FUNDAMENTA
MATHEMATICAE
156 (1998)

Definability within structures related to Pascal's triangle modulo an integer

by

Alexis B è s (Paris) and **Ivan K o r e c** (Bratislava)

Abstract. Let Sq denote the set of squares, and let SQ_n be the squaring function restricted to powers of n; let $\perp$ denote the coprimeness relation. Let $B_n(x,y) = \binom{x+y}{x}$ MOD n. For every integer $n \geq 2$ addition and multiplication are definable in the structures $\langle \mathbb{N}; B_n, \perp \rangle$ and $\langle \mathbb{N}; B_n, \mathrm{Sq} \rangle$; thus their elementary theories are undecidable. On the other hand, for every prime p the elementary theory of $\langle \mathbb{N}; B_p, \mathrm{SQ}_p \rangle$ is decidable.

1. Introduction. Since Julia Robinson's result [Ro] that $+$ and $\times$ are first-order definable in the structure $\langle \mathbb{N}; S, | \rangle$, where $\mathbb{N}$ denotes the set of nonnegative integers, S stands for the successor function and $|$ for the divisibility relation, there have been many works on definability within fragments of arithmetic, which showed deep connections with number theory and automata theory—see e.g. [BJW], and the survey papers [BHMV], [Ce]. The field is obviously related to the study of decidability of logical theories: one often proves undecidability of a theory by means of definability techniques, and in turn decidability arguments can be used for proving undefinability of properties (see e.g. [MMT]).

For every $n \in \mathbb{N}$, the *Pascal triangle modulo* n is the binary function on $\mathbb{N}$ defined by

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

where $\binom{\cdot}{\cdot}$ denotes the binomial coefficient, and MOD denotes the remainder by integer division.

Arithmetical properties of Pascal triangles modulo n have been widely investigated (see e.g. [Di], [Bo], [Si]). In this paper we study definability and

1991 *Mathematics Subject Classification*: Primary 11B65, 03B25; Secondary 11U05, 03F30.

Key words and phrases: Pascal's triangle modulo n, decidability, definability.

The second author was supported by Grant 1227/94 of Slovak Academy of Sciences.

decidability questions related to structures containing B_n and some extra predicate or function. Let us recall some known results in this area:

- If $n \geq 2$ has (at least) two distinct prime divisors then addition and multiplication are definable in the structure $\langle \mathbb{N}; B_n \rangle$; thus its elementary theory is undecidable [Ko1].
- If $n \geq 2$ is a prime number then the elementary theory of $\langle \mathbb{N}; B_n, + \rangle$ is decidable [Ko3].
- If $n \geq 2$ is a prime power but not a prime then addition is definable in $\langle \mathbb{N}; B_n \rangle$; moreover, the elementary theory of $\langle \mathbb{N}; B_n \rangle$ (or $\langle \mathbb{N}; B_n, + \rangle$) is decidable [Be].

In Section 3 we study the structure $\langle \mathbb{N}; B_n, \perp \rangle$, where $\perp$ denotes the coprimeness relation (i.e. $x \perp y$ if and only if x and y have no common prime divisor). We use arithmetical results of Richard to define $+$ and $\times$ in this structure, from which we deduce the undecidability of its elementary theory. In Section 4 we consider the structure $\langle \mathbb{N}; B_n, \mathrm{Sq} \rangle$, where Sq denotes the set of squares; this time again, defining $+$ and $\times$ we prove that this structure has an undecidable elementary theory; this result was proved in [Ko2] for the case $n = 2$. We then investigate in Section 5 the structure $\langle \mathbb{N}; B_n, \mathrm{SQ}_n \rangle$, where SQ_n is the squaring function restricted to powers of n. It is shown that the elementary theory of $\langle \mathbb{N}; B_n, \mathrm{SQ}_n \rangle$ is decidable if and only if n is prime.

The equality sign will be considered as a logical symbol. Let $\mathcal{L}$ be a first-order language, and let $\mathcal{M}$ be an $\mathcal{L}$-structure with domain M. Recall that an n-ary relation R over M is *definable* in $\mathcal{M}$ if and only if there exists a first-order $\mathcal{L}$-formula φ with n free variables such that for all $a_1, \ldots, a_n \in M$, $R(a_1, \ldots, a_n)$ holds if and only if $\mathcal{M} \models \varphi[a_1, \ldots, a_n]$. In the same way, a function over M is definable in $\mathcal{M}$ if its graph is definable in $\mathcal{M}$.

Usually function symbols denote *total* functions; however, to simplify formal definitions we shall introduce function symbols denoting *partial* functions. These partial functions always have positive range and thus could be completed to total ones by the value 0 (which is definable in the structures we consider).

We do not distinguish between a function or predicate and the corresponding formal symbol for it.

2. Definability results for $\langle \mathbb{N}; B_n \rangle$. The section introduces auxiliary results and definitions which will be used throughout the paper. For every integer $n \geq 2$ and every $x \in \mathbb{N}$, we call any finite sequence $a_0, a_1, \ldots, a_k$ of nonnegative integers less than n such that $x = \sum_{0 \leq i \leq k} a_i n^i$ an *n-ary expansion* of x. We write $x = [a_k \ldots a_0]_n$, and the a_i's are called *digits* of the n-ary expansion. Since adding to the sequence $\langle a_i \rangle_{i \leq k}$ an arbitrary number of leading zero digits preserves the first equality, any integer has an infinite number of n-ary expansions, and for all integers x, y one can always find n-ary expansions of x and y with the same number of digits.

The following theorem, which is a slight modification of a result of Lucas ([Lu], see also [Fi]), relates the value of $\binom{x+y}{x}$ modulo p, for p prime, to the p-ary expansions of x and y.

THEOREM 2.1 (Lucas). *Let p be a prime. For any $x, y \in \mathbb{N}$, if $x = [x_n \ldots x_1 x_0]_p$ and $y = [y_n \ldots y_1 y_0]_p$ then*

$$\binom{x+y}{x} \equiv \prod_{i=0}^{n} \binom{x_i + y_i}{x_i} \pmod{p}.$$

For the remainder of this section, let p denote a prime number. For any $x = [x_n \ldots x_0]_p$ and $y = [y_n \ldots y_0]_p$, let $x \sqsubseteq_p y$ mean that $x_i \le y_i$ for every $i \le n$. The following two theorems specify the expressive power of $\langle \mathbb{N}; B_p \rangle$.

THEOREM 2.2 (Korec [Ko1]). *The relation $\sqsubseteq_p$ is definable in the structure $\langle \mathbb{N}; B_p \rangle$.*

If we consider any integer x as a finite multiset of powers of p, with $p-1$ as the maximal allowed multiplicity of a membership, then $\sqsubseteq_p$ can be understood as the multiset inclusion.

THEOREM 2.3 (Korec [Ko2]). *The following relations and functions are definable in the structure $\langle \mathbb{N}; B_p \rangle$:*

$$\begin{array}{rl}
x \sqsubset_p y & (\textit{proper multiset inclusion}),\\
x \prec_p y & (\textit{covering relation in } (\mathbb{N}, \sqsubseteq_p)),\\
z = x \sqcap_p y & (\textit{meet operation in } (\mathbb{N}, \sqsubseteq_p)),\\
z = x \sqcup_p y & (\textit{join operation in } (\mathbb{N}, \sqsubseteq_p)),\\
0, 1, \ldots, p-1 & (\textit{the constants } 0, 1, \ldots, p-1),\\
\mathrm{Pow}_p(x) & (x \textit{ is a power of } p),\\
\mathrm{OneDig}_p(x) & (x \textit{ has at most one nonzero digit}),\\
\mathrm{Dig}_p^i(w, x) & (\mathrm{Pow}_p(w) \textit{ and the corresponding digit of } x \textit{ is } i).
\end{array}$$

Since we shall work within extensions of $\langle \mathbb{N}; B_p \rangle$, we will freely use the above symbols in the sequel.

Let $\mathrm{NextPow}_p = \{(p^n, p^{n+1}) : n \in \mathbb{N}\}$. We shall use the following lemma in Sections 3 and 4.

LEMMA 2.4. *Addition is first-order definable in the structure $\langle \mathbb{N}; B_p, \mathrm{NextPow}_p \rangle$.*

Proof. The defining formula for $+$ will express the usual algorithm of addition in base p. The following (finite) set of quintuples of integers will be used as an abbreviation:

$$X = \{(i,j,k,m,n) : \\ i,j,m \in \{0,1,\dots,p-1\} \wedge k,n \in \{0,1\} \wedge i+j+k = m+np\}.$$

Now a defining formula for addition is

$$z = x+y \Leftrightarrow \\ \exists v\Big(\mathrm{Dig}_p^0(1,v) \wedge \forall w\Big(\mathrm{Pow}_p(w) \Rightarrow \bigvee_{(i,j,k,m,n)\in X} \Big(\mathrm{Dig}_p^i(w,x) \wedge \mathrm{Dig}_p^j(w,y) \\ \wedge \mathrm{Dig}_p^k(w,v) \wedge \mathrm{Dig}_p^m(w,z) \wedge \exists z(\mathrm{NextPow}_p(w,z) \wedge \mathrm{Dig}_p^n(z,v))\Big)\Big)\Big).$$

In this formula, v stands for the "vectors of carries", an integer whose digits are 0 or 1, each digit 1 corresponding to a carry. ∎

3. Definability within $\langle \mathbb{N}; B_n, \perp\rangle$. In [Ko3] the second author proved that for any $n \geq 2$ addition and multiplication are definable in the structure $\langle \mathbb{N}; B_n, |\rangle$, where $|$ denotes the division relation. The proof rests on a $\{B_p, |\}$-definition of $\mathrm{NextPow}_n$. In this section we improve this result by showing that the same holds for the structure $\langle \mathbb{N}; B_n, \perp\rangle$, where $x \perp y$ holds if and only if x and y have no common prime divisor (this relation is easily definable in $\langle \mathbb{N}; |\rangle$).

We shall prove that $+$ and $\times$ are definable in $\langle \mathbb{N}; B_n, \perp\rangle$. Since by [Wo] multiplication is definable in $\langle \mathbb{N}; +, \perp\rangle$, it is sufficient to define addition in $\langle \mathbb{N}; B_n, \perp\rangle$. Moreover, we only need to consider the case of n prime, since $+$ is definable in $\langle \mathbb{N}; B_n\rangle$ whenever $n \geq 2$ is not prime [Ko1], [Be].

The proof is based upon the following two theorems due to D. Richard [Ri], who used them as definability tools in the study of the structure $\langle \mathbb{N}; S, \perp\rangle$, where S denotes the successor function. For every $x \in \mathbb{N}$, denote by $\mathrm{Supp}(x)$ the *support* of x, that is, the set of its prime divisors.

THEOREM 3.1 (Richard). *For every integer $x \geq 2$ and all $\alpha, \beta \in \mathbb{N}$ the following holds*:

(i) *The equality* $\mathrm{Supp}(x^\alpha + 1) = \mathrm{Supp}(x^\beta + 1)$ *is equivalent to "$\alpha = \beta$ or ($x = 2$ and $\alpha, \beta \in \{1,3\}$)".*

(ii) *The equality* $\mathrm{Supp}(x^\alpha - 1) = \mathrm{Supp}(x^\beta - 1)$ *is equivalent to "$\alpha = \beta$ or ($x = 2^u - 1$ for some $u \geq 2$, and $\alpha, \beta \in \{1,2\}$)".*

THEOREM 3.2 (Richard). *For every integer $x \geq 2$ and all $\alpha, \beta \in \mathbb{N}$, the inclusion*

$$\mathrm{Supp}(x^\alpha - 1) \subseteq \mathrm{Supp}(x^\beta - 1)$$

is equivalent to "$\alpha \mid \beta$ or ($x = 2^u - 1$ for some $u \geq 2$, and $\alpha \in \{1,2\}$)".

We now intend to define $\mathrm{NextPow}_p$ in $\langle \mathbb{N}; B_p, \perp\rangle$. