Mathematical Institute
Slovak Academy of Sciences, Bratislava

Preprint 18/1996

Ivan Korec

Undecidability and uniform definability in classes of structures related to Pascal's triangles modulo n

June 24, 1996

PREPRINT SERIES

UNDECIDABILITY AND UNIFORM DEFINABILITY IN CLASSES OF STRUCTURES RELATED TO PASCAL'S TRIANGLES MODULO n

Ivan KOREC, Bratislava

Abstract. Classes of structures containing $B_n(x,y) = \binom{x+y}{x} \mod n$ or related relations are considered. Definability of usual arithmetical operations and operations modulo n in such classes is investigated. Further, for every infinite set X of positive integers the elementary theory of the class $\{\langle \mathbb{N}; B_n \rangle \mid n \in X\}$ is shown to be undecidable (although it may happen that every its element has decidable theory).

1. Introduction

Let $\mathbb{N}$ denote the set of nonnegative integers, let $\mathbf{s}$ denote the successor, and $\mathbb{N}_n = \{0, 1, \dots, n-1\}$. Let $\mathbb{P}$ be the set of primes, Pow_n the set of powers of n, let $\mid$ be the divisibility relation, $\oplus_n$, $\otimes_n$ the arithmetical operations modulo n. Let DIV, MOD denote the quotient and the remainder by integer division, and let $B_n(x,y) = \binom{x+y}{x} \,\mathrm{MOD}\, n$; the latest function will be called Pascal's triangle modulo n. Some further symbols, e.g. $\leq$, $+$ will be used in their usual meaning; $\leq_M$ will denote the restriction of the usual order to M. The p-adic expansion of an integer will be denoted by $[x_k \dots x_1 x_0]_p$. Some special symbols will be introduced later.

Definability and decidability results proved before for unique structures containing B_n will be extended for classes of such structures. (Of course, it is not always possible). Our classes will be parametrized by an integer n ranging over a set $X \subseteq \mathbb{N} \setminus \{0, 1\}$. A structure will be associated to every value $n \in X$ (in a uniform way); its signature may not depend on n. Most of considered structures will have the base set $\mathbb{N}$; therefore e.g. $\oplus_n$ and $\otimes_n$ will be sometimes extended to $\mathbb{N}$.

We shall use a usual language of first order logic with equality, including commonly used abbreviations, e. g. relativized quantifiers. The meaning of a nonlogical symbol will be usually fixed, up to it dependence on n or other integer parameter. The nonlogical symbols will be chosen rather freely; for example, some composed expressions containing n will be used for constants. Syntax of the expression will remember the meaning of the constant, but the expression is formally not decomposable. Similarly we work with relations and functions. So for example Pow_n will denote the unary relation (or predicate) "to be a power of n".

2. Auxiliary results about Pascal's triangles modulo n

We shall use Lucas Theorem which says (slightly reformulated) that for every prime p and $x = [x_k x_{k-1} \dots x_1 x_0]_p$, $y = [y_k y_{k-1} \dots y_1 y_0]_p) \in \mathbb{N}$ we have

$$B_p(x,y) \equiv B_p(x_k, y_k) \cdot \ldots \cdot B_p(x_1, y_1) \cdot B_p(x_0, y_0) \pmod{p}.$$

This work was supported by Grant 2/1227 of Slovak Academy of Sciences.
1991 *Mathematics Subject Classification.* Primary 03F30, Secondary 05A10, 11B65.
Key words and phrases. Uniform definability, Undecidability, Pascal's triangle modulo n.

Another useful result is that the exponent of a prime p in the factorization of $\binom{x+y}{x}$ is equal to the number of carries in the addition of x, y in p-ary number system. (See e.g. [Bo].)

Now we shall prepare some results about the structure of the functions B_n ($n > 1$). Remember briefly a result of [K1]; the notion was introduced in [CG]. If n is a prime power then B_n is *modular*, more precisely, if $n = p^e$, p a prime, $e \geq 1$, then B_n is a fixed point of an $\big((\frac{n}{p}, \frac{n}{p}), (n, n)\big)$-substitution. It means the following. For every $m > 0$ we can cut B_n into $m \times m$ array words in the alphabet $\mathbb{N}_n$; let $W_n(m, x, y)$ be the word with the top element $B_n(mx, my)$. (We imagine B_n displayed with $B_0, 0)$ at the top.) Then for $m = p^{e-1}$ and all $x, y \in \mathbb{N}$ we have

$$(2.1) \qquad W_n(m, x, y) = W_n(m, x, y) \implies W_n(pm, x, y) = W_n(pm, x, y).$$

(Notice that the formula holds also for every $m = p^k$, $k \geq e - 1$.) The formula (1.1) induces a mapping of a set of $m \times m$ array words into a set $\pm \times pm$ array words which induces the *array substitution* mentioned above. The whole B_n can be obtained by iterating this array substitution starting from $W_n(m, 0, 0)$. This enables us to study the structure of B_n. For $e = 1$ (i.e. n prime) we have in essential only symbols from $\mathbb{N}_n$ on the left-hand side of 2.1; in this case we obtain a *uniform array morphism*, and B_n is *strictly modular*; the iteration can start from the unique symbol 1.

Let us define

$$Ones_n(x) = \begin{cases} \text{the least } y \text{ such that } B_n(x, y) \neq 1 & \text{if } \; x > 0 \\ 0 & \text{if } \; x = 0. \end{cases}$$

Informally, $Ones_n(x)$ (for $x > 0$) is the number of starting ones in the xth diagonal of x. (Diagonals of a GPT were defined to be parallel with margins; now we need not distinguish left and right diagonals because all B_n are commutative.) The function $Ones_n$ can be used to express the period of xth diagonal of B_n; this period is

$$Per_n(x) = \text{ the least } y \text{ such that } \quad Ones_n(y) \geq x.$$

If $n = p_1^{e_1} \dots p_s^{e_s}$ is the factorization of $n > 1$ then B_n can be imagined as a superposition (or "a direct product") of B_{n_i}, $i = 1, ..., s$, where $n_i =_i^{e_i}$. More precisely, the values $B_{n_i}(x, y)$ for distinct i are independent on each other, and together they uniquely determine the value $B_n(x, y)$ (by Chinese Remainder Theorem). From that we can obtain:

Lemma 2.1. (i) If p is a prime and $e \geq 1$ then for every integer $x > 0$ we have

$$Ones_{p^e}(x) = p^{k+e-1}, \qquad\qquad Per_{p^e}(x) = p^{e + \lfloor \log_p x \rfloor}$$

where k is the greatest integer such that $p^k | x$. (Notice that $Per_{p^e}(0) = 1$, and by definition $Ones_{p^e}(0) = 0$.) Further, for every integer $k \geq e - 1$ we have

$$(2.1.1) \qquad\qquad \big\{B_{p^e}(xp^k, p^k) \mid x \in \mathbb{N}_{p^e}\big\} = \mathbb{N}_{p^e}.$$

(ii) If $n = p_1^{e_1} \dots p_s^{e_s}$ is the factorization of $n > 1$ and $n_i = p_i^{e_i}$ for $i = 1, \dots, s$ then for all $x \in \mathbb{N}$

$$\begin{aligned} Ones_n(x) &= \min\big(\, Ones_{n_1}(x), \dots, Ones_{n_s}(x)\big), \\ Per_n(x) &= Per_{n_1}(x) \cdot \ldots \cdot Per_{n_s}(x). \end{aligned}$$

(iii) For every $n > 1$ the range of $Ones_n$ consists of 0 and all powers of prime divisors of n:

$$\{\, Ones_n(x) \mid x > 0 \,\} = \{ p^e \mid p \in \mathbb{P} \wedge p|n \wedge e \in \mathbb{N} \}.$$

Sketch of proof. All results can be easily obtained , and are not new in essential. We present only a remark to the proof of (2.2.1). The inclusion $\subseteq$ is obvious; hence it suffices to show that the mapping $x \mapsto B_{p^e}(xp^k, p^k)$ is injective. If it is not then the period of the p^kth diagonal of B_{n^e} would be less than the formula in (i) says. $\square$

Theorem 2.2. *If $n > 1$ and p is a prime then*

$$\{ B_n(nx + p - 1, ny + 1) \mid x, y \in \mathbb{N} \} = \begin{cases} \{ x \in \mathbb{N}_n \mid p|x \} & \textit{if } p|n, \\ \mathbb{N}_n & \textit{if } p \nmid n. \end{cases} \tag{2.2.1}$$

Proof. The inclusion $\subseteq$ can be proved easily; for $p \nmid x$ it is obvious, for $p|n$ Lucas theorem can be applied: We have $B_p(p-1, 1) = 0$, hence $B_p(nx+p-1, ny+1) = 0)$, and then $B_n(nx + p - 1, ny + 1) \equiv 0 \pmod p$. It remains to show the inclusion $\supseteq$.

Let $n = p_1^{e_1} \dots p_s^{e_s}$ be the factorization of $n > 1$ and $n_i = p_i^{e_i}$ for $i = 1, \dots, s$. let r be an element of the right-hand side of (2.2.1) (i.e., $r \in \mathbb{N}_n$, and if $p = p_i$ then $p|r$).

Let us start with the case $s = 1$ (i.e., n is a prime power). Then we can use Lemma 2.2. Let us choose a sufficiently large power m of p_1 so that $m \geq n$ and

$$B_n(mx - i, my + i) = 0 \ \text{ for all } i,\ 1 < |i| < p \text{ and } x > 0,\ y > 0.$$

Then we have

$$B_n(mx + p - 1, my + 1) \equiv B_n(mx, my) \cdot B_n(p - 1, 1) \pmod n.$$

If $p \neq p_1$ then $B_n(p - 1, 1)$, n are relatively prime. If $p = p_1$ then $B_n(p - 1, 1) = p$; however, in this case $p|r$. Hence in both cases there is $u \in B_n$ such that $u \cdot B_n(p - 1, 1) \equiv r \pmod n$. It remains to find x, y such that $B_n(x, y) = u$; this is possible (even with $y = 1$) by (2.1.1).

Now let $s > 1$. By (2.2.1) applied for prime powers moduli n_i for every $i = 1, \dots, s$ there are positive integers a_i, b_i such that

$$a_i \equiv p - 1 \pmod{n_i}, \qquad b_i \equiv 1 \pmod{n_i}, \qquad B_{n_i}(a_i, b_i) = r \,\mathrm{MOD}\, n_i$$

for $i = 1, \dots, s$. Let q_i be the least power of p_i greater than a_i, b_i, and n_i (here and below again for $i = 1, \dots, s$). Then for every $z_i \in \mathbb{N}$ we have

$$B_{n_i}(a_i + z_i q_i, b_i) = B_{n_i}(a_i, b_i) = r \,\mathrm{MOD}\, n_i.$$

Since $B_n(x, b_i) \equiv B_{n_i}(a_i, b_i) \pmod{n_i}$ we obtain

$$x \equiv a_i \pmod{q_i} \quad \Longrightarrow \quad B_n(x, b_i) \equiv r \pmod{n_i}.$$

By Chinese remainder theorem there is x which satisfies all s required congruences; then obviously also $x \equiv p - 1 \pmod n$ holds. Now let Q_i be the least power of p_i which is greater than x, b_i, and n_i. Similarly as above we can obtain

$$y \equiv b_i \pmod{Q_i} \quad \Longrightarrow \quad B_n(x, y) \equiv r \pmod{n_i}.$$

Again, there is y which satisfies all s required congruences. Then we also have $y \equiv 1 \pmod n$, and the congruences for $B_n(x, y)$ give $B_n(x, y) = r$. $\square$

3. UNIFORM DEFINABILITY BY PRIME MODULI

We start with this special case because it is substantially simpler than the case of general moduli, and because the general case will be often reduced to the case of prime moduli.

The following lemma summarizes some older results; they were originally obtained for usual (i.e., not uniform) definability, but the defining formulas need not be changed in essential. The meaning of most symbols is usual; when necessary, a short explanation is given (either in the lemma or in the proof). Now notice only that $\mathbf{cs}_p$ and $\overline{\mathbf{s}}_p$ will replace the successor $\mathbf{s}$ (which is not definable); $\overline{\mathbf{s}}_p$ coincides with $\mathbf{s}$ as much as possible.

