Acta Univ. M. Belii
Math. no.4 (1996), pp. 53-66

DEFINABILITY OF PASCAL'S TRIANGLES MODULO 4 AND 6 AND SOME OTHER BINARY OPERATIONS FROM THEIR ASSOCIATED EQUIVALENCE RELATIONS

IVAN KOREC

Abstract. Pascal's triangles modulo n can be considered as binary operations on the set $\mathbb{N}$ of nonnegative integers. To every binary operation f on a set M an equivalence relation R on M^2 can be associated in which (x,y) is equivalent with (u,v) if and only if $f(x,y)=f(u,v)$. The equivalence R can be considered as a 4-ary relation on M, and we can try to reconstruct f from R, more precisely, to define elementarily f in $\langle M;R\rangle$. (Some abstract information about f is used by this.) This problem will be solved for Pascal's triangles modulo n for $1\le n\le 6$. The answer is positive for $n=4$ and $n=6$, negative for $n=1$ and n prime (even greater than 6). As a corollary we obtain that the operations $+$, $\times$ are definable in the structure $\langle \mathbb{N}; \mathrm{EqB}_6\rangle$, where $\mathrm{EqB}_6=\big\{(x,y,u,v)\in\mathbb{N}^4 \mid \binom{x+y}{x}\equiv\binom{u+v}{u} \pmod 6\big\}$; the integer 6 cannot be replaced by any smaller positive integer. The above mentioned problem will be solved (positively, resp. negatively) also for addition and multiplication on the set $\mathbb{N}$, resp. $\mathbb{Z}$, and for some other operations.

1. Introduction

To every mapping $f: X\to Y$ an equivalence relation R on X can be associated by the formula $R(x,y) \iff f(x)=f(y)$. In particular, to every binary operation $*$ on a set M an equivalence relation R on M^2 can be associated. We can consider R as a 4-ary relation on the set M in the obvious way.

Definition. *Let $*$ be a binary operation on a set M. We shall say that R is the associated equivalence relation of the operation $*$ if*

$$R=\big\{(x,y,u,v)\in M^4 \mid x*y=u*v\big\}.$$

Notice once more that the associate equivalence relation is not an equivalence relation on M but may be considered as an equivalence relation on M^2. (Analogously we could associate a $2n$-ary relation to an n-ary operation also for $n\neq 2$.) We can also define R in the groupoid $\langle M;*\rangle$ by the first order formula

$$R(x,y,u,v) \iff x*y=u*v.$$

1991 *Mathematics Subject Classification.* Primary 03B10, 11B65 Secondary 08A99.

Key words and phrases. Elementary definability, Binomial coefficients, Equivalence relations.

This work was supported by Grant 224 of Slovak Academy of Sciences.

The relation R was constructed from $*$. We can ask whether, conversely, $*$ can be reconstructed from R. Generally speaking, it is impossible because distinct operations can have equal associated equivalence relations. However, sometimes it can be done if additional information about the structure $\langle M; *\rangle$ is available. In what follows usually the structure $\langle M; *\rangle$ will be given up to isomorphism; this is the strongest possible *abstract* information about $\langle M; *\rangle$, but it also need not suffice. Further, the answer can depend on the chosen type of reconstructability. We shall deal with first order definability, and so our goal is to define (elementarily, i.e., by a first order formula) the operation $*$ in the structure $\langle M; R\rangle$.

We shall investigate Pascal's triangles modulo n from this point of view. Pascal's triangle modulo n will be denoted by B_n, and it is defined by the formula

$$B_n(x, y) = \binom{x+y}{x} \operatorname{MOD} n;$$

the symbol MOD denotes the rest by integer division. In the present paper moduli $n \leq 6$ will be considered; the greater moduli will be considered later. However, the answer to our problem seems to depend on the factorization of n. So examples for all three typical cases are presented here: n prime, n prime power (with the exponent $e > 1$) and n divisible by at least two distinct primes. Besides Pascal's triangles modulo n also several more classical examples of binary operations will be considered.

We shall use the classical first order predicate calculus with equality. We shall use five usual logical connectives with usual priority rules and other method to simplify or shorter the formulas. Classical mathematical symbols (like $+$, $\times$ etc.) will be used in their usual sense; it may depend on the considered base set. Predicate and functional symbols are formed rather freely (groups of several letters, subscripts, superscripts, ...) but, of course, from the formal point of view every such symbol is considered as indecomposable.

2. Illustrating examples

Let us describe the problem from previous section informally for the case M finite. Let in the Cayley table of $\langle M; *\rangle$ the inside elements are replaced by colours (distinct elements by distinct colours). We obtain the coloured table (without information about the used association of colours to the elements of M). Then coloured table shows us the equivalence relation associated to $*$ (and nothing more: the coloured table can be constructed, up to the choice of colours, from this relation). Moreover, we obtain some additional information about $\langle M; *\rangle$. For example, we can obtain the Cayley table of an isomorphic copy of the structure; this is the strongest possible *abstract* information about $\langle M; *\rangle$. Of course, the order of the elements in its headings need not correspond to that in the coloured table. Our goal is to reconstruct the coloured table, i.e. to replace the colours by the elements of M in the original way. In principle, we could simply check all binary operations on M. However, we shall use the considerations which will be useful also for the infinite cases considered later; for example, we shall look for "invariants" expressible by first order formulas.

Example 2.1. Let $\langle M; *\rangle$ be a groupoid , where $M = \{0, 1, 2, 3\}$ and $*$ is the operation which must be reconstructed. We are given the Cayley table of an isomorphic copy $\mathcal{A}$

of $\langle M; * \rangle$ and the coloured table constructed as described above. They are given in the left-hand and the central part of Figure 1; let the capitals correspond to colours: Red, Green, Blue, Yellow.

	a	b	c	d
a	a	d	b	c
b	c	d	c	b
c	a	a	a	d
d	b	c	d	a

	0	1	2	3
0	R	G	B	Y
1	B	R	Y	G
2	G	B	Y	B
3	Y	R	R	R

	0	1	2	3
0	1	2	3	0
1	3	1	0	2
2	2	3	0	3
3	0	1	1	1

Figure 1.

We have to associate elements to colours and (as a by-product) find an isomorphism between $\langle M; * \rangle$ and the structure $\mathcal{A}$ (with Cayley's table) displayed on the left. Since $\mathcal{A}$ has no nontrivial automorphism the isomorphism will be determined uniquely. The Red colour occurs in the table 5 times, and the only element which occurs 5 times in the left table (except headings) is a; therefore Red must be associated to a. Similarly Green must be associated to b. The Yellow occurs once at the main diagonal, hence it must be associated to d. It remains to associate Blue to c. There are only two distinct colours in the row of 3, therefore 3 must be associated to c, and hence to Blue. The only pair of commuting elements of $\langle M; * \rangle$ is $\{0, 3\}$ and the only such pair in $\mathcal{A}$ is $\{c, d\}$. Therefore 0 must be associated to d, and hence to Yellow. There remain the colours Red, Green and the elements 1, 2. We cannot associate Red to 2 because the obtained algebra would have no idempotent, and $\mathcal{A}$ has one. Therefore we have to associate Red to 1, and finally Green to 2. The completed Cayley table is on the right-hand side of Figure 1.

Remark. A faster (but less illustrative) method in this case would be to consider the invariants "number of distinct symbols in the row and in the column" for the elements of $\mathcal{A}$ and the elements of M. So we obtain immediately the isomorphism mentioned above. Then we can "forget" colours, and fill in the table of $\langle M; * \rangle$.

Example 2.2. Let us consider the tables on the left-hand part of Figure 2; their roles are similar to those in Figure 1. Now we cannot reconstruct the operation $*$ uniquely (and we cannot define it from its associated equivalence relations) because there are two distinct (although isomorphic) algebras which fulfil the given conditions.

	a	b
a	a	b
b	b	a

	0	1
0	R	G
1	G	R

	0	1
0	0	1
1	1	0

	0	1
0	1	0
1	0	1

Figure 2.

More formally, let $\langle \{0, 1\}, \oplus \rangle$ be the additive group modulo 2. Then the operation $\oplus$

is not definable in the structure $\big\langle\{0,1\};R\big\rangle$, where

$$R=\big\{(x,y,u,v)\in\{0,1\}^4 \mid x\oplus y=u\oplus v\big\}$$

is the the associated equivalence relation of $\oplus$.

Example 2.3. Let us consider the left-hand and the central table of Figure 3; their role is similar to those in Example 2.1.

	a	b	c
a	a	c	c
b	c	b	c
c	c	c	c

	0	1	2
0	R	G	G
1	G	B	G
2	G	G	G

	0	1	2
0	0	2	2
1	2	1	2
2	2	2	2

Figure 3.

The algebra on the left is idempotent, hence the reconstructed algebra is also idempotent. Hence the elements 0, 1, 2 must be associated to the colours Red, Blue, Green, respectively; we can see it immediately from the diagonal of the central table. However, the element and the colour associated to a are not uniquely determined. It can be either 0 and Red or 1 and Blue; both choices are possible, and determine the two isomorphisms between the left-hand and the right-hand table.

Example 2.4. Let us consider the left-hand and the central table of Figure 3, and let us replace any non-diagonal G in the central table by R. The only possible solution of our problem can be the operation on the right. However, it is not a solution indeed. So we can see that the table of an isomorphic image and the coloured table cannot be combined arbitrarily. They really must correspond to the same algebra.

Example 2.5. Let us consider two operations on the set $\{0,1\}$: logical conjuction (now denoted by $\bullet$) and Sheffer's function denoted by $*$; the tables are given in Figure 4.

$\bullet$	0	1
0	0	0
1	0	1

$*$	0	1
0	1	1
1	1	0

Figure 4.

The corresponding algebras are not isomorphic; the first one is idempotent while the other is not. Nevertheless, we can see that $\mathrm{Eq}_\bullet=\mathrm{Eq}_*$. Both elements 0, 1 are definable (as constants) from the relation $\mathrm{Eq}_\bullet$, and hence the operations $\bullet$ and $*$ (as well as all other binary operations on $\{0,1\}$) are definable, too. (Of course, the defining formulas must be distinct.)

Example 2.6. Let us consider a set M of cardinality greater than 1 and the operation $*$ on M be defined by $x * y = x$ for all $x, y \in M$. Then $\mathrm{Eq}_*(x, y, z, w) \iff x = z$. We cannot define the elements of M (as constants) in the structure $\langle M; \mathrm{Eq}_* \rangle$. Nevertheless, the operation $*$ is definable in this structure. (Of course, we need not use Eq_* at all.)

3. Some results for more classical structures

Theorem 3.1. *Let $*$ be an idempotent operation on a nonempty set M and let Eq_* be its associated equivalence relation. Then the operation $*$ is first order definable in the structure $\langle M; \mathrm{Eq}_* \rangle$.*

Proof. The operation $*$ can be defined by the formula

$$z = x * y \iff \mathrm{Eq}_*(z, z, x, y).$$

Indeed, since always $z * z = z$ the equations $z = x * y$ and $z * z = x * y$ are equivalent. □

Remark. Theorem 3.1 is formulated for a single algebra. We can reformulate it for the class of all (nonempty) idempotent groupoids without any difficulties. However, it cannot be extended to the class of all groupoids, as Example 2.5 shows.

For the next theorem remember that *the center* of a group is its subset consisting of all elements which commute with every element. The center of a group is always nonempty because it contains its neutral element.

Theorem 3.2. *Let $\langle M; * \rangle$ be a group and let Eq_* be the associated equivalence relation of the operation $*$. Then $*$ is definable in the structure $\langle M; \mathrm{Eq}_* \rangle$ if and only if the center of the group $\langle M; * \rangle$ consists of unique element.*

Proof. If the center of $\langle M; * \rangle$ contains only the neutral element of G then we can define this element and then the operation $*$ in $\langle M; * \rangle$ as follows:

$$\begin{aligned} x = 1 &\iff \forall y, u, v \big(\mathrm{Eq}_*(x, y, u, v) \implies \mathrm{Eq}_*(y, x, u, v) \big), \\ z = x * y &\iff \mathrm{Eq}_*(z, 1, x, y). \end{aligned}$$

If the center contains an element $a \neq 1$ then we shall consider the operation $\otimes$ defined by $x \otimes y = a * x * y$. The structure $\langle M; \otimes \rangle$ is a group isomorphic with $\langle M; * \rangle$ (and distinct from it). However, both operations have the same associated equivalence relations Eq_*, and hence none of them can be definable in $\langle M; \mathrm{Eq}_* \rangle$. □

Theorem 3.3. (i) *The operation $+$ (on the set $\mathbb{N}$) is definable in the structure $\langle \mathbb{N}; \mathrm{EqPlus} \rangle$, where $\mathrm{EqPlus} = \{(x, y, u, v) \in \mathbb{N}^4 \mid x + y = u + v\}$.*

(ii) *The operation $\times$ (on the set $\mathbb{N}$) is definable in the structure $\langle \mathbb{N}; \mathrm{EqTimes} \rangle$, where* $\mathrm{EqTimes} = \{(x, y, u, v) \in \mathbb{N}^4 \mid xy = uv\}$.

Proof. In $\langle \mathbb{N}; \mathrm{EqPlus} \rangle$ we can define

$$x = 0 \iff \forall y, z \big(\mathrm{EqPlus}(x, x, y, z) \implies x = y \wedge x = z \big).$$

Then we have $z = x + y \iff \mathrm{EqPlus}(z, 0, x, y)$. The proof of (ii) is similar; we shall define 1 at first. □

Theorem 3.4. (i) *The operation* $+$ *(on the set* $\mathbb{Z}$*) is not definable in the structure* $\langle \mathbb{Z}, \mathrm{EqPlus} \rangle$, *where* $\mathrm{EqPlus} = \{(x, y, u, v) \in \mathbb{Z}^4 \mid x + y = u + v\}$.

(ii) *The operation* $\times$ *(on the set* $\mathbb{Z}$*) is not definable in the structure* $\langle \mathbb{Z}; \mathrm{EqTimes} \rangle$, *where* $\mathrm{EqTimes} = \{(x, y, u, v) \in \mathbb{Z}^4 \mid xy = uv\}$.

Proof. For (i) we can apply Theorem 3.2 because the center of the commutative group $\langle \mathbb{Z}; + \rangle$ is $\mathbb{Z}$.

For (ii) let us consider the mapping $f : x \mapsto -x$. We can see that f is an automorphism of $\langle \mathbb{Z}; \mathrm{EqTimes} \rangle$, and f is not an automorphism of $\langle \mathbb{Z}, \times \rangle$. Therefore $\times$ cannot be definable in $\langle \mathbb{N}; \mathrm{EqTimes} \rangle$. (Remarks: 1. f is the only nontrivial automorphism of the considered structure. 2. We can define the set $\{-1, 1\}$ (as a unary relation), but we cannot distinguish the element 1.) □

4. Auxiliary results about Pascal's triangles modulo n

Here we shall present some notions and results useful for the next section. The results will be given without proofs; they are either classical or easy or contained in [Bo90] or [Ko93]. We shall start with n-adic masking relation for arbitrary $n > 1$, although it is closely related to Pascal's triangle modulo n only for n prime. If a number $x \in \mathbb{N}$ is given by its n-adic digits $a_r, a_{r-1}, \dots, a_0$ we shall write $x = [a_r a_{r-1} \dots a_0]_n$. Leading zeros are allowed if necessary (e. g., to obtain equal numbers of digits in two integers). For $x = [a_r \dots a_1 a_0]_n$, $y = [b_r \dots b_1 b_0]_n$ we shall write $x \sqsubseteq_n y$ if it holds $a_i \le b_i$ for all $i = 0, 1, \dots, r$. The relation $\sqsubseteq_n$ will be called *n-adic masking relation.*

Claim 4.1. *For every integer* $n > 1$ *the relation* $\sqsubseteq_n$ *is a partial order on the set* $\mathbb{N}$. *In the structure* $L = \langle \mathbb{N}; \sqsubseteq_n \rangle$ *we can define:*

$x \sqsubset_n y$	*proper masking relation;*
$x \sqcap_n y$	*meet operation in L;*
$x \sqcup_n y$	*join operation in L;*
0	*the constant* 0 *(zero) as the smallest element of L;*
$\mathrm{Pow}_p(x)$	*x is a power of p;*
$\mathrm{CFAdd}_p(x, y, z)$	*carry-free addition: $x + y = z$, and no carry occurs when $x + y$ is computed.*

The structure $\langle \mathbb{N}; \sqcup_n, \sqcap_n \rangle$ *is a distributive lattice with the smallest element* 0.

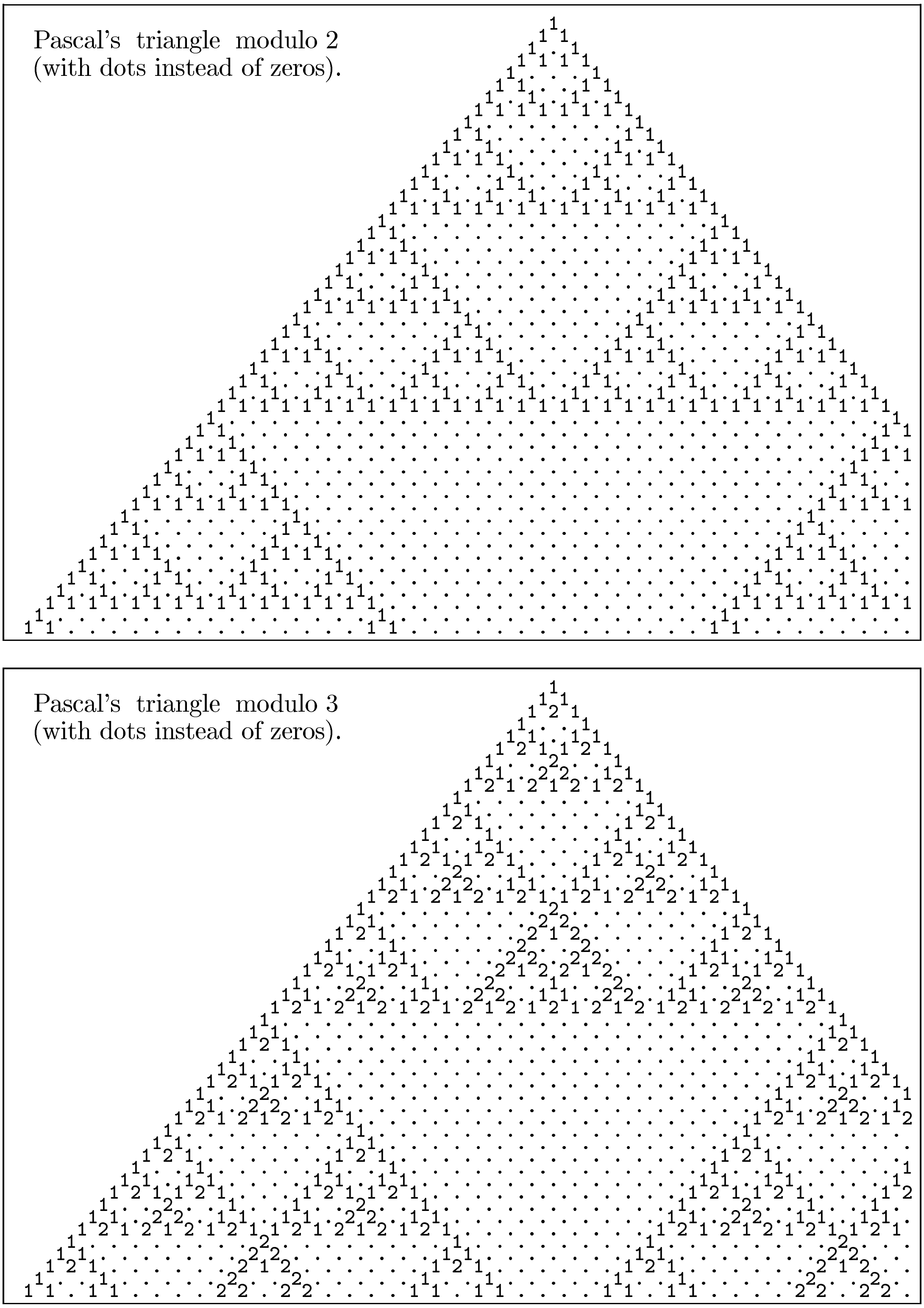
Figure 4 contains Pascal's triangles modulo 2 and modulo 3. The coordinate system with the axes oriented right downward and left downward is used, and the elements 0 are replaced by dots. (The same system is used in further figures, too.) We can see their rather simple "fractal" structure, which is common for all Pascal's triangles modulo prime numbers. A very useful tool in investigating them is Lucas' theorem, see e. g. [Bo90]. We shall give it in a slightly modified form, with $\binom{x+y}{x}$ instead of $\binom{x}{y}$.

Theorem 4.2. *If* n *is a prime and*

$$x = [a_r \dots a_1 a_0]_n, \qquad y = [b_r \dots b_1 b_0]_n \tag{4.2.1}$$

then

$$\binom{x+y}{x} \equiv \binom{a_0 + b_0}{a_0} \cdot \binom{a_1 + b_1}{a_1} \cdot \ldots \cdot \binom{a_r + b_r}{a_r} \pmod{n}. \tag{4.2.2}$$



Pascal's triangle modulo 2
(with dots instead of zeros).

Pascal's triangle modulo 3
(with dots instead of zeros).

Figure 4.

Corollary 4.3. *For n, x, y as in Theorem 4.2 we have*

$$B_n(x,y) = 0 \ \text{ if and only if } \ a_i + b_i \geq n \text{ for some } i \in \{0, 1, \ldots, r\}.$$

Theorem 4.4. *For every prime n the relation $\sqsubseteq_n$ is first order definable in the structure $\langle \mathbb{N}; B_n \rangle$.*

Proof. The defining formula can be

$$x \sqsubseteq_n y \iff \forall z \big(B_n(x,z) = 0 \implies B_n(y,z) = 0 \big). \tag{4.4.1}$$

To prove that, some considerations about n-adic digits must be done and Corollary 4.3 applied. □

Claim 4.5. *For every prime n and $x, y, e \in \mathbb{N}$, the integer $\binom{x+y}{x}$ is divisible by n^e if and only if at least e carries occur in the addition of x, y in n-adic number system.*

For the proof binomial coefficients must be expressed by factorials, and the exponents of n in factorizations of the factorials ought to be computed.

5. Definability of Pascal's triangles modulo n

Now we shall investigate definability of the operations B_n (i.e., Pascal's triangles modulo n) from their associated equivalence relations EqB_n defined by

$$\mathrm{EqB}_n = \big\{ (x,y,u,v) \in \mathbb{N}^4 \mid B_n(x,y) = B_n(u,v) \big\}.$$

In the present paper we shall consider only few small values of n.

Let us define $VB_n(x) = \big\{ B_n(x,y) \mid y \in \mathbb{N} \big\}$ and let $\mathrm{CVB}_n^k(x)$ mean that $\mathrm{card}(VB_n(x)) = k$. The functions VB_n cannot be (first order) defined in $\langle \mathbb{N}; B_n \rangle$ simply because their values are *subsets* of $\mathbb{N}$, and not elements of $\mathbb{N}$. However, the predicates CVB_n^k (for $1 \leq k \leq n$) can be defined:

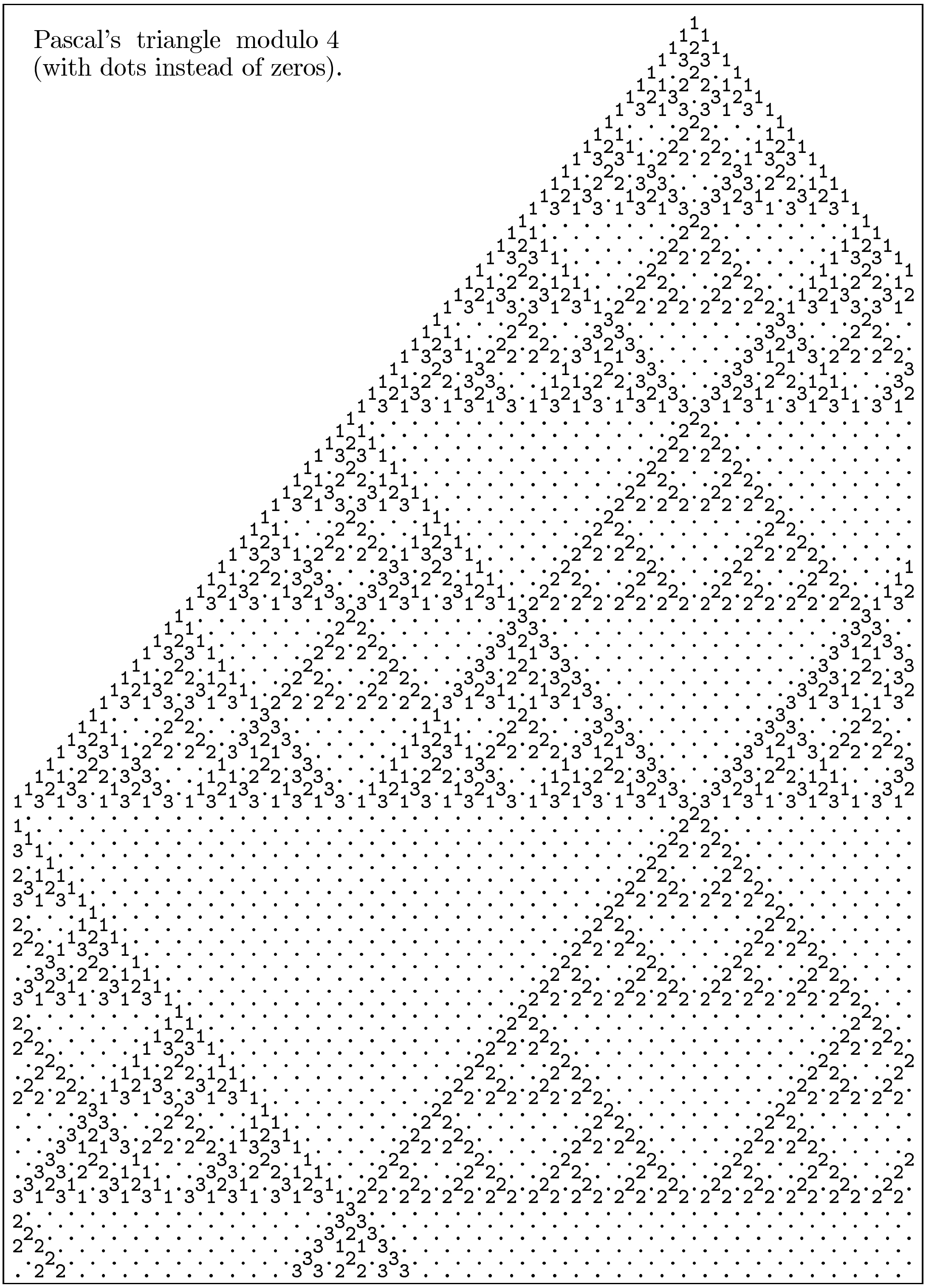
$$\begin{aligned} \mathrm{CVB}_n^k(x) \iff & \exists y_1, \ldots, y_k \bigwedge_{i=2}^{k} \bigwedge_{j=1}^{i-1} \neg\, \mathrm{EqB}_n(x, y_i, x, y_j) \wedge \\ & \wedge \forall y_1, \ldots, y_{k+1} \bigvee_{i=2}^{k+1} \bigvee_{j=1}^{i-1} \mathrm{EqB}_n(x, y_i, x, y_j); \end{aligned}$$

for $k = 1$ the first member no the right can be deleted. Further, let $\mathrm{EB}_n^{i_1 \cdots i_k}(x,y)$ mean $B_n(x,y) \in \big\{ i_1, \ldots, i_k \big\}$. In particular, let $\mathrm{EB}_n^i(x,y)$ mean $B_n(x,y) = i$.

Now we shall investigate Pascal's triangle modulo 4; its structure is more complicated than that of B_2 but there is an obvious relationship between them; it is expressed by the formula $B_2(x,y) = B_4(x,y) \operatorname{MOD} 2$. The function B_4 is displayed in Figure 5.

Theorem 5.1. *The operation B_4 (Pascal's triangle modulo 4) is first order definable in the structure $\langle \mathbb{N}; \mathrm{EqB}_4 \rangle$, where EqB_4 is the equivalence relation associated to B_4.*

Proof. Pascal's triangle modulo 4 is displayed in Figure 2. We can see that it contains only 1's on its margin (i.e. for $x = 0$ or $y = 0$) and (with exception on the top) only even



Pascal's triangle modulo 4
(with dots instead of zeros).

Figure 5.

elements on its axis. The first property is obvious. The second one can be easily proved from Lucas' Theorem (used for the modulus 2 and $x = y$). Therefore we can define

$$\begin{aligned} x = 0 &\iff \forall y, z\, \mathrm{EqB}_4(x, y, x, z), \\ \mathrm{EB}_4^1(x, y) &\iff \mathrm{EqB}_4(x, y, 0, 0), \\ \mathrm{EB}_4^{02}(x, y) &\iff \exists z\bigl(z \neq 0 \wedge \mathrm{EqB}_4(x, y, z, z)\bigr). \end{aligned}$$

The formula $\mathrm{EB}_4^{02}(x, y)$ obviously corresponds to $B_2(x, y) = 0$. Therefore we can define the masking relation $\sqsubseteq_2$ by a formula similar to (4.4.1) as follows:

$$x \sqsubseteq_2 y \iff \forall z\bigl(\mathrm{EB}_4^{02}(x, z) \implies \mathrm{EB}_4^{02}(y, z)\bigr).$$

The structure $\langle \mathbb{N}; \sqsubseteq_2 \ \rangle$ is a partially ordered set with the smallest element 0; we can consider it as a distributive lattice in the usual way (see Claim 4.1); let the lattice operations be $\sqcup_2$, $\sqcap_2$. We can define the set Pow_2 as the set of atoms of the lattice. Further we can define

$$\begin{aligned} \mathrm{EB}_4^2(x, y) &\iff \exists z\bigl(\mathrm{Pow}_2(z) \wedge \mathrm{EqB}_4(x, y, z, z)), \\ \mathrm{EB}_4^0(x, y) &\iff \mathrm{EB}_4^{02}(x, y) \wedge \neg\, \mathrm{EB}_4^2(x, y), \\ \mathrm{EB}_4^3(x, y) &\iff \neg\, \mathrm{EB}_4^{02}(x, y) \wedge \neg\, \mathrm{EB}_4^1(x, y). \end{aligned}$$

Now we shall use that $B_4(2^x, 2^x + 2^y) = 0$ only if $y = x + 1$; indeed, only in this case two carries occur in the addition of 2^x and $2^x + 2^y$ (in binary number system; see Claim 4.5). This enables us to define the constants 1, 2, 3. (We could also define addition, but we need not that now.)

$$\begin{aligned} x = 1 &\iff \mathrm{Pow}_2(x) \wedge \forall y\bigl(\mathrm{Pow}_2(y) \implies \mathrm{EB}_4^2(y, x \sqcup_2 y)\bigr), \\ x = 2 &\iff \mathrm{Pow}_2(x) \wedge \mathrm{EB}_4^0(1, x \sqcup_2 1)\bigr), \\ 3 &= 1 \sqcup_2 2. \end{aligned}$$

Finally, the function B_4 can be defined by

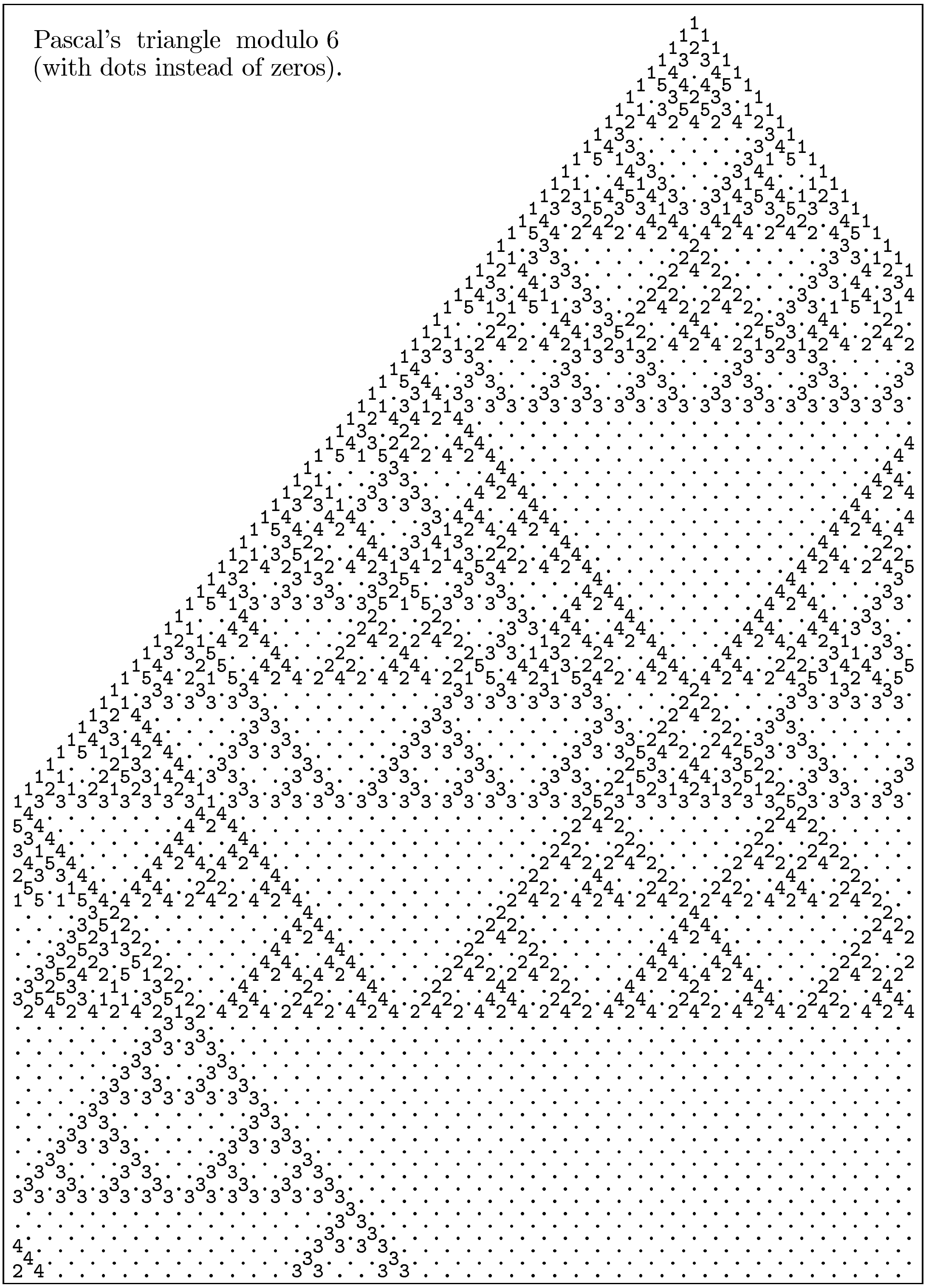
$$z = B_4(x, y) \iff z = 0 \wedge \mathrm{EqB}_4(x, y, 1, 3) \vee \bigvee_{i=1}^{3} \bigl(z = i \wedge \mathrm{EqB}_4(x, y, 1, i - 1)\bigr),$$

