2)}$ are already present in $\mathbf{V}_3^{(2)}$. Their number is 10, a number which no longer increases in $\mathbf{V}_m$ as m grows.

References

1. M. Abramowitz and I. A. Stegun (Eds.), *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, 9th ed. (Dover, New York, 1972).
2. J. B. Holt, On the irreducibility of Legendre polynomials, II, *Proc. London Math. Soc.* **12** (1913) 126-132.
3. J. Wahab, New cases of irreducibility for Legendre polynomials, *Duke Math. J.* **19** (1952) 165-176.
4. L. Carlitz, Congruence properties of the polynomials of Hermite, Laguerre and Legendre, *Math. Z.* **59** (1954) 474-483.
5. T. Honda, Two congruence properties of Legendre polynomials, *Osaka J. Math.* **13** (1976) 131-133.
6. P. S. Landweber, Supersingular elliptic curves and congruences for Legendre polynomials, in *Elliptic curves and modular forms in algebraic topology, Lecture Notes in Math.*, ed. P. S. Landweber, **1326** (Springer, New York 1988), pp. 69-83.
7. N. Yui, Jacobi quartics, Legendre polynomials and formal groups, in *Elliptic curves and modular forms in algebraic topology, Lecture Notes in Math.*, ed. P. S. Landweber, **1326** (Springer, New York 1988), pp. 182-215.
8. J.-L. Brylinski, Legendre polynomials and the elliptic genus, *J. Algebra* **145** (1992) 83-93.
9. A. Robert, Polynômes de Legendre mod 4, *C. R. Acad. Sci. Paris, Sér. I Math.* **316** (1993) 1235-1240.
10. M. Zuber, Propriétés de congruence de certaines familles classiques de polynômes, *C. R. Acad. Sci. Paris, Sér. I Math.* **315** (1992) 869-872.
11. J.-P. Allouche, G. Skordev, Schur congruences, Carlitz sequences of polynomials and automaticity, *Discr. Math., Discrete Math.* **214** (2000) 21-49.
12. F. v. Haeseler, H.-O. Peitgen, G. Skordev, On the fractal structure of the rescaled evolution set of Carlitz sequences of polynomials, *Discrete Appl. Math.* **103** (2000) 89-109.
13. J.-P. Allouche, J. Shallit, *Automatic Sequences*, (Cambridge University Press, Cambridge, 2003).
14. R. Horn, C. Johnson, Topics in Matrix Analysis, (Cambridge University Press, Cambridge, 1994).
15. F. v. Haeseler, H.-O. Peitgen, G. Skordev, Pascal's triangle, dynamical systems and attractors, *Ergodic Theory Dynam. Systems* **12** (1992) 479-486.
16. H.-O. Peitgen, H. Jürgens, D. Saupe, *Chaos and Fractals*, (Springer-Verlag, Berlin, 1993).
17. P. Borwein, L. Jorgenson, Visible structures in number theory, *Amer. Math. Monthly* **108** (2001) 897-910.
18. A. Barbé, On a class of fractal matrices (I): "Excess-matrices and their self-similar properties," *Int. J. Bifur. Chaos Appl. Sci. Engrg.* **2**(1992) 841-860.