Lemma 3.1. *The following relations and functions are uniformly definable in the class* $\{\langle \mathbb{N}; B_p\rangle \mid p \in \mathbb{P}\}$:

(1) *Constants* 0, 1, $\lceil p-1\rceil$.
(2) *Binary relations* $\sqsubseteq_p$ *(p-ary masking relation),* $\sqsubset_p$, $\prec_p$ *(strict order and covering relation associated to* $\sqsubseteq_p$*),* $\leq_p$ *(usual order restricted to* $\mathbb{N}_p$*).*
(3) *Unary predicates* $p|x$, $x<p$, $x \geq p$, $\mathrm{Pow}_p(x)$.
(4) *Binary operations* $\sqcap_p$, $\sqcup_p$ *(lattice operations derived from* $\sqsubseteq_p$*).*
(5) *Unary operations* $\mathbf{cs}_p$ *(cyclic successor) and* $\overline{\mathbf{s}}_p$.

Proof. Using Lucas theorem we can define

$$x \sqsubseteq_p y \iff \forall z\big(B_p(x,z)=0 \implies B_p(y,z)=0\big);$$

Notice that $\langle \mathbb{N}; \sqsubseteq_p \rangle$ is a distributive lattice with the smallest element 0. Its atoms are powers of p. Therefore 0 and Pow_p are definable. Also $\sqcap_p$, $\sqcup_p$, $\sqsubset_p$, $\prec_p$ can be defined in the usual way; we show that only one for the latest relation:

$$x \prec_p y \iff x \sqsubset_p y \wedge \neg\exists z\big(x \sqsubset_p z \wedge z \sqsubset_p y\big).$$

The constant 1 can be defined as $B_p(0,0)$. (Notice that $\sqsubseteq_p$ do not suffice to define 1.) From now on, we shall use only $\sqsubseteq_p$ and 1. We can define

$$\begin{aligned}
p|x &\iff x \sqcap_p 1 = 0,\\
x<p &\iff \forall y\big(y \neq 0 \wedge y \sqsubseteq_p x \implies 1 \sqsubseteq_p y\big),\\
x \geq p &\iff \neg(x<p),\\
x \leq_p y &\iff x<p \wedge y<p \wedge x \sqsubseteq_p y,\\
y = \lceil p-1\rceil &\iff y<p \wedge \neg\exists z\big(z<p \wedge y \sqsubset_p z\big),\\
y = \mathbf{cs}_p(x) &\iff x \sqsubset_p \lceil p-1\rceil \wedge y<p \wedge x \prec_p y \vee \neg(x \sqsubset_p \lceil p-1\rceil) \wedge y=0,\\
\overline{\mathbf{s}}_p(x) &= x \sqcup_p \mathbf{cs}_p(x \sqcap_p \lceil p-1\rceil).
\end{aligned}$$

□

Theorem 3.2. *Addition and multiplication modulo p (extended by the value 0 to the whole* $\mathbb{N}$*) are uniformly definable in the class* $\{\langle \mathbb{N}; B_p\rangle \mid p \in \mathbb{P}\}$.

Proof. Addition modulo p can be defined by

$$\begin{aligned}
z = u \oplus_p v \iff \exists x,y\Big(&x \neq \overline{\mathbf{s}}_p(x) \wedge y \neq \overline{\mathbf{s}}_p(y) \wedge u = B_p\big(x, \overline{\mathbf{s}}_p(y)\big) \wedge\\
&\wedge v = B_p\big(\overline{\mathbf{s}}_p(x), y\big) \wedge z = B_p\big(\overline{\mathbf{s}}_p(x), \overline{\mathbf{s}}_p(y)\big)\Big) \vee\\
&\vee u<p \wedge v=0 \wedge z=u \vee u=0 \wedge v<p \wedge z=v \vee\\
&\vee (u \geq p \vee v \geq p) \wedge z=0.
\end{aligned}$$

The idea is to find u, v as neighbour elements in some row of B_p (displayed in the usual way); then z appears below them. Since we cannot use the usual successor $\mathbf{s}$ some cases must be considered separately. In the above formula the condition $x \neq \overline{\mathbf{s}}_p(x)$ arranges that $\overline{\mathbf{s}}_p(x) = x+1$, and similarly for y. Notice that necessary x, y can be chosen less than p^2.

Multiplication modulo p can be defined by the formula

$$z = x \otimes_p y \iff \exists u_1, u_2, v_1, v_2 \Big(u_1 < p \wedge u_2 < p \wedge p|v_1 \wedge p|v_2 \wedge x = B_p(u_1, u_2) \wedge \\ \wedge\, y = B_p(v_1, v_2) \wedge z = B_p(u_1 \sqcup_p v_1, u_2 \sqcup_p v_2) \Big).$$

Here Lucas theorem was applied; v_1, v_2 can be multiples of p less than p^2. $\square$

Theorem 3.3. *Addition $+$ on the set $\mathbb{N}$ is uniformly definable in the class* $\big\{ \langle \mathbb{N}; B_p, \mathbf{s} \rangle \mid p \in \mathbb{P} \big\}$.

Proof. The usual strict order of powers of p and the function $NextPow_p$ can be defined by the formulas

$$\begin{aligned} x <_{\mathrm{Pow}_p} y &\iff \mathrm{Pow}_p(x) \wedge \mathrm{Pow}_p(y) \wedge \exists z \big(y = \mathbf{s}(z) \wedge x \sqsubseteq_p z \big), \\ y = NextPow_p(x) &\iff x <_{\mathrm{Pow}_p} y \wedge \neg \exists z \big(x <_{\mathrm{Pow}_p} z \wedge z <_{\mathrm{Pow}_p} y \big) \vee \\ &\quad\ \vee \neg\, \mathrm{Pow}_p(x) \wedge y = 0. \end{aligned}$$

Notice that using of $\mathbf{s}$ in the definitions above cannot be avoided. From now on we shall use only $NextPow_p$, and not $\mathbf{s}$ directly.

In the definition of $+$ we shall express the process of addition in p-ary number system. Therefore we shall need the addition of p-ary digits with a carry. It is given in the following definition, where x, y are the input digits, w_1 is the input carry, z is the output digits and w_2 is the output carry.

$$\begin{aligned} \mathrm{DigAdd}_p(x, y, w_1, z, w_2) \iff\ & x < p \wedge y < p \wedge w_1 \leq_p 1 \wedge w_2 \leq_p 1 \wedge \\ & \wedge\, z = (x \oplus_p y) \oplus_p w_1 \wedge \\ & \wedge \big(w_2 = 1 \iff x \oplus_p y \sqsubset_p x \sqcup_p y\ \vee \\ & \qquad \vee\, x \oplus_p y = \lceil p-1 \rceil \wedge w_1 = 1 \big); \end{aligned}$$

Further, the function

$$Dig_p(u, v) = \lceil p-1 \rceil \oplus_p B_p(u, v)$$

will be useful. If u is a power of p then $Dig_p(u, v)$ is the p-ary digits of v in the order determined by (the exponent of) u. Indeed, if $u = p^e$ and $v = [v_k v_{k-1} \dots v_1 v_0]_p$ then by Lucas theorem

$$Dig_p(u, v) = \lceil p-1 \rceil \oplus_p B_p(u, v) = \lceil p-1 \rceil \oplus_p B_p(1, v_e) = \lceil p-1 \rceil \oplus_p (1 \oplus_p v_e) = v_e.$$

Now we can define

$$z = x + y \iff \exists w \forall u, v \Big(\mathrm{Pow}_p(u) \wedge v = NextPow_p(u) \implies \\ \implies \mathrm{DigAdd}_p \big(Dig_p(u, x), Dig_p(u, y), Dig_p(u, w), \\ Dig_p(v, z), Dig_p(v, w) \big) \Big).$$

Here w represents the carries which occur by the addition of x, y. $\square$

The following auxiliary notion will be used in the proof of Theorem 3.5; $r>1$ is a prime power, $r=p^e$ for some prime p and $e\geq 1$. Since p is determined by r it is not written as a subscript.

$$\begin{aligned}
M_r(x) =& \begin{cases} rx & \text{if } \operatorname{Pow}_p(x)\\ 0 & \text{otherwise,}\end{cases}\\
Red_r(x) =& \begin{cases} p^{u \operatorname{MOD} e} & \text{if } x=p^u, u\in\mathbb{N}\\ 0 & \text{if } \neg Pow_p(x),\end{cases}\\
\mathrm{RM}_r =& \big\{(x,y,z\in(\mathbb{N}_r\cap\operatorname{Pow}_p)^3 \mid xy=z\vee xy=rz\big\}.
\end{aligned}$$

The substantial property of Red_r and RM_r is that they enable us to choose the product of any two powers x, y of p from (at most) e consecutive powers of p. Indeed, Red_r is (the graph of) an associative binary operation on the set $\mathbb{N}_r\cap\operatorname{Pow}_p$. The corresponding semigroup is a homomorphic image of the multiplicative semigroup of powers of p, and Red_r is the homomorphism. So $Red_r(xy)$ is uniquely determined by $Red_r(x)$, $Red_r(y)$; the correct value can be read from RM_r.

As an example consider $r=8$; the set RM_8 is equal to

$$\big\{(1,1,1),(1,2,2),(1,4,4),(2,1,2),(2,2,4),(2,4,1),(4,1,4),(4,2,1),(4,4,2)\big\}.$$

We have e.g. $Red_8(16)=2$, $Red_8(32)=4$ and $Red_8(512)=1$. Notice that if r is prime (i.e. $e=1$) then $\mathrm{RM}_r=\big\{(1,1,1)\big\}$, and also Red_r is trivial.

Lemma 3.4. *The operation Red_r and the relation RM_r are uniformly definable in the class $\big\{\langle\mathbb{N};B_p,+,M_r\rangle \mid p\in\mathbb{P}\wedge r=p^e, e\geq 1\big\}$.*

Proof. We can (define and) use $\leq$, $<$, 1, $r=M_r(1)$ and other symbols introduced above. Further we shall us the idea of coding of finite sets of powers of p by their sums. The integer w below codes the set $\big\{y,ry,r^2y,\ldots,x\big\}$.

$$\begin{aligned}
y=Red_r(x) \iff & \neg\operatorname{Pow}_p(x)\wedge y=0\vee\\
&\vee\operatorname{Pow}_p(x)\wedge\operatorname{Pow}_p(y)\wedge y<r\wedge\\
&\wedge\forall w\Big(\forall z\big(\operatorname{Pow}_p(z)\wedge z\neq x\wedge z\sqsubseteq_p w \implies M_r(z)\sqsubseteq_p w\big)\wedge\\
&\qquad\wedge y\sqsubseteq_p w\implies x\sqsubseteq_p w\Big).
\end{aligned}$$

To define RM_r we have to code subsets of $(\mathbb{N}_r\cap\operatorname{Pow}_p)^2$; they will be coded by pairs of integers. We define

$$\begin{aligned}
\mathrm{Code}_r(w_1,w_2,x,y) \iff \exists z,u,v\Big(&Red_r(z)=1\wedge u\sqsubseteq_p w_1\wedge v\sqsubseteq_p w_2\wedge\\
&\wedge z\leq u\wedge u<M_r(z)\wedge z\leq v\wedge v<M_r(z)\wedge\\
&\wedge Red_r(u)=x\wedge x\neq 0\wedge Red_r(v)=y\wedge y\neq 0\Big);
\end{aligned}$$

The intended meaning of the above is: the pair (x,y) belongs to the set associated to (w_1,w_2). Now we can define

$$\begin{aligned}
\mathrm{RM}_r(x,y,z) \iff \forall w_1,w_2\Big(&\forall u,v\big(\mathrm{Code}_r(w_1,w_2,NextPow_p(u),v)\implies\\
&\implies\mathrm{Code}_r(w_1,w_2,u,Red_r(NextPow_p(v)))\big)\wedge\\
&\wedge\mathrm{Code}_r(w_1,w_2,x,y)\implies\mathrm{Code}_r(w_1,w_2,1,z)\Big).
\end{aligned}$$

To explain the formula, notice that the expressed assumptions on the set Y coded by (w_1, w_2) are:

(1) If $(pu, v) \in Y$ then $(u, Red_r(pv)) \in Y$. ($Red_r(pv)$ is either pv or 1.)
(2) $(x, y) \in Y$.

The conclusion is $(1, z) \in Y$. If Y is minimal then $Red_r(u, v)$ is the same for all $(u, v) \in Y$, and hence $Red_r(x, y) = Red_r(1, z) = z$. $\square$

Theorem 3.5. *The operations* $+$, $\times$ *on* $\mathbb{N}$ *are uniformly definable in the class* $\{\langle \mathbb{N}; B_p, B_q\rangle \mid p, q$ *distinct primes*$\}$.

Proof. We can define Pow_p, Pow_q (and further symbols, with subscripts p, q) like in Lemma 3.1, and then Then we can define $\overline{\mathbf{s}}_q$. Since $\overline{\mathbf{s}}_q$ coincide with $\mathbf{s}$ on the predecessors of powers of p we can define

$$x <_{\mathrm{Pow}_p} y \iff \mathrm{Pow}_p(x) \wedge \mathrm{Pow}_p(y) \wedge \exists z\big(y = \overline{\mathbf{s}}_q(z) \wedge x \sqsubseteq_p z\big).$$

Now we can define $+$ like in the previous theorem. After that we can (define and) freely use $<$, $\leq$ etc. In particular, we can use the predecessor function which will be denoted $x - 1$ (with $0 - 1 = 0$).

To define $\times$, we shall gradually define some subsets of the multiplication considered as a ternary relation.

The multiplication of powers of p by powers of q can be defined by

$$\begin{aligned}\mathrm{Mult}^1_{p,q}(x, y, z) \iff{}& \mathrm{Pow}_p(x) \wedge \mathrm{Pow}_q(y)\wedge \\ &\wedge z > 0 \wedge z \sqcap_p (x-1) = 0 \wedge z \sqcap_q (y-1) = 0\wedge \\ &\wedge \forall w\big(w > 0 \wedge w \sqcap_p (x-1) = 0 \wedge w \sqcap_q (y-1) = 0 \implies \\ &\qquad\qquad\qquad\qquad\qquad\qquad \implies z \leq w\big).\end{aligned}$$

To define multiplication among powers of p we shall a first define the unary operation M_r, where r is the least power of p greater than q.

$$\begin{aligned}y = M_r(x) \iff{}& \neg\,\mathrm{Pow}_p(x) \wedge y = 0\vee \\ &\vee \exists u, v\big(\mathrm{Mult}^1_{p,q}(x, q, u) \wedge \mathrm{Mult}^1_{p,q}(\mathit{NextPow}_p(x), q, v)\wedge \\ &\qquad\qquad \wedge \mathrm{Pow}_p(y) \wedge u < y \wedge y < v\big)\end{aligned}$$

Now we can define Red_r and RM_r by Lemma 3.4. (For $p > q$ the defined notions are trivial but we can define them).

Now multiplication among powers of p can be defined by

$$\begin{aligned}\mathrm{Mult}^2_p(x, y, z) \iff{}& \mathrm{Pow}_p(x) \wedge \mathrm{Pow}_p(y) \wedge \mathrm{Pow}_p(z)\wedge \\ &\wedge \exists u_1, v_1, u_2, v_2\Big(\mathrm{Pow}_q(u_1) \wedge v_1 = \mathit{NextPow}_q(u_1)\wedge \\ &\qquad \wedge \mathrm{Mult}^1_{p,q}(x, u_1, u_2) \wedge \mathrm{Mult}^1_{p,q}(x, v_1, v_2)\wedge \\ &\qquad \wedge u_1 \leq y \wedge y < v_1 \wedge u_2 \leq z \wedge z < v_2\wedge \\ &\qquad \wedge \mathrm{RM}_r(Red_r(x), Red_r(y), Red_r(z))\Big).\end{aligned}$$

The idea was to find two consecutive powers of q such that y lies between them, and to multiply them by x. So an interval for $z = xy$ is obtained. If this interval contains two or more powers of p (which is possible only for $q > p$) then the right one is chosen by the last line. (Notice that in this stage the method from [K2] is not suitable for uniform definability.)

Now the multiplication by powers of p can be defined by

$$\begin{aligned}\mathrm{Mult}_p^3(x,y,z) \iff{} & \mathrm{Pow}_p(x) \wedge z \sqcap_p (x-1) = 0 \wedge \\ & \wedge \forall u,v\big((\mathrm{Mult}_p^2(x,u,v) \implies \mathit{Dig}_p(u,y) = \mathit{Dig}_p(v,z)\big).\end{aligned}$$

Similarly we can define Mult_q^2, the multiplication among powers of q and the multiplication Mult_q^3 by powers of q.

Multiplication of arbitrary positive integers can be defined by the following idea: For every positive integer (also every positive real) an arbitrarily exact approximation of the form $\frac{p^i}{q^j}$ can be found. We can replace one factor by such approximation, and obtain an approximation of the product using Mult_p^3, Mult_q^3. The formulas can be found in [K2]. After that, it is easy to define the multiplication of arbitrary nonnegative integers. □

4. Uniform definability for arbitrary moduli

We shall start with some auxiliary definitions. As in the previous section, we shall prefer readable abbreviations, for example $x < n$ instead of (formally more correct) $\mathbb{N}_n(x)$. Of course, "$x < n$" will be understood only as an abbreviation; we cannot decompose it into x, binary $<$ and n. We shall use $\equiv_n$ for the congruence modulo n (as binary relation), and analogously for other moduli. In particular, $\equiv_m$ is the congruence modulo the period m of the margin of B_n of width n. Further we denote

$$\mathrm{PP}_n = \big\{x \in \mathbb{N}_n \mid (\exists p \in \mathbb{P})(\exists e \in \mathbb{N})\big(x = p^e\big)\big\};$$

Th set PP_n consists of all "small" powers of prime divisors of n, where "small" means "less than n". To define PP_n and its strict order $<_{\mathrm{PP}_n}$ we shall use the auxiliary predicate

$$\mathrm{UpTo}_n(x,y) \iff x < n \wedge B_n(x,y) \neq 1 \wedge (\forall z < x)\big(B_n(z,y) = 1\big).$$

However, the presented formula cannot be considered as the definition of UpTo_n in the considered structures because $<$ (in "$z < x$") is not available.

We can define

$$\begin{aligned}
x < n &\iff \exists y,z\big(x = B_n(y,z)\big),\\
x \geq n &\iff \neg(x < n),\\
x = 0 &\iff \forall y,z\big(B_n(x,z) = B_n(y,z)\big),\\
& 1 = B_n(0,0),\\
x = \lceil n-1 \rceil &\iff x < n \wedge B_n(x,1) = 0,\\
y = \mathbf{cs}_n(x) &\iff x < n \wedge y = B_n(x,1) \vee x \geq n \wedge y = 0,\\
x \equiv_n y &\iff B_n(x,1) = B_n(y,1),\\
x \equiv_m y &\iff (\forall z < n)\big(B_n(x,z) = B_n(y,z)\big),\\
\mathrm{UpTo}_n(x,y) &\iff x < n \wedge B_n(x,y) \neq 1 \wedge \\
& \quad \wedge (\forall z < n)\big(B_n(z,y) = 1 \wedge \mathbf{cs}_n(z) \neq x \implies B_n(\mathbf{cs}_n(z),y) = 1\big),\\
\mathrm{PP}_n(x) &\iff \exists y\ \mathrm{UpTo}_n(x,y),\\
x <_{\mathrm{PP}_n} y &\iff \mathrm{PP}_n(x) \wedge \exists z\big(\mathrm{UpTo}_n(y,z) \wedge B_n(x,z) = 1\big).
\end{aligned}$$

Theorem 4.1. *The operation + on $\mathbb{N}$ is uniformly definable in the class $\{\langle \mathbb{N}; B_n\rangle \mid n \text{ composed}\}$.*

Proof. We shall start with the definition of the smallest prime divisor of n; let us denote it by p. Notice that we need n composed here. Then we shall define the set $\mathbb{N}_p$, the constant $\lceil p-1\rceil$, and the set $\mathbb{N}_{n,p}$ of "small" multiples of p (i.e., smaller than n).

$$\begin{aligned}
x = p &\iff 1 <_{\mathrm{PP}_n} x \wedge \forall y\big(y <_{\mathrm{PP}_n} x \implies y = 1\big),\\
x < p &\iff \forall y\big(\mathrm{UpTo}_n(p, y) \implies B_n(x, y) = 1\big),\\
x = \lceil p-1\rceil &\iff \mathbf{cs}_n(x) = p,\\
\mathbb{N}_{n,p}(x) &\iff \exists x, y\big(x \equiv_n \lceil p-1\rceil \wedge y \equiv_n 1 \wedge x = B_n(x, y)\big).
\end{aligned}$$

Now we shall define $\sqsubseteq_p$; in its original definition (Lemma 3.1) $B_p(\dots) = 0$ was used; now it will be replaced with the help of $\mathbb{N}_{n,p}$ and B_n. After that we can define $\sqcap_p$ (the definition not written), and then also B_p itself.

$$\begin{aligned}
x \sqsubseteq_p y &\iff \forall z\big(\mathbb{N}_{n,p}\big(B_n(x, z)\big) \implies \mathbb{N}_{n,p}\big(B_n(y, z)\big)\big),\\
B_p(x, y) &= \lceil p-1\rceil \sqcap_p B_n(x, y).
\end{aligned}$$

Now we can define + like in Theorem 3.3. $\square$

To formulate the next theorem, let us denote

$$\mathrm{MPD} = \big\{n \in \mathbb{N} \mid n > 1 \wedge n \text{ is not a prime power}\big\}.$$

(The letters abbreviate "many prime divisors".)

Theorem 4.2. *The operations $+$, $\times$ on $\mathbb{N}$ are uniformly definable in the class $\{\langle \mathbb{N}; B_n\rangle \mid n \in \mathrm{MPD}\}$.*

Proof. We shall define B_q, where q is the second least divisor of n. We can use all defined notions from the previous proof. In particular, + is already defined. We can define

$$x = q \iff 1 <_{\mathrm{PP}_n} q \wedge p \nmid q \wedge \forall y\big(y <_{\mathrm{PP}_n} x \implies y = 1 \vee p|y\big).$$

Now we can define the set $\mathbb{N}_{n,q}$ of "small" multiples of q. We can continue as above, but since + is available we can also define B_q as follows:

$$z = B_q(x, y) \iff z < q \wedge \exists w\big(\mathbb{N}_{n,q}(w) \wedge B_n(x, y) = w + z\big).$$

Now we can apply Theorem 3.3. $\square$

Lemma 4.3. *There are formulas $\mathbb{P}[n]$, $\mathrm{MPD}[n]$ such that for every integer $n > 1$:*

(1) *n is a prime if and only if the formula $\mathbb{P}[n]$ is true in $\langle \mathbb{N}; B_n\rangle$;*
(2) *$n \in \mathrm{MPD}$ if and only if the formula $\mathrm{MPD}[n]$ is true in $\langle \mathbb{N}; B_n\rangle$*

Proof. If the constant n and the unary predicates $\mathbb{P}$, MPD would be definable, we could simply use the formulas $\mathbb{P}(n)$, $\mathrm{MPD}(n)$. However, this is not true in general. We have to find another formulas, but for easy readability we introduced very similar abbreviations for them. The brackets show us that they cannot be simply understood as atomic formulas.

The formula $\mathbb{P}[n]$ can be $\forall x, y(x \equiv_m y \iff x \equiv_n y)$. It expresses $m = n$; remember that $\equiv_m$ was defined without explicit computing m. However, $m = n$ if and only if n is prime; otherwise m is a proper multiple of n (it could be computed by Lemma 2.1, but we need not it).

The formula $\mathrm{MPD}[n]$ can be

$$(\exists z \geq n)\forall x, y\big(x \equiv_m y \implies B_n(x, z) = B_n(y, z)\big).$$

It expresses that n does not belong to the range of the function $Ones_n$. Since this range contains all powers of prime divisors of n the formula also expresses that n is not a prime power. $\square$

Theorem 4.4. *The operations $\oplus_n$, $\otimes_n$ (extended to $\mathbb{N}$ by the value 0) are uniformly definable in $\{\langle \mathbb{N}; B_n\rangle \mid n > 1\}$.*

Proof. Let us take the right-side of the definition of $\oplus_p$ from the proof of Theorem 3.2, let us eliminate all defined symbols from it. Finally, replace (all occurrences of) B_p by B_n. Let the obtained formula be $\alpha(x, y, z)$.

Let us denote by $\beta(x, y, z)$ the formula

$$\exists u, v\big(B_n(u, v+1) = x \wedge B_n(u+1, v) = y \wedge B_n(u+1, v+1) = z\big).$$

By Theorem 4.1 the formula

$$z = x + y \iff \beta(x, y, z)$$

can be used as a definition of $\oplus_n$ in the class $\{\langle \mathbb{N}; B_n\rangle \mid n \text{ composed}\}$. We can to combine the above definition as follows:

$$z = x \oplus_n y \iff \mathbb{P}[n] \wedge \alpha(x, y, z) \vee \neg\mathbb{P}[n] \wedge \beta(x, y, z).$$

The operation $\otimes_n$ can be defined in the same way. In the construction of the new formula $\beta(x, y, z)$ we can use that for every k there are u, v such that $B_n(n^k u, n^k v) = x$. If k is sufficiently large then we have $B_n(n^k u + t, n^k v + y - t) = 0$ for all integer t, $0 < |t| < n$, and hence for $0 < y < n$ we obtain

$$B_n(n^k u + 1, n^k v + y - 1) = x \otimes_n y. \qquad \square$$

Remark. We could also define the function B_p, where p is the smallest prime divisor of n in the class $\{\langle \mathbb{N}; B_n\rangle \mid n > 1\}$. For n prime we have $B_p = B_n$, for n composed B_p was defined.

5. Undecidability of theories of classes of Pascal's triangles modulo n

We shall need the following theorem about multiplicative semigroups modulo n with usual order. (Notice that the considered structures are not ordered semigroups, and after joining addition modulo n they will not become ordered rings.)

Theorem 5.1. *Every infinite subclass of* $\{\langle \mathbb{N}_n; \otimes_n, <_{\mathbb{N}_n} \rangle \mid n > 1\}$ *has undecidable elementary theory.*

Proof. Let for a considered class n ranges over $X \subseteq \mathbb{N}$. We may assume that X contains no elements less than 16 (or we can consider them separately). We shall use the predicate symbol $<$ without subscript.

We can define usual $+$, $\times$ for "small" integers (approximately up to $\lfloor \sqrt[4]{n} \rfloor$). For $\times$ we can simply take $\otimes_n$. To define a replacement of $+$, we use a modification of Julia Robinson's definition of $+$ from $\times$ and $\mathbf{s}$. We can start as follows:

$$\begin{aligned}
y = \mathbf{cs}_n(x) &\iff x < y \wedge \neg\exists z(x < z \wedge z < y) \vee \neg\exists z(x < z) \wedge y = 0,\\
\mathrm{Sm}_n(x) &\iff (\forall y < x)(y \oplus_n x < \mathbf{cs}_n(y) \oplus_n x),\\
\mathrm{Small}_n(x) &\iff \mathrm{Sm}_n(x) \wedge \mathrm{Sm}_n\big(\mathbf{cs}_n(x \otimes_n x)\big),\\
\mathrm{SmPlus}_n(x,y,z) &\iff \mathrm{Small}_n(x) \wedge \mathrm{Small}_n(y) \wedge \mathrm{Small}_n(z) \wedge\\
&\qquad \wedge \Big(z = 0 \wedge x = 0 \wedge y = 0 \vee z \neq 0 \wedge\\
&\qquad \wedge \mathbf{cs}_n(x \otimes_n z) \otimes_n \mathbf{cs}_n(y \otimes_n z) = \mathbf{cs}_n\big(z \otimes_n z \otimes_n \mathbf{cs}_n(x \otimes_n y)\big)\Big).
\end{aligned}$$

For "small" integers x, y, z we can replace $\otimes_n$ and $\mathbf{cs}_n$ in the latest equation by $\times$ and $\mathbf{s}$, and we obtain the formula used in [Ro].

Now to every Diophantine equation E we can construct a formula Φ_E which is true in the considered class if and only if E has no solution (in $\mathbb{N}$). The formula Φ_E can be constructed as follows. Let us write a formula with the non-logical symbols $+, \times, 1$ which expresses that E has no solution. It can be

$$\forall x_1, \dots x_s (A \implies x_1 \neq x_2),$$

where A is a conjunction of atomic formulas of the forms

$$x_i = x_j + x_k, \qquad x_i = x_j \times x_k, \qquad x_i = 1 \qquad (1 \leq i, j, k \leq s).$$

The number s can be bigger than the number of unknowns of the equation E because the variables $x_1, \dots, x_s$ correspond not only to the unknowns but also to the subterms of both sides of E. However, a solution of E determines the values of all variables x_i.) Let A' arise from A so that all atomic formulas $x_i = x_j + x_k$ are replaced by $\mathrm{SmPlus}_n(x_j, x_k, x_i)$ and all $\times$ are replaced by $\otimes_n$. Then the requested formula Φ_E will be

$$\forall x_1, \dots x_s \big(\bigwedge_{i=1}^{s} \mathrm{Small}_n(x_i) \wedge A' \implies x_1 \neq x_2 \big).$$

If E has a solution then its components are "small" (in the sense Small_n) for n sufficiently big. Let us take any such $n \in X$. In the corresponding structure Φ_E is false; hence it is not true in the considerd class. If E has no solution then the formula Φ_E is true in the considered class. Indeed, for every n and any values of x_i either the values are not "small" (and the antecedent is not fulfilled) or $\otimes_n$, SmPlus_n correspond to $\times$, $+$ (and the consequent is fulfilled provided A' is). So Φ_E has the required property.

By the above, if the considered theory is decidable then we can decide solvability of Diophantine equations. However, this is impossible by [Ma]. □

Remark. $<_{\mathbb{N}_n}$ cannot be replaced by $\oplus_n$ (or by $\mathbf{cs}_n$) in Theorem 5.1 because by [Ax] the elementary theory of $\{\langle \mathbb{N}_n; \otimes_n, \oplus_n \rangle \mid n \in \mathbb{P}\}$ is decidable.

Theorem 5.2. *Every infinite subclass of* $\{\langle \mathbb{N}; B_n \rangle \mid n > 1\}$ *has undecidable elementary theory.*

Proof. Let $\{\langle \mathbb{N}; B_n \rangle \mid n \in X\}$ be the considered class. It suffices to interpret the class $\{\langle \mathbb{N}_n; \otimes_n, <_{\mathbb{N}_n} \rangle \mid n \in X\}$ in it. This is possible because $\mathbb{N}_n$ (as a unary predicate), the operation $\otimes_n$ and the relation $<_{\mathbb{N}_n}$ are (uniformly) definable. Definitions of the first two symbols were considered above. For the third one we can use

$$x <_{\mathbb{N}_n} y \iff y < n \wedge \big(\mathbb{P}[n] \wedge x \sqsubset_n y \vee \neg\mathbb{P}[n] \wedge \exists z\, \alpha(x, z, y)\big),$$

where $\alpha(x, y, z)$ is from the definition of $+$ for n composed (Theorem 4.1). □

Corollary 5.3. *Let* $X \subseteq \mathbb{N} \setminus \{0, 1\}$*. Then the elementary theory of the class* $\{\langle \mathbb{N}; B_n \rangle \mid n \in X\}$ *is undecidable if and only if* X *is infinite or* X *contains an element divisible by two primes.*

Proof. For X infinite we can use the previous theorem. If X is finite and $k \in X$ is divisible by two primes we use that the property "$n = k$" is expressible by a formula, and that the structure $\langle \mathbb{N}; B_k \rangle$ has undecidable theory (because $+$, $\times$ are definable in it). Conversely, if X is finite and all its elements are prime powers we can use the result of [Be] that each structure $\langle \mathbb{N}; B_n \rangle$ (and even $\langle \mathbb{N}; B_n, + \rangle$), $n \in X$, has decidable theory. Then the whole class has decidable theory, too. □

References

[Be] A. Bès, *On Pascal triangles modulo a prime power*, Proceedings Logic Colloquium'94 Clermont Ferrand (submitted 1994), 14pp.

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

[Bü] J. R. Büchi, *Weak second-order arithmetic and finite automata*, Zeitschrift für Math. Logik Grundlagen Math. **6** (1960), 66-92.

[CG] A. Černý, J. Gruska, *Modular trellises*, Acta Informaticae **9** (1986), 253-282.

[K1] I. Korec, *Generalized Pascal triangles*, In: K. Halkowska and S. Stawski, ed.: Proceedings of the V Universal Algebra Symposium, Turawa, Poland, May 1988, World Scientific, Singapore, 1989, pp. 198-218.

[K2] ———, *Definability of arithmetic operations in Pascal triangle modulo an integer divisible by two primes*, Grazer Mathematische Berichte **318** (1993), 53-61.

[K3] ———, *Structures related to Pascal's triangle modulo 2 and their elementary theories*, Mathematica Slovaca **44** (1994), no. 5, 531-554.

[K4] ———, *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.

[Ma] Ju. Matijasewitch, *Hilbert's Tenth Problem*, MIT Press, 1993.

[Pu] H. Putnam, *Decidability and essential undecidability*, Journal of Symbolic Logic **22** (1957), 39-54.

[Ro] J. Robinson, *Definability and decision problems in arithmetic*, Journal of Symbolic Logic **14** (1949), no. 2, 98-114.

[Wo] A. R. Woods, *Some problems in number theory and their connections*, PhD Thesis, University of Manchester, 1981.

Mathematical Institute, Slovak Academy of Sciences, Štefánikova 49,
814 73 Bratislava, Slovakia
E-mail address: korec@savba.sk

This preprint series was founded in 1996. Its purpose is to present manuscripts of submitted or unpublished papers and reports of fellows of the Mathematical Institute of the Slovak Academy of Sciences in Bratislava and its Košice branch. The authors are fully responsible for the content of the preprints. Postal addresses:

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

Tel./Fax (+421 7) 5249 7316

Mathematical Institute
Slovak Academy of Sciences
Grešákova 6
SK–040 01 Košice
SLOVAKIA

Tel./Fax (+421 95) 6228291

PostScript files of preprints are available at WWW address:
`http://www.mat.savba.sk/preprints`

Latest preprints of the series:

18/1996 *Ivan Korec*: Undecidability and uniform definability in classes of structures related to Pascal's triangles modulo n

17/1996 *Beloslav Riečan*: Probability theory on some ordered structures

16/1996 *Beloslav Riečan*: Weak observables in MV algebras

15/1996 *Anatolij Dvurečenskij, Hee Sik Kim*: On connections between BCK-algebras and difference posets

14/1996 *Anatolij Dvurečenskij, Karl Svozil*: Product of partition logics, orthoalgebras and automata

13/1996 *Robin L. Hudson, Sylvia Pulmannová*: Chaotic expansion of elements of the universal enveloping algebra of a Lie algebra associated with a quantum stochastic calculus

12/1996 *Sylvia Pulmannová*: Congruences in partial abelian semigroups

11/1996 *Karol Nemoga, Štefan Schwarz*: An explicit description of the set of all normal bases generators of a finite field

10/1996 *Ján Jakubík*: Subdirect product decompositions of MV-algebras

9/1996 *Ivan Korec*: Reversibility in generalized Pascal triangles and binary reversibility in one-dimensional cellular automata

8/1996 *Jozef Bobok, Milan Kuchta*: X-minimal patterns and generalization of Sharkovskiĭ's theorem

7/1996 *Jarmila Hedlíková, Sylvia Pulmannová*: Generalized difference posets and orthoalgebras

6/1996 *Ján Borsík, Roman Frič*: Pointwise convergence fails to be strict

5/1996 *Miroslav Ploščica*: Affine completions of distributive lattices

4/1996 *Ján Haluška*: Equal temperament and Pythagorean tuning: a geometrical interpretation in the plane

3/1996 *Winfried Just, Peter Vojtáš*: On matrix rapid filters

2/1996 *Anatolij Dvurerečenskij*: Fuzzy set representations of some quantum structures

1/1996 *Miloslav Duchoň, Beloslav Riečan*: On the product of semigroup valued measures

(continued on inside back cover)