Mathematical Institute
Slovak Academy of Sciences, Bratislava

Preprint 2/1997

Ivan Korec

Elementary definability from Pascal's triangle modulo p and the set of e-th powers

January 14, 1997

PREPRINT SERIES

Elementary definability from Pascal's triangle modulo p and the set of e-th powers

Ivan KOREC

Abstract. Let B_p denote Pascal's triangle modulo p, i.e. $B_p(x,y) = \binom{x+y}{x} \operatorname{MOD} p$ and let Pow_p denote the set of e-th powers. For all pairs (p,e), $2 \leq p \leq 20$, $2 \leq e \leq 20$ except $p = 2$, $e > 2$ even and $p = 3$, $e = 9, 18$ the operations $+$, $\times$ are first order definable in $\langle \mathbb{N}; B_p, \mathrm{Pow}^e \rangle$. In the mentioned exceptional cases the operations $+$, $\times$ are not definable.

1991 Mathematics Subject Classification: Primary 03B10, 11B65 Secondary 03C07

1. Introduction

We shall investigate first order definability of arithmetical operations $+$, $\times$ (on the set $\mathbb{N}$ of nonnegative integers) from the Pascal triangle modulo p (see the notation B_p in the next section) and the set of e-th powers; the former is considered as a binary operation on $\mathbb{N}$ and the latter as a unary relation on $\mathbb{N}$. Various systems of operations and/or relations which suffice to define these operations have been studied for a long time. Classical results in this direction were obtained by J. Robinson, who proved (among many other results) that $+$, $\times$ are definable from the successor operation and divisibility relation. By Gödel's theorem every structure (over $\mathbb{N}$) in which $+$, $\times$ are definable has undecidable elementary theory. This is one of the reasons to study similar questions.

Some definability results concerning Pascal's triangles modulo n were obtained by A. Bès and the author. A problem which remained open was whether $+$, $\times$ are definable from the Pascal's triangle modulo 2 and the set of cubes; it corresponds to the values $p = 2$ and $e = 3$ above. (Notice that the cases $p = 2$, $e = 2$ and $p = 2$, $e = 4$ were solved. More information is contained in the next section.) In the present paper we shall solve the problem not only for $p = 2$, $e = 3$ but also for many other values of p and e, including all pairs of values $p \leq 20$, $e \leq 20$. (For $p = 2$, $e = 3$ we shall prove that $+$, $\times$ are definable.)

This work was supported by Grant 2/1227 of Slovak Academy of Sciences.

Key words and phrases. Elementary definability, Pascal's triangle modulo n, Undecidable theories.

Section 2 contains some notations, technicalities and previous results. Also the problem described above is strictly formulated, and it is solved for p composed (and $e \geq 2$); hence only the cases p prime remain for the further sections. Section 3 contains some auxiliary results about last digits of e-th powers in p-adic number system. Section 4 contains a theorem which reduces definability of $+$, $\times$ to definability of some constants. Finally, in Section 5 results of previous sections are applied to the mentioned problem for some values of p, e. Some results are obtained using a computer but the amount of computations for p, e up to 20 is not too big (and for $p = 2$, $e = 3$ the computer is unnecessary at all).

2. Notation and other preliminaries

Let $\mathbb{N}$ be the set of nonnegative integers, let $+$, $\times$ be usual arithmetical operations on $\mathbb{N}$ and let MOD denote the remainder by integer division. For positive integer p let B_p denote Pascal's triangle modulo p, i.e. the function

$$B_p(x,y) = \binom{x+y}{x} \operatorname{MOD} p.$$

For positive integer e let Pow^e denote the set of e-th powers, i. e.

$$\mathrm{Pow}^e = \{x^e \mid x \in \mathbb{N}\}.$$

We shall consider the structures $\langle \mathbb{N}; B_p, \mathrm{Pow}^e \rangle$, and the central question considered in the present paper (and mentioned already in the introduction) is:

Problem 2.1. Are the operations $+$, $\times$ first order definable in the structure $\langle \mathbb{N}; B_p, \mathrm{Pow}^e \rangle$?

Of course, the answer can depend on the values of the parameters p, e. We shall assume that p, e are positive integers.

For the notion of (first order) formulas, truth, definability, etc. we refer to [Mo] or to some other textbook of mathematical logic. However, we do not distinguish between the function or predicate and the corresponding symbol for it. The equality sign is considered as a logical symbol. If $\leq$ on $\mathbb{N}$ is defined in a considered structure we shall also freely use $<, >, \geq$; moreover, since $0, 1, 2, \ldots$ and the successor $\mathbf{s}$ are also first order definable we may use them, too. The letters u, v, x, y, z (possibly with subscripts) will be used as individual variables in the formulas, the symbols $\neg, \wedge, \vee, \implies, \iff$ as logical connectives (they are written in the order given by their priorities) and $\exists, \forall$ as quantifiers. Relativized quantifiers $(\forall x < y)$, $(\exists x \geq y)$ etc. and other usual abbreviations also will be used. The symbol $\exists!$ will denote "there is exactly one". The symbols $\bigwedge, \bigvee$ will abbreviate conjunction and disjunction of several formulas, respectively; to specify these formulas, metavariables $i, j, k, \ldots$ will also be used.

The following two theorems contain some results of the previous papers [Be94], [BK96], [Ko94], … Therefore their proofs will be omitted or only briefly sketched. The theorems cover trivial or sooner considered cases of Problem 2.1, and will be used below.

Theorem 2.2. *The elementary theory of the structure* $\langle \mathbb{N}; B_p, \mathrm{Pow}^e \rangle$ *is decidable in the following cases:*
(i) $p = 1$ *(and e is arbitrary);*
(ii) p *is a prime power and* $e = 1$.
In these cases the operations $+$, $\times$ *are not definable.*

Proof. In the case (i) the operation B_1 is equal to 0 identically; therefore it can be replaced by the unary relation $\{0\}$ without changing definability (and expressibility) power. Then we have a structure with two unary relations only, and its theory is decidable.

For (ii) notice that $\mathrm{Pow}^1 = \mathbb{N}$, hence we can delete Pow^1 without changing definability power. However, the structure $\langle \mathbb{N}; B_p \rangle$ (and even the structure $\langle \mathbb{N}; B_p, + \rangle$) has decidable theory.

The last part is a consequence of Gödel's incompleteness theorem. (We need only the fact that the elementary theory of $\langle \mathbb{N}; +, \times \rangle$ is undecidable.) $\square$

Theorem 2.3. *The operation* $+$, $\times$ *are first order definable in the structure* $\langle \mathbb{N}; B_p, \mathrm{Pow}^e \rangle$ *(and hence its elementary theory is undecidable) in the following cases:*
(i) p *is divisible by two distinct primes;*
(ii) p *is composed and* $e > 1$*;*
(iii) $p > 1$ *and* $e = 2$.

Proof. (i) holds because by [Ko93] the operations $+$, $\times$ are definable already in the structure $\langle \mathbb{N}; B_p \rangle$.

In (ii) we need to consider only the case when p is a prime power (with exponent greater than 1); the other cases are covered by (i). Notice that in this case by [Be] addition is definable from B_p alone. Further, by [Pu57] we can define $\times$ from $+$ and Pow^e.

In (iii) we may assume that p is prime; the other cases are covered by (ii). The result is proved in [BK96], for $p = 2$ also in [Ko94]. At first ordering of powers of p ought to be defined. After that we can define addition. Finally, multiplication can be defined from $+$ and Pow^e. $\square$

By the above theorems we need to consider Problem 2.1 only for p prime. Now we shall introduce some notation concerning Pascal's triangles modulo a prime and we shall present some their properties. If a number $x \in \mathbb{N}$ is given by its p-adic digits $a_r, a_{r-1}, \ldots, a_0$ we shall write $x = [a_r a_{r-1} \ldots a_0]_p$. Leading zeros are allowed if necessary (e. g., to obtain equal numbers of digits in two integers).

The main tool for investigating Pascal's triangles modulo a prime is Lucas' theorem, see e.g. [Bo90]. We present it in a little modified form, with $\binom{x+y}{x}$ instead of $\binom{x}{y}$.

Theorem 2.4. *If* p *is a prime and* $x = [a_r \dots a_1 a_0]_p$, $y = [b_r \dots b_1 b_0]_p$ *then*

$$\binom{x+y}{x} \equiv \binom{a_0+b_0}{a_0} \cdot \binom{a_1+b_1}{a_1} \cdot \dots \cdot \binom{a_r+b_r}{a_r} \pmod{p}.$$

Corollary 2.5. *For* p, x, y *as in Theorem 2.4 we have*

$B_p(x,y) = 0$ *if and only if* $a_i + b_i \geq p$ *for some* $i \in \{0, 1, \dots, r\}$.

For $x = [a_r \dots a_1 a_0]_p$, $y = [b_r \dots b_1 b_0]_p$ we shall write $x \sqsubseteq_p y$ if it holds $a_i \leq b_i$ for all $i = 0, 1, \dots, r$. The relation $\sqsubseteq_p$ will be called *n-adic masking relation.* As we shall see, $\sqsubseteq_p$ is definable from B_p, and it may replace B_p in many (but not all!) definability results.

Theorem 2.6. (i) *For every prime* n *the relation* $\sqsubseteq_p$ *is first order definable in the structure* $\langle \mathbb{N}; B_p \rangle$.