and the proof is finished. □

Now we shall deal with Pascal's triangle modulo 6; it is displayed in Figure 6. Notice that B_6 is connected with B_2 and B_3 by the formulas

$$B_2(x, y) = B_6(x, y) \,\mathrm{MOD}\, 2, \qquad B_3(x, y) = B_6(x, y) \,\mathrm{MOD}\, 3.$$

They obviously enable us to compute the values of B_2 and B_3. However, since 2, 3 are relatively prime we can also compute the values of B_6 from the values of B_2 and B_3. We can also use results about rather simple B_2, B_3 in the investigation of B_6.



Pascal's triangle modulo 6
(with dots instead of zeros).

Figure 6.

Theorem 5.2. *The operation B_6 (Pascal's triangle modulo 6) is first order definable in the structure $\langle \mathbb{N}; \mathrm{EqB}_6 \rangle$, where EqB_6 is the equivalence relation associated to B_6.*

Proof. For every $x \in \mathbb{N}$ we have $VB_6(x) = \{1\}$, $VB_6(x) = \{0,1,2,3,4,5\}$ or $VB_6(x) = \{0,1,3,4\}$. The second case is the most frequent. The first case takes place only for $x = 0$. The third case takes place for those $x > 0$ which have no 1's in their 3-adic expansion. Indeed, congruence considerations show that $VB_6(x) = \{0,1,3,4\}$ is equivalent with the conjunction of $VB_2(x) = \{0,1\}$ and $VB_3(x) = \{0,1\}$. For $x > 0$ the first condition is always satisfied, hence it need not be considered. For the second condition we have to use Lucas' theorem for $n = 3$, and that $B_3(2,a) \in \{0,1\}$ for every $a \in \{0,1,2\}$.

Using the above facts we can define:

$$\begin{aligned}
x = 0 &\iff \forall y, z\, \mathrm{EqB}_6(x,y,x,z),\\
\mathrm{EB}_6^1(x,y) &\iff \mathrm{EqB}_6(x,y,0,0),\\
\mathrm{EB}_6^{024}(x,y) &\iff \exists z\big(z \neq 0 \wedge \mathrm{EqB}_6(x,y,z,z)\big),\\
\mathrm{EB}_6^{0134}(x,y) &\iff \exists u,v\big(\,\mathrm{CVB}_6^4(u) \wedge \mathrm{EqB}_6(x,y,u,v)\big),\\
\mathrm{EB}_6^{0}(x,y) &\iff \exists u\big(\,\mathrm{CVB}_6^4(u) \wedge \mathrm{EqB}_6(x,y,u,u)\big),\\
\mathrm{EB}_6^{03}(x,y) &\iff \mathrm{EB}_6^{0134}(x,y) \wedge \big(\mathrm{EB}_6^{0}(x,y) \vee \neg\, \mathrm{EB}_6^{024}(x,y)\big) \wedge \neg\, \mathrm{EB}_6^{1}(x,y).
\end{aligned}$$

(The meaning of the defined predicates was explained above; now we have to check that these defining formulas correspond to the intended meaning. It is not difficult.)

The formulas $\mathrm{EB}_6^{024}(x,y)$ and $\mathrm{EB}_6^{03}(x,y)$ obviously correspond to $B_2(x,y) = 0$ and $B_3(x,y) = 0$. Therefore we can define the masking relations for the bases 2, 3 as follows:

$$\begin{aligned}
x \sqsubseteq_2 y &\iff \forall z\big(\,\mathrm{EB}_6^{024}(x,z) \implies \mathrm{EB}_6^{024}(y,z)\big),\\
x \sqsubseteq_3 y &\iff \forall z\big(\,\mathrm{EB}_6^{03}(x,z) \implies \mathrm{EB}_6^{03}(y,z)\big),
\end{aligned}$$

Now we could use the result of [Ko93] that for distinct primes p, q the operations $+$, $\times$ are definable in $\langle \mathbb{N}; \sqsubseteq_p, \sqsubseteq_q \rangle$. Then all arithmetical operations and relations, hence B_6, too are definable in such structures. However, we shall use a more elementary consideration.

Using $\sqsubseteq_2$ we can define Pow_2 and $\sqcup_2$. Using $\sqsubseteq_3$ we can define Pow_3 and $\sqcup_3$. Further we can define

$$\begin{aligned}
&x = 1 \iff \mathrm{Pow}_2(x) \wedge \mathrm{Pow}_3(x),\\
&x = 2 \iff 1 \sqsubseteq_3 x \wedge x \neq 1 \wedge \forall y\big(y \sqsubseteq_3 x \implies y \sqsubseteq_3 1 \vee y = x\big),\\
&\quad 3 = 1 \sqcup_2 2, \qquad 4 = 1 \sqcup_3 3, \qquad 5 = 2 \sqcup_3 3.
\end{aligned}$$

If we have the constant $0, 1, \ldots, 5$ we can define B_6 as follows:

$$z = B_6(x,y) \iff z = 0 \wedge \mathrm{EqB}_6(x,y,1,5) \vee \bigvee_{i=1}^{5} \big(z = i \wedge \mathrm{EqB}_6(x,y,1,i-1)\big). \quad \square$$

Corollary 5.3. *The operations* $+$, $\times$ *are first order definable in the structure* $\langle \mathbb{N}; \mathrm{EqB}_6 \rangle$, *where* EqB_6 *is the equivalence relation associated to* B_6.

In the corollary we cannot replace 6 by 4 because multiplication is not definable in $\langle \mathbb{N}; B_4 \rangle$; moreover, the elementary theory of $\langle \mathbb{N}; \mathrm{EqB}_4 \rangle$ is decidable.

In the theorems we cannot replace 6 (or 4) by any other positive integer $n \leq 6$. The function B_1 is a constant function (with the value 0), hence $\mathrm{EqB}_1 = \mathbb{N}^4$ is trivial, and we cannot define neither 0 nor B_1 in the structure $\langle \mathbb{N}; \mathrm{EqB}_4 \rangle$. The other cases are covered by the next theorem.

Theorem 5.4. *If* n *is prime then* B_n *is not definable in* $\langle \mathbb{N}; \mathrm{EqB}_n \rangle$.

Proof. Let n be prime. Every permutation of the set Pow_p induces an automorphism of the structure $\langle \mathbb{N}; \mathrm{EqB}_n \rangle$. However, only permutations which preserve 1 induce automorphisms of $\langle \mathbb{N}; B_n \rangle$. In particular, the mapping $f : \mathbb{N} \to \mathbb{N}$ defined by

$$f(xn^2 + yn + z) = xn^2 + zn + y \quad \text{for all} \quad x \in \mathbb{N},\ 0 \leq y < n,\ 0 \leq z < n$$

is an automorphism of $\langle \mathbb{N}; \mathrm{EqB}_n \rangle$, but it is not an automorphism of $\langle \mathbb{N}; B_n \rangle$. (The corresponding permutation interchanges 1 and n, and preserves the other powers of n.) Therefore B_n cannot be definable in $\langle \mathbb{N}; \mathrm{EqB}_n \rangle$. □

Remarks. 1. The proof of Theorem 5.4 shows the unique reason of non-definability of B_n in $\langle \mathbb{N}; \mathrm{EqB}_n \rangle$. In the structure $\langle \mathbb{N}; \mathrm{EqB}_n, 1 \rangle$ the function B_n is definable.

2. The relation $\sqsubseteq_n$ is definable in $\langle \mathbb{N}; \mathrm{EqB}_n \rangle$. Conversely EqB_2 is definable in $\langle \mathbb{N}; \sqsubseteq_2 \rangle$. However, if n is an odd prime then EqB_n is not definable in $\langle \mathbb{N}; \sqsubseteq_n \rangle$.

References

[Be94] A. Bès, *On Pascal triangles modulo a prime power*, Proceedings Logic Colloquium'94 (Annals of Pure and Applied Logic) (submitted 1994), 15pp.

[BK96] A. Bès — I. Korec, *Definability within structures related to Pascal triangles modulo an integer*, A manuscript (1996), 17pp.

[Bo90] B. A. Bondarenko, *Generalized Pascal triangles and pyramids, their fractals, graphs and applications (in Russian)*, "Fan", Tashkent, 1990.

[Ko90] I. Korec, *Pascal triangles modulo n and modular trellises*, Computers and Artificial Intelligence **9** (1990), 105-113.

[Ko93] ———, *Definability of arithmetic operations in Pascal triangle modulo an integer divisible by two primes*, Grazer Matematische Berichte **318** (1993), 53-62.

[Ko94] ———, *Structures related to Pascal's triangle modulo* 2 *and their elementary theories*, Mathematica Slovaca **44** (1994), no. 5, 531-554.

[Ko94a] ———, *Theories of generalized Pascal triangles*, Proceedings of the Logic Colloquium'94, Clermont-Ferrand, July 21–30, 1994 (submitted July 1994), 1-7.

[Ko95] ———, *Elementary theories of structures containing generalized Pascal triangles modulo a prime*, Discrete Mathematics and Applications, Blagoevgrad/Predel, Sept. 12-16, 1994 (S. Shtrakov and Iv. Mirchev, eds.), Blagoevgrad, 1995, pp. 91-102.

[Ko95a] ———, *Theories of generalized Pascal triangles (Abstract)*, Bulletin of the Association for Symbolic Logic **1** (1995), no. 2, 214-215.

[Mo76] J. D. Monk, *Mathematical logic*, Springer Verlag, New York, 1976.

(Received October 11, 1996)

Mathematical Institute
Slovak Academy of Sciences
Štefánikova 49
814 73 Bratislava
SLOVAKIA

E-mail address: korec@savba.sk