(ii) *For every prime* p *the relation* $\sqsubseteq_p$ *is a partial order on the set* $\mathbb{N}$. *In the structure* $L = \langle \mathbb{N}; \sqsubseteq_p \rangle$ *we can define:*

$x \sqcap_p y$	*meet operation in* L;
$x \sqcup_p y$	*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;
$\mathrm{OneDig}_p(x)$	x *has at most one nonzero digit;*
$Dig_p^i(u,x)$	$\mathrm{Pow}_p(u)$ *and the corresponding digit of* x *is* i, *or "*u *occurs* i*-times in* x*";*
$\mathrm{CFAdd}_p(x,y,z)$	*carry-free addition:* $x+y=z$, *and no carry occurs when* $x+y$ *is computed.*

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

Proof. The defining formula for $\sqsubseteq_p$ can be

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

To prove that, some considerations about p-adic digits must be done and Corollary 2.5 applied. The predicates and functions in (ii) can be defined by usual approach of Lattice theory. For example, Pow_p is the set of atoms of $\langle \mathbb{N}; \sqcup_p, \sqcap_p \rangle$.

We shall introduce one special abbreviation connected with the partial order $\sqsubseteq_p$. For every formula $\alpha(x)$ we shall denote by $\mathbf{Least}_x(\alpha(x))$ the formula

$$\alpha(x) \wedge \forall u \big(\alpha(u) \implies x \sqsubseteq_p u \big),$$

where u is a variable which do not occur in $\alpha(x)$. We shall apply that for the definition of $\sqcup_p$ and 0.

$$z = x \sqcup_p y \iff \mathbf{Least}_z\big(x \sqsubseteq_p z \wedge y \sqsubseteq_p z\big), \qquad x = 0 \iff \mathbf{Least}_x\big(x = x\big).$$

Of course, these formulas are mainly illustrating examples. The abbreviation is more useful for longer $\alpha(x)$. □

Theorem 2.6 shows us that we can express the statements about finite sets of powers of p by first order formulas concerning $\langle \mathbb{N}; B_p \rangle$. So we can indirectly use some machinery of weak monadic second order formulas (restricted to Pow_p) following the ideas contained e.g. in [Bü60].

For any set $X \subseteq \mathbb{N}$ we shall denote by $<_X$ the restriction of the usual order $<$ to the set X. Analogously we shall use $\leq_X$. If X has at least two elements then $<_X$ and $\leq_X$ are interdefinable.

Theorem 2.7. *Let $p \geq 2$, $e \geq 2$. Then the operations $+$, $\times$ are first order definable in $\langle \mathbb{N}; B_p, \mathrm{Pow}^e \rangle$ if and only if the relation $<_{\mathrm{Pow}_p}$ is first order definable in this structure.*

In essential, Theorem 2.7 is contained in [BK96] (and for $p = 2$ also in [Ko94]).

3. Last digits of e-th powers

Here we shall investigate which groups of digits can occur at the last (or: the lowest) positions of e-th powers in p-adic number system. Besides p, e we introduce integer parameters n, f, k by the conditions

$$(3.1) \qquad p \text{ prime}, \quad e \geq 2, \quad e = p^n f, \quad p \nmid f, \quad k = \frac{p-1}{\gcd(f, p-1)}.$$

(The symbol gcd denotes the nonnegative greatest common divisor.) The values of n, f, k are uniquely determined by p and e; they help us to express some statements below briefly.

To formulate the results we shall use some notions of the theory of formal languages. Using p-adic expansions we can associate a word $\overline{x}$ in the alphabet $\Sigma = \{0, 1, \ldots, p-1\}$ to every integer $x \in \mathbb{N}$ in the usual way. (We shall use Σ and overlining without the index p, but they do depend on p.) This overlining is in a sense inverse to $[\ ]_p$: if $y = \overline{x}$ then $[y]_p = x$. Further, to every $Y \subseteq \mathbb{N}$ the formal language $\overline{Y} = \{\overline{x} \mid x \in Y\}$ will be associated. We shall also use some notions and notation from formal language theory, e.g. concatenation (without a symbol), power as repeated concatenation, iteration $X^* = \bigcup_{i=0}^{\infty} X^i$, etc. The symbol $\mathrm{Fin}(X)$ will denote the set of all final subwords of words from X; for example, if $X = \{0011\}$ then $\mathrm{Fin}(X) = \{0011, 011, 11, 1, \varepsilon\}$, where ε denotes the empty word.

Theorem 3.1. *Let the integers* p, e, n, f, k *satisfy* (3.1). *Then:*

(i) *If* p *is odd then there are* k *pairwise distinct nonzero digits* $a_1, \dots a_k$ *and* k *words* $w_1, \dots, w_k \in \Sigma^n$ *such that*

$$\text{(3.2)} \qquad \mathrm{Fin}(\overline{\mathrm{Pow}^e}) = \mathrm{Fin}(\Sigma^* \{w_1 a_1, \dots, w_k a_k\}(0^e)^*);$$

we can arrange $a_1 = 1$, *and then* $w_1 = 0^n$.

(ii) *For* $p = 2$ *and* $n > 0$ *the formula* (3.2) *also holds, but with* $w_1 = 0^{n+1}$. *For* $p = 2$ *and* $n = 0$ *the formula* (3.2) *holds (with* w_1 *the empty word).*

Proof. The number of zeros at the end of any nonzero e-th power is a multiple of e; this is expressed by the factor $(0^e)^*$ in (3.2). Also $0 \in \mathrm{Pow}^e$ can be easily considered (and (3.2) holds independently of allowing leading zeros in $\overline{\mathrm{Pow}^e}$). So we can consider below only the e-th powers not divisible by p; let M^e denote the set of such e-th powers.

Let us consider p odd at first. Let r be the primitive root modulo p^{n+1}; by [Vi49] we can choose r independently on n. Take arbitrary $m \geq 0$, and consider the multiplicative group modulo p^{m+1}. This is a cyclic group with $\varphi(p^{m+1}) = p^m \cdot (p-1)$ elements, and r is its generator; φ denotes Euler's function. The $(m+1)$-tuples of lowest digits on M^e correspond to the e-th powers of elements of this cyclic group. For $m = 0$ we obtain k distinct e-th powers of r (modulo p). For $m = n$ we still obtain k distinct powers. However, for $m > n$ we obtain $p^{m-n}k$ distinct powers. This is possible only if the digits at the positions 1, … , n are uniquely determined by the digit at the 0-th position (i.e. some a_i). However, the digits at the $(n+1)$-th and any higher position can be chosen completely arbitrarily; otherwise we cannot obtain sufficiently many elements in the cyclic groups modulo p^m. The formula (3.2) expresses these facts.

By the above the digits a_i and the words w_i can be obtained from the congruences

$$[w_{i+1} a_{i+1}]_p \equiv r^{ie} \pmod{p^{n+1}}, \qquad i = 0, 1, \dots, k-1.$$

Hence the n-th, $(n-1)$-th, … , first digits of any $x \in M^e$ are uniquely determined by its 0-th digit (i.e. some a_i).

The situation for $p = 2$, $n > 1$ is a little different because the multiplicative group modulo 2^e is not cyclic; it is a direct product of cyclic groups of orders 2^{e-2} and 2. Therefore w_1 becomes one digit longer. □

The words w_i can be expressed more explicitly if we define a function

$$W_p : \{0, 1, 2, \dots, p-1\} \times \mathrm{Pow}_p \to \{0, 1, 2, \dots, p-1\}$$

by the formula

$$W_p(x, p^i) = \text{ the } i\text{-th } p\text{-adic digit of } x^{p^{i+1}} \text{ (from the right).}$$

(We do not investigate first order definability of W_p.) Notice that the exponent p^{i+1} can be replaced by any p^j, $j > i$, and that W depends only on p, and not on e; the words w_i depends on both parameters p, e (and also on the order of a_i).

Then we can write

$$w_i = W_p(a_i, p^n)W_p(a_i, p^{n-1})\dots W_p(a_i, p^1).$$

Lemma 3.2. *If* (3.1) *holds and* $k > 1$ *then for every positive* $j \le n$ *there is* $i \in \{1, \dots, k\}$ *such that* $W_p(a_i, p^j) \neq 0$.

Proof. We have $r^{ke} - 1 \equiv 0 \pmod{p^{n+1}}$. Dividing by $r^e - 1$ (which is relatively prime to p if $k > 1$) we obtain

$$1 + r^e + r^{2e} + \dots r^{(k-1)e} \equiv 0 \pmod{p^{n+1}},$$

and therefore

$$[w_1 a_1]_p + [w_2 a_2]_p + \dots + [w_{k-1} a_{k-1}]_p \equiv 0 \pmod{p^{n+1}}.$$

Hence the left side is a positive multiple of p^{n+1}. This may happen only if (by p-adic addition of the left side) a carry occurs at every position from 0-th to n-th. Hence a nonzero digit must occur at every of these positions (which is formally expressed in Lemma 3.2). □

4. Reductions to definability of constants

We have reduced the definability of $+$, $\times$ in the considered structures to the definability of $<_{\mathrm{Pow}_p}$. Now we shall look for further reducibilities. Throughout the whole section the parameters will satisfy (3.1). First of all, we shall exclude some cases from further considerations.

Theorem 4.1. *If* p *is an odd prime and* e *is a multiple of* $\frac{p^2\cdot(p-1)}{2}$ *or if* $p = 2$ *and* $e > 2$ *is even then* $+$, $\times$ *are not first order definable in* $\langle \mathbb{N}; B_p, \mathrm{Pow}^e \rangle$.

Proof. Let us consider odd p at first. Then by the previous section every e-th power has equal digits at the first and at the second position (i.e., at the positions corresponding to p^1 and p^2). We can see that also immediately from the congruence

$$x^e \equiv 0,\ 1,\ p^3 - 1 \pmod{p^3} \tag{4.1}$$

which holds for all $x \in \mathbb{N}$. (The formula (4.1) ought to be understood as a disjunction of three congruences. The third case takes place only when e is an odd multiple of $\frac{p^2\cdot(p-1)}{2}$ and x is a quadratic non-residue modulo p.) In the first two cases the corresponding digits are 0 and in the third case they are equal to $p - 1$.

Now we shall use isomorphism argument. Let the mapping f be defined by

$$f(xp^3 + x_2p^2 + x_1p + x_0) = xp^3 + x_1p^2 + x_2p + x_0$$

for all $x_0, x_1, x_2 < p$ and $x \in \mathbb{N}$. The mapping f is derived from the permutation of Pow_p which interchanges p and p^2, and preserves the other powers of p. The mapping f obviously preserves every $x \in \mathrm{Pow}^e$. By Lucas' theorem f is a (nontrivial) automorphism of $\langle \mathbb{N}; B_p \rangle$. Therefore f is a (nontrivial) automorphism of $\langle \mathbb{N}; B_p, \mathrm{Pow}^e \rangle$. However, f preserves neither $+$ nor $\times$, hence they are not definable in the considered structure.

The proof for $p = 2$ is the same in essential, but the third rest disappears in the congruence (4.1). (The case $e = 2$ had to be excluded because of (iii) of Theorem 2.3. In this case the rest 4 would appear in the congruence (4.1), and f fails to be an automorphism.) $\square$

In terms of the parameters (3.1) Theorem 4.1 covers all cases when $n \geq 2$ and $k \leq 2$. For $p = 2$ it covers all cases $k \geq 1$ except $e = 2$ (which is contained in Theorem 2.3 with the opposite answer). The condition for undefinability of $+$, $\times$ in Theorem 4.1 is rather strong. However, it is only a necessary condition, as the following example shows.

Example 4.2. Let $p = 89$ and $e = 22 \cdot 89^2$ (hence $n = 2$, $k = 4$). By computation we can verify that

$$89^3 \mid \left(43 \cdot 89^2 + 43 \cdot 89 + 34\right)^2 + 1.$$

Hence four (non-congruent) solutions of the congruence $y^4 \equiv 1 \pmod{89^3}$ are ± 1 and $\pm[43, 43, 34]_{89} = \pm 344464$, where the numbers in brackets must be understood as digits in the 89-adic number system. Since $x^{4e} \equiv 0, 1 \pmod{89^3}$ we have

$$x^e \equiv 0,\ 1,\ 89^3 - 1,\ [43, 43, 34]_{89},\ [45, 45, 55]_{89} \pmod{89^3}$$

for every $x \in \mathbb{N}$. The digits corresponding to 89^1 and 89^2 are equal to each other in every of five cases above. Now we can apply the same automorphism argument as in Theorem 4.1. In this example e can be multiplied by any odd positive integer; multiplying by even positive integer is also possible but then the obtained values will be covered by Theorem 4.1.

Further we shall consider mainly the cases which are decided neither by "positive" Theorem 2.3 nor "negative" Theorem 4.1. So besides the conditions (3.1) we shall usually assume $n \leq 1$ or $k \geq 3$ (these assumptions will be explicitly repeated in the theorems whenever used). We shall use all notations and results of Section 2. Further we define

$$\mathrm{Pow}_p^e(x) \iff \mathrm{Pow}_p(x) \wedge \mathrm{Pow}^e(x), \qquad \mathrm{OP}_p^e(x) \iff \mathrm{Pow}_p(x) \wedge \neg\, \mathrm{Pow}_p^e(x).$$

If we consider unary predicates as subsets of $\mathbb{N}$ then Pow_p^e is the set of powers of p^e (in symbols: $\mathrm{Pow}_p^e = \mathrm{Pow}_p \cap \mathrm{Pow}^e$) and $\mathrm{OP}_p^e = \mathrm{Pow}_p \setminus \mathrm{Pow}_p^e$ is the set of other powers of p. (Hence for example $\mathrm{Pow}_2^3 = \mathrm{Pow}_8$ and OP_2^3, "other powers", is the set of those powers of 2 which are not cubes.) Further we define

$$\begin{aligned} y = LtP_p^e(x) \iff{}& \mathrm{OP}_p^e(x) \wedge \mathbf{Least}_y \Big(\forall u \big(u \sqsubseteq_p y \wedge \mathrm{Pow}_p(u) \implies \mathrm{Pow}_p^e(u) \big) \wedge \\ & \wedge \forall z \big(\mathrm{Pow}^e(z) \wedge x \sqcap_p z \neq 0 \implies y \sqcap_p z \neq 0 \big) \Big) \vee \\ & \vee \neg\, \mathrm{OP}_p^e(x) \wedge y = 0. \end{aligned}$$

We can accept this definition only if y satisfying the right-hand side exists and is unique. This is clear for $\neg\,\mathrm{OP}_p^e(x)$ (but this part is not very important). For $\mathrm{OP}_p^e(x)$ the uniqueness is also obvious, and the existence will be proved in the next lemma, which gives also the explicit formula for $LtP_p^e(x)$ (in the important case).

Lemma 4.3. *If* (3.1) *holds then for every* $r, s \in \mathbb{N}$, $0 < s < e$ *we have*

$$LtP_p^e(p^{er+s}) = \begin{cases} \sum_{i=0}^{r} p^{ei} & \textit{if } \; k > 1 \textit{ or } s > n, \\ \sum_{i=0}^{r-1} p^{ei} & \textit{otherwise.} \end{cases}$$

Proof. Let r, s satisfy the assumptions and let $x = p^{er+s}$, $y = LtP_p^e(x)$. Then y is a sum of several distinct powers of p^e; it obviously need not have any digit greater than 1. If an e-th power has a nonzero digit at the $(er+s)$-th position then it must have a nonzero digit also at an et-th position for some $t \le r$. (For $s \le n$ and $k = 1$ we may claim $t < r$ here. This special case also needs some modifications below.) Hence y (if it exists) satisfies $y \sqsubseteq_p \sum_{i=0}^{r} p^{ei}$. Now we shall use Theorem 3.1. For every $r_0 > r$ and $t \le r$ (or $t < r$ in the special case) we can find an e-th power u with nonzero digit at the $(er+s)$-th position and at the et-th position, and with zeros at ej-th positions for all $j < r_0$, $j \ne t$. (The other digits of u are not important. Notice that some a_i in (3.2) corresponds to the et-th position of u.) Therefore $p^{et} \sqsubseteq_p y$ for every $t \le r$ (or $t < r$ in the special case), and we obtain the requested formula. □

We shall need the following function $NearP_p^e$ (mnemonics: near power of p^e):

$$(4.2) \quad NearP_p^e(x) = \begin{cases} \min\{y \in \mathrm{Pow}_p^e \mid x < py\} & \text{if } k \ne 1, \\ \min\{y \in \mathrm{Pow}_p^e \mid x < p^{n+1}y\} & \text{if } k = 1,\ p \text{ is odd prime}, \\ \min\{y \in \mathrm{Pow}_2^e \mid x < 2y\} & \text{if } p = 2,\ n = 0, \\ \min\{y \in \mathrm{Pow}_2^e \mid x < 2^{n+2}y\} & \text{if } p = 2,\ n > 0. \end{cases}$$

In the case $k \ne 1$ (and hence $p > 2$) the unique nonzero digit of $NearP_p^e(x)$ is at higher or equal position than any nonzero digit of x. The same holds for the third case $p = 2$, $n = 0$. In the second case we consider the powers p^{ue+i}, $1 \le i \le n$ as "lower" than p^{ue} because there is no power of p with nonzero digit at a $(ue+i)$-th position and the lowest nonzero digit at the ue-th position. (Let us consider the formula (3.2). The powers p^{ue+i} correspond here to the symbols of w_1 and the power p^{ue} corresponds to the symbol a_1.) The fourth case is similar; we only must apply the part (ii) of Theorem 3.1. (Only for the case $e = 2$ the explanation fails. However, we need not consider this case.)

Example 4.4. For better explanation let us consider the sequences:

$$\ldots,\{\boldsymbol{3^{15}},3^{14},3^{13},3^{12},3^{11}\},\{\boldsymbol{3^{10}},3^{9},3^{8},3^{7},3^{6}\},\{\boldsymbol{3^{5}},3^{4},3^{3},3^{2},3^{1}\},\{\boldsymbol{3^{0}}\}$$

$$\ldots,\{3^{13},\boldsymbol{3^{12}},3^{11},3^{10},3^{9},3^{8}\},\{3^{7},\boldsymbol{3^{6}},3^{5},3^{4},3^{3},3^{2}\},\{3^{1},\boldsymbol{3^{0}}\}$$

$$\ldots,\{\boldsymbol{2^{12}},2^{11},2^{10}\},\{\boldsymbol{2^{9}},2^{8},2^{7}\},\{\boldsymbol{2^{6}},2^{5},2^{4}\},\{\boldsymbol{2^{3}},2^{2},2^{1}\},\{\boldsymbol{2^{0}}\}$$

$$\ldots,\{2^{14},2^{13},\boldsymbol{2^{12}},2^{11},2^{10},2^{9}\},\{2^{8},2^{7},\boldsymbol{2^{6}},2^{5},2^{4},2^{3}\},\{2^{2},2^{1},\boldsymbol{2^{0}}\}$$

The four rows above present examples to the four cases of the definition of $NearP_p^e$; the pair (p,e) is equal to $(3,5)$, $(3,6)$, $(2,3)$ and $(2,6)$, respectively. The powers of p are presented in descending order which corresponds to the usual writing of integers in the p-adic system. Every displayed set collects the powers of p with the same value of $NearP_p^e$; the value is printed in bold. Any $x \in \mathbb{N}$ can be understood as a multiset of powers of p, and then $NearP_p^e(x)$ is the bold-written element of the leftest set which meets x.

Lemma 4.5. *If* (3.1) *holds then the relation* $<_{\mathrm{Pow}_p^e}$ *and the operation* $NearP_p^e$ *are first order definable in the structure* $\langle \mathbb{N}; B_p, \mathrm{Pow}^e\ \rangle$.

Proof. By Lemma 4.3 the initial segments of Pow_p^e (including the empty one) correspond to the values of the functions LtP_p^e). Therefore we can define

$$\begin{aligned} x <_{\mathrm{Pow}_p^e} y \iff & \mathrm{Pow}_p^e(x) \wedge \mathrm{Pow}_p^e(y) \wedge x \neq y \wedge \\ & \wedge \forall z\big(\mathrm{OP}_p^e(z) \wedge y \sqsubseteq_p LtP_p^e(z) \implies x \sqsubseteq_p LtP_p^e(z)\big). \end{aligned}$$

The idea is that a smaller power of p^e belongs to more initial segments of Pow_p^e than the bigger one. Now we can define $NearP_p^e$ by the formula

$$\begin{aligned} y = NearP_p^e(x) \iff & \mathrm{Pow}_p^e(y) \wedge \forall z\Big(z <_{\mathrm{Pow}_p^e} y \vee z = y \iff \\ & \iff \exists u\big(u \sqsubseteq_p x \wedge \mathrm{Pow}_p^e(u) \wedge (z <_{\mathrm{Pow}_p^e} u \vee z = u) \vee \\ & \vee \exists v(v \sqsubseteq_p x \wedge u \sqsubseteq_p LtP_p^e(v)) \wedge z <_{\mathrm{Pow}_p^e} u\big)\Big). \end{aligned}$$

(This formula is not suitable for $p = 2$, $e = 2$. In this case we know by Theorem 2.3 that all arithmetical relations are definable. Hence in this case Lemma 4.5 holds, too; however, we shall not need it.) □

Lemma 4.6. *If* (3.1) *holds then*

$$\begin{aligned} & \mathrm{Pow}_p(x) \wedge \mathrm{Pow}_p(y) \wedge NearP_p^e(x) \neq NearP_p^e(y) \implies \\ & \qquad \implies \big(x < y \iff NearP_p^e(x) <_{\mathrm{Pow}_p^e} NearP_p^e(y)\big). \end{aligned} \tag{4.3}$$

The proof is easy. As we can see, the predicates from Lemma 4.5 help us very much in defining of $<_{\mathrm{Pow}_p}$: we are already able to compare the powers of p which are far from each other. A further help (for near powers of p) will be given by the functions $F_p^{e,i}$ introduced in the following lemma.

Lemma 4.7. *Let* (3.1) *hold and let* $i > n$ *or* $k > 1$. *If the constant* p^i *is first order definable in the structure* $\langle \mathbb{N}; B_p, \mathrm{Pow}^e \rangle$ *then the unary function*

$$F_p^{e,i}(x) = \begin{cases} p^i x & \text{if } \mathrm{Pow}_p^e(x), \\ 0 & \text{otherwise} \end{cases} \tag{4.4}$$

also is first order definable in this structure.

Proof. In the structure $\langle \mathbb{N}; B_p, \mathrm{Pow}^e \rangle$ we can define the constants $0,\ 1,\ \dots,\ p-1$ and the binary predicates

$$\mathrm{B}_p^i(x,y) \iff B_p(x,y) = i, \qquad i = 0,1,\dots,p-1.$$

Conversely, the function B_p is definable in the structure

$$\langle \mathbb{N}; \mathrm{B}_p^0, \mathrm{B}_p^1, \dots, \mathrm{B}_p^{p-1}, 1, \mathrm{Pow}^e \rangle. \tag{4.5}$$

Therefore we may consider the structure (4.5) instead of $\langle \mathbb{N}; B_p, \mathrm{Pow}^e \rangle$. (Also the structure $\langle \mathbb{N}; \mathrm{B}_p^0, \mathrm{B}_p^1, 1, \mathrm{Pow}^e \rangle$ would suffice.)

Notice that for every $s \in \mathrm{Pow}_p^e$ the structure

$$\langle \{sx \mid x \in \mathbb{N}\}; \mathrm{B}_p^0, \mathrm{B}_p^1, \dots, \mathrm{B}_p^{p-1}, s, \{sx \mid x \in \mathrm{Pow}^e\} \rangle \tag{4.6}$$

(where B_p^i are suitably restricted) is isomorphic to (4.5). Further, by Lemma 3.2 there is $x \in \mathrm{Pow}^e$ such that $p^i \sqsubseteq_p sx$.

Let us consider now the expression p^i as a constant symbol and let

$$y = p^i \iff \alpha(y)$$

be a definition of p^i in the structure (4.5). We may assume that the variables x, x_1 do not occur in $\alpha(y)$.

Now we shall distinguish two cases. Let us assume $k > 1$ or $n = 0$ at first. Let $\beta(x,z)$ be the formula

$$\forall u \big(\mathit{NearP}_p^e(u) \leq_{\mathrm{Pow}_p^e} x \wedge u \sqcap_p x = 0 \implies u \sqcap_p z = 0 \big)$$

For $x \in \mathrm{Pow}_p^e$ the formula $\beta(x,z)$ expresses that z is a multiple of x. Then $F_p^{e,i}$ can be defined by the formula

$$y = F_p^{e,i}(x) \iff \mathrm{Pow}_p^e(x) \wedge \beta(x,y) \wedge \alpha^*(y) \vee \neg\, \mathrm{Pow}_p^e(x) \wedge y = 0,$$

where $\alpha^*(y)$ arises from $\alpha(y)$ by replacing the constant 1 by the variable x and by relativization of all bounded variables to $\beta(x,\cdot)$. The relativizaton $\gamma^\bullet$ of a formula γ (not containing x) to $\beta(x,.)$ is defined recursively:

$$\gamma^\bullet = \gamma, \qquad \text{and} \qquad [\gamma_1 \wedge \gamma_2]^\bullet = \gamma_1^\bullet \wedge \gamma_2^\bullet$$

for any atomic formula γ, arbitrary formulas γ_1, γ_2 and any logical connective instead of $\wedge$ (with the obvious modification for $\neg$), and

$$[\forall u\ \gamma]^\bullet = \forall u\big(\beta(x,u) \implies \gamma^\bullet\big), \qquad [\exists\ u\gamma]^\bullet = \exists u\big(\beta(x,u) \wedge \gamma^\bullet\big)$$

for arbitrary (here admissible) formula γ and variable u.

The second case is a little more complicated. If $k = 1$ and $n > 0$ we cannot express the property "z is a multiple of x" so directly as above. We shall express a weaker property which will depend on a further parameter x_1. Let

$$X = \big\{xp^j \mid 1 \leq j \leq n\big\} \cup \big\{z \in \mathrm{Pow}_p \mid z < x\big\};$$

it is important that $p^i \notin X$. Further, for $x \in \mathrm{Pow}^e$ and x_1 the sum of a subset of X denote

$$M(x,x_1) = \big\{z \in \mathbb{N} \mid (\forall u \in X)(u \sqsubseteq_p z \implies u \sqsubseteq_p x_1)\big\}$$

Let $\beta_0(x,x_1)$ and $\beta(x,x_1,z)$ be formulas which for $x \in \mathrm{Pow}_p^e$ express the properties
"x_1 is the sum of n distinct powers of p from the set X" and
"u belongs to $M(x,x_1)$";
they can be easily written. If $x \in \mathrm{Pow}_p^e$ and $x_1 = x \cdot \sum_{i=1}^n p^i$ then $\beta_0(x,x_1)$ holds and $\beta_1(x,x_1,z)$ expresses that z is a multiple of x. However, the formula $\beta_0(x,x_1)$ does not uniquely determine x_1 as a function of x (and it is not clear how to write such formula). Nevertheless, whenever $\mathrm{Pow}_p^e(x)$ and $\beta_0(x,x_1)$ hold, the structure

$$\big\langle M(x,x_1); \mathrm{B}_p^0, \mathrm{B}_p^1, \ldots, \mathrm{B}_p^{p-1}, s, \mathrm{Pow}^e \cap M(x,x_1)\big\rangle$$

(with B_p restricted to $M(x,x_1)$) is isomorphic to the structure (4.6) (and (4.5), too). Therefore $F_p^{e,i}$ can be defined by the formula

$$\begin{aligned} y = F_p^{e,i}(x) \iff{}& \mathrm{Pow}_p^e(x) \wedge \forall x_1\big(\beta_0(x,x_1) \implies \beta_1(x,x_1,y) \wedge \alpha^*(y)\big) \vee \\ & \vee \neg\, \mathrm{Pow}_p^e(x) \wedge y = 0, \end{aligned}$$

where $\alpha^*(y)$ arises from $\alpha(y)$ by replacing the constant 1 by the variable x and by relativization of all bounded variables to $\beta_1(x,x_1,\cdot)$. The relativization to $\beta_1(x,x_1,.)$ is defined similarly as the relativization to $\beta(x,\cdot)$ above. □

Theorem 4.8. (Reduction Theorem.) *For every pair of integers $p > 1$, $e > 1$, the operations $+$, $\times$ are first order definable in the structure $\langle \mathbb{N}; B_p, \mathrm{Pow}^e \rangle$ if and only if the constants p^i, $i = 1, \ldots, e-1$ are first order definable in the structure $\langle \mathbb{N}; B_p, \mathrm{Pow}^e, <_{\mathrm{Pow}_p^e}, NearP_p^e \rangle$.*

Proof. By Lemma 4.5 both structures above are equivalent from the definability point of view. Therefore the "only if" part of the theorem is obvious; we shall prove only the opposite part. Further, we need not consider the cases covered by Theorem 2.3 and Theorem 4.1. Therefore we may assume (3.1) and $k \geq 3$ or $n \leq 1$. By Lemma 4.7 we can transform definitions of the constants p^i into definitions of unary functions $F_p^{e,i}$. We can also define the function $F_p^{e,0}$ (using $<_{\mathrm{Pow}_p^e}$ and 0 only).

If $n = 1$, $k = 1$ we do not obtain the function $F_p^{e,1}$ immediately by Lemma 4.7, but nevertheless we can define it using the fact that the sets of positive values of $F_p^{e,i}$, $0 \leq i < e$ form a partition of $\mathrm{Pow}^e \setminus \{0\}$. (Another way is to define p^{e+1}, then $F_p^{e,e+1}$, and using it and the constant p^1 the function $F_p^{e,1}$.)

Using the functions $F_p^{e,i}$ we can define

$$\begin{aligned} x <_{\mathrm{Pow}_p} y \iff & \exists u, v \Big(u <_{\mathrm{Pow}_p^e} v \wedge \bigvee_{i=0}^{e-1} x = F_p^{e,i}(u) \wedge \bigvee_{i=0}^{e-1} y = F_p^{e,i}(v) \Big) \vee \\ & \vee \exists u \Big(\mathrm{Pow}_p^e(u) \wedge \bigvee_{i=0}^{e-2} \bigvee_{j=i+1}^{e-1} \big(x = F_p^{e,i}(u) \wedge y = F_p^{e,j}(u) \big) \Big) \end{aligned}$$

(Remark: If $k > 1$ or $n = 0$ we may replace the first member on the right by $\mathit{NearP}_p^e(x) <_{\mathrm{Pow}_p^e} \mathit{NearP}_p^e(y)$.) Now we can apply Theorem 2.7. □

Theorem 4.8 reduces the problem of definability od +, × to the definability of some constants. Its proof used some rather complicated metamathematical considerations (see Lemma 4.7). They can be avoided if we ask only a reduction to definability of unary functions $F_p^{e,i}$ from (4.4). The proof of the next theorem can be extracted from the proof above.

Theorem 4.9. *For every pair of integers $p > 1$, $e > 1$, the operations $+$, $\times$ are first order definable in the structure $\langle \mathbb{N}; B_p, \mathrm{Pow}^e \rangle$ if and only if the unary operations $F_p^{e,i}$, $i = 1, \ldots, e-1$ (see (4.4)) are first order definable in the structure $\langle \mathbb{N}; B_p, \mathrm{Pow}^e, <_{\mathrm{Pow}_p^e}, \mathit{NearP}_p^e \rangle$.*

We shall finish the present section by a conjecture. If it is true then we can replace "$i = 1, \ldots, e-1$" in the Reduction Theorem 4.8 by "$i = 1, \ldots, n$". This would be advantageous because, generally speaking, the bound n is much smaller than $e - 1$.

Conjecture 4.10. If (3.1) holds and $i > n$ then the constant p^i is first order definable in the structure $\langle \mathbb{N}; B_p, \mathrm{Pow}^e \rangle$.

The conjecture implies that for every $p > 1$, $e > 1$ the operations +, × are *parametrically* definable in the structure $\langle \mathbb{N}; B_p, \mathrm{Pow}^e \rangle$. Then the elementary theory of the structure $\langle \mathbb{N}; B_p, \mathrm{Pow}^e \rangle$ is undecidable because the structure $\langle \mathbb{N}; +, \times \rangle$ is interpretable in $\langle \mathbb{N}; B_p, \mathrm{Pow}^e \rangle$.

5. Concrete definability results

Generally speaking, Theorem 4.8 can be easily applied for small primes p and small exponents e. We shall start with the values $p=2$, $e=3$, the smallest ones not covered by Theorem 2.3 and Theorem 4.1; this case was left as an open problem in [Ko94].

Theorem 5.1. *The operations* $+$, $\times$ *are first order definable in the structure* $\langle \mathbb{N}; B_2, \mathrm{Pow}^3 \rangle$ *(and hence its elementary theory is undecidable).*

Proof. We shall show that the constants 2, 4 are definable in the structure

$$\langle \mathbb{N}; B_2, \mathrm{Pow}^3, <_{\mathrm{Pow}_2^3}, \mathit{NearP}_2^3 \rangle.$$

We can define 1, 8, 64 (using $<_{\mathrm{Pow}_2^3}$ only) and then

$$\begin{aligned} x = 27 &\iff \mathrm{Pow}^3(x) \wedge \neg\, \mathrm{Pow}_2(x) \wedge \mathit{NearP}_2^3(x) = 64, \\ x = 2 &\iff \mathrm{OP}_2^3(x) \wedge \mathit{NearP}_2^3(x) = 8 \wedge x \sqsubseteq_2 27, \\ x = 4 &\iff \mathrm{OP}_2^3(x) \wedge \mathit{NearP}_2^3(x) = 8 \wedge x \neq 2. \end{aligned}$$

Now we can apply Reduction Theorem 4.8. □

We shall give an alternative proof which will use neither Reduction Theorem 4.8 nor Lemma 4.7. So we avoid *some* metamathematical considerations. However, the mathematical (or: number-theoretical) ideas remain unchanged.

Proof II. We can define $<_{\mathrm{Pow}_2^3}$ and NearP_2^3 by Lemma 4.5, and then $\mathrm{TPow}_2^3 = \{2^{3i+1} \mid i \in \mathbb{N}\}$ by the formula

$$\begin{aligned} \mathrm{TPow}_2^3(x_1) \iff \exists x_0, x_3, x_4, x_6 \Big(& x_0 <_{\mathrm{Pow}_2^3} x_3 \wedge x_3 <_{\mathrm{Pow}_2^3} x_6 \wedge \\ & \wedge \forall z \big(x_0 <_{\mathrm{Pow}_2^3} z \wedge z <_{\mathrm{Pow}_2^3} x_6 \implies z = x_3 \big) \wedge \\ & \wedge \mathit{NearP}_2^3(x_1) = x_3 \wedge \mathit{NearP}_2^3(x_4) = x_6 \wedge \\ & \wedge \mathrm{OP}_2^3(x_1) \wedge \mathrm{OP}_2^3(x_4) \wedge \mathrm{Pow}^3(x_0 \sqcup_2 x_1 \sqcup_2 x_3 \sqcup_2 x_4) \Big). \end{aligned}$$

Indeed, the right-hand side expresses that x_0, x_3, x_6 are three consecutive powers of 2^3. Then it expresses that x_1, x_4 also are powers of 2 and

$$x_0 = 2^{3i}, \qquad x_1 = 2^{3i+u}, \qquad x_3 = 2^{3i+3}, \qquad x_4 = 2^{3i+3+v}, \qquad x_6 = 2^{3i+6}$$

for some $i \in \mathbb{N}$ and $u, v \in \{1, 2\}$. Finally, the definition expresses that

$$x_0 \sqcup_2 x_1 \sqcup_2 x_3 \sqcup_2 x_4 = x_0 + x_1 + x_3 + x_4 = 2^{3i} \cdot \left(1 + 2^u + 2^3 + 2^{3+v}\right)$$

is a cube. This is possible if and only if $u = v = 1$, and hence $\mathrm{TPow}_2^3(x_1)$.

Using TPow_2^3 we can define

$$x <_{\mathrm{Pow}_2} y \iff \mathrm{Pow}_2(x) \wedge \mathrm{Pow}_2(y) \wedge \Big(\mathit{NearP}_2^3(x) <_{\mathrm{Pow}_2^3} \mathit{NearP}_2^3(y) \vee$$
$$\vee\, \mathit{NearP}_2^3(x) = \mathit{NearP}_2^3(y) \wedge x \neq y \wedge \big(\mathrm{TPow}_2^3(x) \vee \mathrm{Pow}_2^3(y)\big)\Big).$$

Now we can apply Theorem 2.7. ☐

Theorem 5.2. *For every pair if integers* (p,e), $2 \le p \le 20$, $2 \le e \le 20$ *except* $p = 2$, $e > 2$ *even and* $p = 3$, $e = 9, 18$ *the operations* $+$, $\times$ *are first order definable in the structure* $\langle \mathbb{N}; B_p, \mathrm{Pow}^e \rangle$. *In the listed exceptional cases the operations* $+$, $\times$ *are not definable.*

Proof. For p composed we can apply Theorem 2.3. The cases of undefinability are covered by Theorem 4.1. For every of the other cases we shall apply Theorem 4.8 (or Theorem 4.9; then little modifications are necessary).

Definability of the necessary constants will be shown as follows. We shall define a finite directed edge-labelled, vertex-coloured complete bipartite graph. (At least in principle we must be able to define all its components by first order formulas in the language of $\langle \mathbb{N}; B_p, \mathrm{Pow}^e \rangle$ or, equivalently, of $\langle \mathbb{N}; B_p, \mathrm{Pow}^e, <_{\mathrm{Pow}_p^e}, \mathit{NearP}_p^e \rangle$.) The first group of its vertices will contain some e-th powers relatively prime to p. The second group of vertices will contain some powers of p, including all constants which we need to define (for applying Theorem 4.8). Every edge goes from a vertex of the first group into a vertex of the second group. It is labelled by a p-adic digit in the obvious way (derived from the p-adic representation of the first vertex). If a vertex of the constructed graph is preserved by all its automorphisms then it is definable (as a constant). We shall show that every automorphism of the graph preserves every constant necessary for applying Reduction Theorem 4.8; so we shall show that these constants are definable. The defining formulas will not be explicitly written because they can be rather long. (However, they could be written without any principal difficulties.)

The above construction will be done with the aid of computer. In the table constructed below rows and columns correspond to the first and the second group of vertices, respectively. C-groups and R-groups corresponds to colouring of vertices, and p-adic digits in the table correspond to labelling of edges. For every pair (p,e) we shall perform the following steps (1)–(5); an explanation is added to every step.

(1) *Computation of a table of e-th powers.* The powers x^e for small (never exceeding 50) positive integers x relatively prime to p are computed in p-adic number system. The bound for x must be "guessed"; usually $p^m + 1$ for some $m \le 2$ is suitable. Only for $p = 2$ we sometimes need $m = 5$, and for $p = 3$ we sometimes need $m = 3$. Notice that we shall need at most $2e+2$ lowest digits of x^e; the other digits need not be computed (and displayed). The computed digits are displayed in a table; an example for $(p,e) = (2,19)$ is given in Table 1. Its rows correspond to the computed x^e and its columns to the powers of p in the obvious way. The heading

Table 1. The case $p = 2$, $e = 19$.

$p=2$	...9	**8**765432109876543210	**9**876543210987654321	**0**	*sums*
1^{19}				**1**	0, 0
3^{19}		10001010100	**0**110101100111101101	**1**	4, 12
5^{19}	0	**1**011000111001000110	**0**000100100010011110	**1**	9, 7
7^{19}	0	**0**111100000110100101	**1**011001001111101011	**1**	9, 12
9^{19}	0	**1**111010111010000001	**1**111111111010101100	**1**	10, 14
11^{19}	1	**0**111010011000111011	**1**100000110010111001	**1**	11, 9
13^{19}	1	**0**000010110001000110	**0**001001000011101010	**1**	6, 7
15^{19}	0	**1**001000000010111101	**0**111111001100010111	**1**	8, 12
17^{19}	1	**0**011000001000100010	**0**001001111000011000	**1**	5, 7
19^{19}	0	**1**111001111011011011	**1**001000010111000101	**1**	14, 8
21^{19}	1	**0**000010001000001010	**0**000011010011110110	**1**	4, 9
23^{19}	1	**0**110101110111011111	**0**110101001110000011	**1**	14, 9
25^{19}	0	**0**010001111010000010	**0**110001010001000100	**1**	7, 6
27^{19}	0	**1**111011001101001101	**1**000111101100010001	**1**	12, 9
29^{19}	1	**0**001010010011110001	**0**001110101011000010	**1**	8, 8
31^{19}	0	**1**111010111001111010	**0**001110101100101111	**1**	13, 11
33^{19} ...	0 ...	**1**111010110011000010 ...	**0**111001011100110000 ...	**1** ·	10, 9 ...
Equal c.s. in $[3^{19}..15^{19}, 18..1]$: $(15,3)$, $(8,4)$,					
Equal c.s. in $[3^{19}..19^{19}, 18..1]$: None.					

column contains the considered elements of Pow^e. From technical reasons the heading row of the table contains only the last (decadic) digits of the corresponding exponents (e.g., 7 instead of 2^7, 2^{17} or 2^{27}).

This is the most troublesome part of the algorithm, where the aid of computer is most useful. All further steps can be easily done by a pencil on a sheet of paper. Of course, they also could be (and were) performed by computer.

(2) *Partitioning of columns using the function* $NearP_p^e$. All displayed columns (or: the corresponding powers of p) are divided into groups with the same value of $NearP_p^e$. These groups are separated by (thin) vertical lines. Moreover, the columns corresponding to the elements of Pow_p^e are written in bold. (Compare with Example 4.4, where the same partition of powers of p is presented.) These groups of columns will be called C-groups. Below we shall deal only with those C-groups which are completely displayed (i.e., only the elements of these groups will be vertices of the graph mentioned above). We need at most three such groups.

(3) *Partitioning of rows using the function* $NearP_p^e$. R-groups of rows (or of the numbers in their headings) will be introduced similarly as the C-groups of columns.

Table 2. Several cases for $p = 3$.

$p=3$	…4	**3**21	**0**
1^3			**1**
2^3		2	**2**
4^3		**2**10	**1**
…	…	…	•

$p=3$	…5	**4**321	**0**
1^4			**1**
2^4		12	**1**
4^4	1	**0**011	**1**
…	…	…	•

$p=3$	…6	5**4**3210987654	3**2**1098765432	1**0**	*sums*
1^{12}				**1**	0, 0
2^{12}			121212	0**1**	0, 9
4^{12}		10	1**1**1201010001	0**1**	1, 8
5^{12}		1220	0**0**1011212221	0**1**	5, 13
7^{12}		10222011	2**1**2110201122	0**1**	9, 15
8^{12}		201201010	1**1**2110100120	0**1**	7, 10
10^{12}		1**0**1121210112	0**1**1021021110	0**1**	13, 10
11^{12}	1	0**2**0100002111	1**0**2001021002	0**1**	8, 9
…	…	…	…	. •	…
Equal c.s. in $[2^{12}..8^{12}, 13..2]$: None.					

$p=3$	…4	3**2**1098	7**6**5432	1**0**	*sums*
1^6				**1**	0, 0
2^6			21	0**1**	0, 3
4^6			1**2**1212	0**1**	0, 9
5^6		2	1**0**1022	0**1**	2, 6
7^6		122	2**2**1011	0**1**	5, 7
8^6		1110	2**2**1210	0**1**	3, 8
10^6		**1**2122	1**0**2020	0**1**	8, 5
11^6		1**0**1000	0**0**0101	0**1**	2, 2
13^6	1	0**0**0020	2**0**0102	0**1**	2, 5
…	…	…	…	. •	…
Equal c.s. in $[2^6..7^6, 7..2]$: None.					

$p=3$	…1	**0**987654321	**0**	*sum*
1^{10}			**1**	0
2^{10}		110122	**1**	7
4^{10}	2	**2**202110101	**1**	10
5^{10}	1	**0**101022021	**1**	9
7^{10}	1	**1**202001202	**1**	10
8^{10}	1	**0**220121220	**1**	12
10^{10}	2	**0**212201010	**1**	9
…	…	…	•	…
Equal c.s. in $[2^{10}..7^{10}, 9..1]$: $(9,7)$,.				
Equal c.s. in $[2^{10}..8^{10}, 9..1]$: None.				

We shall classify the rows by the positions of their leftest nonzero digits (not only displayed ones!). Two rows will belong to distinct R-groups if their leftest nonzero digits

(a) either belong to distinct C-groups,

(b) or they belong to the same C-group, but one of them is bold and the other thin.

The case (b) is not considered if the bold column is not the leftest one in a C-group. It correspond to the case $k = 1$, $n = 1$ in (3.1). There are three such cases among those which we now consider, (p, e) equal to $(3, 6)$, $(3, 12)$ and $(5, 20)$. The cases with $p = 3$ can be found among the examples of Table 2, the last one is in Table 3.

The R-groups are separated from each other by (thin) horizontal lines. For all cases except the three just mentioned we can simply draw horizontal lines between $(p^m - 1)^e$ and $(p^m + 1)^e$ for any integer $m > 0$. (No mistake arises when we “forget” a horizontal line.)

Below we shall deal only with those R-groups which are completely displayed. (The lowest displayed row is used only to show that the previous

Table 3. The case $p = 5$, $e = 20$.

$p = 5$	...2	1**0**987654321098765432	1**0**987654321098765432	1**0**	*sums*
1^{20}				**1**	0, 0
2^{20}			2320233	0**1**	0, 15
3^{20}			241201041001	0**1**	0, 16
4^{20}			1210032444340421	0**1**	0, 35
6^{20}		1	2**3**132044444411240034	0**1**	1, 50
7^{20}		113	2**1**320124423341420410	0**1**	5, 43
8^{20}		3413	2**4**112114124133231004	0**1**	11, 40
9^{20}		130344	1**2**140113401220332102	0**1**	15, 33
11^{20}		33012141	3**4**443134333403302433	0**1**	15, 57
12^{20}		402423440	2**2**042122244121124022	0**1**	23, 40
13^{20}		4020040014	2**3**434001213341240202	0**1**	15, 41
14^{20}		32440434014	4**1**001003312331444143	0**1**	29, 42
16^{20}		2014301411430	0**2**120120410222110442	0**1**	24, 31
17^{20}		11442343142304	2**4**241023120112133224	0**1**	36, 40
18^{20}		41422312412230	2**3**204313211001234440	0**1**	31, 40
19^{20}		224242143040403	1**2**044304343344443344	0**1**	35, 61
21^{20}		3402441434022100	1**2**313131331021102411	0**1**	34, 34
22^{20}		14321424403424210	4**0**433223300142133121	0**1**	41, 42
23^{20}		43243131312124143	4**4**434001203020041213	0**1**	42, 38
24^{20}		210111121000212134	1**4**121010422244322410	0**1**	23, 40
26^{20}		**2**043421122143244002	1**1**001340224430423040	0**1**	41, 38
27^{20}		**4**312302211430044322	1**1**012113342333333303	0**1**	41, 43
28^{20}		1**4**310343131044330313	1**0**134032232302122331	0**1**	45, 38
29^{20}		3**4**212244140400413030	2**0**300323430313344431	0**1**	42, 46
31^{20} ...	2 ...	4**3**413002132234000144 ...	1**0**103323400100012224 ...	0**1** ..	41, 29 ...
Equal c.s. in $[2^{20}..6^{20}, 21..2] : (20, 18)$,					
Equal c.s. in $[2^{20}..7^{20}, 21..2]$: None.					

R-group is complete. It does not correspond to any vertex of the graph above.)

(4) *Distinguishing the rows in every R-group.* A permutation of columns will be called *C-permutation* if it preserves C-groups and bold-written columns. For every row we can compute some numerical values which are invariant with respect to all C-permutations. Such invariants are e.g. the sums of digits in fixed C-groups, and also the digits in bold-written columns. (One or two such sums are sometimes written in the additional column of the table.) If the values of invariants for the rows of an R-group are pairwise distinct we can distinguish the rows, and hence we can define the corresponding elements of Pow^e.

(5) *Distinguishing of columns in the important C-group.* All constants which we need to define belong to one C-group which will be called *important.*

(The exception is p^1 for (p, e) equal to $(3, 6)$, $(3, 12)$, or $(5, 20)$. However, in these cases we can define p^1 by the property that the corresponding column contains 0 only; so we need not consider p^1 more.) We can choose several consecutive rows distinguished in the previous point, and compare the corresponding segments of columns in the important C-group. If these segments are pairwise distinct we can distinguish, and hence define, the corresponding powers of p. Notice that the simplest way is to choose all distinguished rows. However, sometimes much shorter segments of columns suffice, and verifying with them is easier.

The information about distinguishing columns is given in the additional row of the table. In Table 1 we can see that the rows from 3^{19} to 15^{19} do not suffice; the columns (associated to) 2^{15} and 2^3, and also the columns 2^8 and 2^4, would remain undistinguished. The rows from 3^{19} to 19^{19} suffice. However, to obtain them we had to consider the whole new R-group; therefore we had to compute the rows up to 33^{19}. (Two additional rows were joined to one table only for illustration; they arose in two different computations.) On the other hand, the third C-group (from the right) can be avoided; hence a narrower table (with the columns up to 2^{20}) would suffice. (We can define 17^{19} and 19^{19} using the last sums and bold digits. We need not distinguish 21^{19} and 23^{19}, although it is possible by a more complicated consideration.)

All cases from Theorem 5.2 were verified by computer (and ended with success, i.e. with the word "None" in the additional row.) We shall show the tables for several of them, and we shall comment some of the displayed tables.

Table 4. The cases $p = 2$, $e = 5, 7$.

$p = 2$	...1	**0**9876	**5**4321	**0**	*sums*
1^5				**1**	0, 0
3^5		11	**1**1001	**1**	2, 3
5^5	1	**1**0000	**1**1010	**1**	1, 3
7^5	0	**0**0110	**1**0011	**1**	2, 3
9^5	0	**1**1010	**1**0100	**1**	3, 2
11^5	0	**1**0100	**0**1101	**1**	2, 3
13^5	1	**0**1001	**0**1110	**1**	2, 3
15^5	0	**1**1001	**0**0111	**1**	3, 3
17^5	1	**0**1001	**0**1000	**1**	2, 1
...	...	...	...	.	...
Equal c.s. in $[3^5..7^5, 4..1]$: None.					

$p = 2$	...5	**4**321098	**7**654321	**0**	*sums*
1^7				**1**	0, 0
3^7		1000	**1**000101	**1**	1, 3
5^7	0	**0**110001	**0**010110	**1**	3, 3
7^7	1	**0**010000	**1**111011	**1**	1, 6
9^7	1	**1**111011	**0**111100	**1**	6, 4
11^7	0	**1**011001	**1**100001	**1**	4, 3
13^7	0	**1**110111	**0**110010	**1**	6, 3
15^7	0	**0**011011	**0**110111	**1**	4, 5
17^7	0	**1**000101	**0**111000	**1**	3, 3
...	...	...	...	.	...
Equal c.s. in $[3^7..15^7, 6..1]$: None.					

Remember that for $p = 2$ we need consider only odd exponents, and that the case $p = 2$, $e = 3$ was considered in Theorem 5.1. Two further cases, $e = 5$ and $e = 7$, are considered in Table 4. We can see that for $e = 5$ the R-group from 9^5 to 15^5 is unnecessary (and a table with the last row for 9^5 would suffice). Similarly in the table for $e = 7$ the columns up to 2^8 would suffice. Then we would know only the right-hand numbers from the additional columns *sums*, and they would not distinguish the rows 11^7 and 13^7. However, these rows can be distinguished by the bold-written column associated to 2^7.

Some examles for $p = 3$ are presented in Table 2. We can see that for $e = 3$ and $e = 4$ one-element R-groups $\{2^3\}$ and $\{2^4\}$ suffice. (The same was true for $p = 2$, $e = 3$ in Theorem 5.1 with the R-group consisting of 3^3.) Two additional rows for $e = 10$ arose from distinct computations.

Let us consider once more the case $p = 5$, $e = 20$ presented in Table 3. Notice the position of second thin horizontal line. Also notice that we have to consider the R-group from 6^{20} to 29^{20}. We need only its elements 6^{20} and 7^{20} in the last step. However, the whole group had to be computed because we must distinguish these element from the other elements of the group. The sums in the additional column can help us. (The program did not distinguish the bold-written columns in the last step. If it would do, then the element 7^{20} also became unnecessary.)

Table 5. The cases $p = 7$, $e = 12, 14$.

$p = 7$	`...3`	**2**`10987654321`	**0**	*sum*
1^{12}			**1**	0
2^{12}		`1464`	**1**	15
3^{12}		`434225`	**1**	20
4^{12}		`26241411`	**1**	21
5^{12}		`602310615`	**1**	24
6^{12}		`10464122612`	**1**	29
8^{12}		**4**`65163462545`	**1**	51
...	...	...	**.**	...
Equal c.s. in $[2^{12}..6^{12}, 11..1]$: None.				

$p = 7$	`...5`	**4**`3210987654321`	**0**	*sum*
1^{14}			**1**	0
2^{14}		`6552`	**4**	18
3^{14}		`5544034`	**2**	25
4^{14}		`643644344`	**2**	38
5^{14}		`30415201212`	**4**	21
6^{14}		`544263625550`	**1**	47
8^{14}		**6**`3251445634620`	**1**	51
...	...	...	**.**	...
Equal c.s. in $[2^{14}..6^{14}, 13..1]$: None.				

Up to now we have no example for $p = 7$; Table 5 contains two such examples. Without displaying the table notice that for $p = 7$, $e = 18$ we must consider the rows up to 50^{18} because we need the R-group from 8^{18} to 48^{18}.

Several cases for $p = 11$ are displayed in Table 5. The letter `A` (or **A**) is used as the digit for "ten". The tables are displayed without additional rows and columns. (All computations finished with success; in the last steps the rows 8^e, 9^e and 10^e were used). Here we can see that the algorithm presented above could be modified so that the step (4), distinguishing of rows, will be deleted, and the numbers of digits through the R-group from 2^e to $(p-1)^e$ are computed for all columns of the important C-group. (These numbers are obviously invariant under any permutation of the considered R-group.) Generally speaking, this variant probably would be successful if p is not too small with respect to e. (This is more a heuristics than an exact statement. However, we can see that the mentioned variant cannot be successful whenever $(p-1)^e < p^{e-2}$.)

Similarly all remaining cases can be considered. □

Table 6. Several cases for $p = 11$.

$p = 11$	...	**0** 9876543210987654321	**0**
1^{20}			**1**
2^{20}		6568A	**1**
3^{20}		152A22080	**1**
4^{20}		39433371679	**1**
5^{20}		28429111A3463	**1**
6^{20}		969A680A561A5A	**1**
7^{20}		18113303112A0204	**1**
8^{20}		23100035A301A3978	**1**
9^{20}		22064A2983178A2150	**1**
10^{20}		16A9322885328081A12	**1**
12^{20}		**5** 7759873033176540249	**1**
...	...	...	•

$p = 11$	...	**3** 210987654321	**0**
1^{13}			**1**
2^{13}		617	**8**
3^{13}		99992	**5**
4^{13}		3497697	**9**
5^{13}		57706736	**4**
6^{13}		55A246A7A	**7**
7^{13}		380AA35862	**2**
8^{13}		1A217190894	**6**
9^{13}		89AAA9AA280	**3**
10^{13}		3205A8133401	**A**
12^{13}		**3** 110062214722	**1**
...	...	...	•

$p = 11$	...	**3** 21	**0**
1^{3}			**1**
2^{3}			**8**
3^{3}		2	**5**
4^{3}		5	**9**
5^{3}		10	**4**
6^{3}		18	**7**
7^{3}		29	**2**
8^{3}		42	**6**
9^{3}		60	**3**
10^{3}		82	**A**
12^{3}		**1** 33	**1**
...	...	...	•

$p = 11$	...	**4** 321	**0**
1^{4}			**1**
2^{4}		1	**5**
3^{4}		7	**4**
4^{4}		21	**3**
5^{4}		51	**9**
6^{4}		A7	**9**
7^{4}		189	**3**
8^{4}		309	**4**
9^{4}		4A2	**5**
10^{4}		757	**1**
12^{4}		**1** 464	**1**
...	...	...	•

$p = 11$	...	**5** 4321	**0**
1^{5}			**1**
2^{5}		2	**A**
3^{5}		20	**1**
4^{5}		85	**1**
5^{5}		239	**1**
6^{5}		592	**A**
7^{5}		1169	**A**
8^{5}		2268	**A**
9^{5}		4040	**1**
10^{5}		6914	**A**
12^{5}		**1** 5AA5	**1**
...	...	...	•

$p = 11$	...	**5** 43210987654321	**0**
1^{15}			**1**
2^{15}		2268	**A**
3^{15}		811060	**1**
4^{15}		50111014	**1**
5^{15}		11A4041715	**1**
6^{15}		17144A19108	**A**
7^{15}		157047A78167	**A**
8^{15}		1023567687584	**A**
9^{15}		5A66AA3655110	**1**
10^{15}		26A6A368906563	**A**
12^{15}		**3** 7631741796A274	**1**
...	...	...	•

$p = 11$	...	**6** 543210987654321	**0**
1^{16}			**1**
2^{16}		4526	**9**
3^{16}		2233170	**3**
4^{16}		190444055	**4**
5^{16}		5979198273	**5**
6^{16}		998475AA649	**5**
7^{16}		A653008A2030	**4**
8^{16}		8176095A35216	**3**
9^{16}		49747A4A351990	**9**
10^{16}		24373432025A086	**1**
12^{16}		**4** 029490596561A05	**1**
...	...	...	•

The additional row is $\boxed{\text{Equal c.s. in } [8^e..10^e, (e-1)..1]\text{: None.}}$ for every current e.

There are some possibilities to optimalize the presented algorithm. However, it has sense only for much bigger values of p, e, and neither such optimalization nor obtaining of further theoretical results will be considered in the present paper.

Table 7. Some cases of non-definability.

$p=2$	...32	10987**6**5432109876	54321**0**
1^{16}			**1**
3^{16}	10	01000**0**1101011101	00000**1**
5^{16}	11	11001**0**0110111111	00000**1**
7^{16}	00	00010**1**0111110110	00000**1**
9^{16}	00	01111**0**0011111010	00000**1**
11^{16}	00	00101**1**0001101011	00000**1**
13^{16}	00	00001**0**0010010001	00000**1**
15^{16}	11	11100**1**0111011100	00000**1**
17^{16}	00	11111**1**0111100100	00000**1**
19^{16}	10	01100**0**1111101001	00000**1**
21^{16}	01	01110**0**0011010011	00000**1**
...	...	...	......

$p=2$	...**2**	109**8**	765**4**	321**0**
1^4				**1**
3^4			10**1**	000**1**
5^4		1**0**	011**1**	000**1**
7^4		100**1**	011**0**	000**1**
9^4	**1**	100**1**	101**0**	000**1**
11^4	**1**	100**1**	001**1**	000**1**
13^4	**0**	111**1**	100**1**	000**1**
15^4	**0**	010**1**	110**0**	000**1**
17^4	**0**	011**0**	010**0**	000**1**
19^4	**1**	110**1**	000**1**	000**1**
21^4	**1**	011**1**	101**1**	000**1**
...	...	...	...	....

$p=3$	...210	**9**87654321	**0**
1^9			**1**
2^9		20022	**2**
4^9	11	**1**02212100	**1**
5^9	020	**0**02001122	**2**
7^9	022	**1**01120200	**1**
8^9	011	**2**22200222	**2**
10^9	020	**0**02101000	**1**
11^9	222	**0**01101022	**2**
13^9	102	**0**10110100	**1**
...	...	...	.

$p=3$	...321	09**8**765432109876543	21**0**
1^{18}			**1**
2^{18}		111022121	00**1**
4^{18}	20	12**0**101011211010012	00**1**
5^{18}	111	20**0**101210220110122	00**1**
7^{18}	201	21**1**010111100011111	00**1**
8^{18}	200	20**0**022122200101210	00**1**
10^{18}	011	10**0**201020220212020	00**1**
11^{18}	111	01**2**121002102021201	00**1**
13^{18}	021	20**1**020112000110202	00**1**
...	...	...	...

At the end we show in Table 7 several cases when the operations $+$, $\times$ are not definable. Horizontal lines were drown using bigger tables, but now they are not so important. It is substantial that in every case at least two columns are equal (and they will remain equal independently on the number of displayed rows). Therefore the corresponding powers of 2 or 3 cannot be distinguished. In the proof of Theorem 4.1 we used this idea.

References

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

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

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

[Bü60] Büchi, J. R., Weak second-order arithmetic and finite automata. Zeitschrift für Math. Logik und Grundlagen der Math. 6 (1960), 66-92.

[BL69] Büchi, J. R. — Landweber. Definability in the monadic second-order theory of successor. Journal for Symbolic Logic 34 (1969), 166-170.

[Ce95] Cegielski, P., Definability, decidability and complexity. Annals of Mathematics on Artificial Intelligence. 16 (1996) 311-341.

[Ko90] Korec, I., 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), 531-554.

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

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

[Ko95a] —, Theories of generalized Pascal triangles (Abstract). Bulletin of the Association for Symbolic Logic 1 (1995) 214-215

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

[Pu57] Putnam, H., Decidability and essential undecidability. Journal of Symbolic Logic 22 (1957), 39-54.

[Ro49] Robinson, J., Definability and decision problems in arithmetic. Journal of Symbolic Logic 14 (1949), 98-114.

[Sh67] Shoenfield, J. R., Mathematical logic. Addison Wesley, 1967. Russian translation: "Nauka", Moscow 1976.

[Vi49] I. M. Vinogradov, I. M., Fundamentals of Number Theory (in Russian). "Gostechizdat", Moscow 1949.

[Wo81] Woods, A. R., Some problems in number theory and their connections. PhD Thesis, University of Manchester 1981.

Address of author:

Mathematical Institute, Slovak Academy of Sciences,
Štefánikova 49, 814 73 Bratislava, Slovakia

E-mail: 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:

2/1997 *Ivan Korec*: Elementary definability from Pascal's triangle modulo p and the set of e-th powers

1/1997 *Ján Jakubík*: Lexicographic products of half linearly ordered groups

34/1996 *Emília Halušková*: Direct limits of monounary algebras

33/1996 *Ivan Korec*: A list of arithmetical structures strongest with respect to the first order definability

32/1996 *Ivan Korec*: Definability of Pascal's triangles modulo 4 and 6 and some other binary operations from their associated equivalence relations

31/1996 *Anatolij Dvurečenskij*: Measures and states on BCK-algebras

30/1996 *Ján Haluška*: Uncertainty and tuning in music

29/1996 *Ján Haluška*: On numbers 256/243, 25/24, 16/15

28/1996 *Ján Haluška*: COMMA 32 805/32 768

27/1996 *Beloslav Riečan*: On the sum of observables in MV algebras of fuzzy sets

26/1996 *Beloslav Riečan*: On the strong law of large numbers for weak observables in MV algebras

25/1996 *Ivan Korec*: Algebraical constructions of reversible generalized Pascal triangles and one–dimensional cellular automata

24/1996 *Peter Vojtáš*: Uncertain reasoning with floating connectives

23/1996 *Ivan Korec*: Definability of addition from multiplication and neighbourhood relation and some related results

22/1996 *Ivan Korec*: Open problems more or less related to generalized Pascal triangles

21/1996 *Sylvia Pulmannová*: On connections among some orthomodular structures

20/1996 *Pekka Lahti, Sylvia Pulmannová*: Coexistent observables and effects in quantum mechanics

19/1996 *Ivan Korec*: Definability of arithmetical operations from Pascal's triangle modulo n and arithmetical functions

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

(continued on inside back cover)

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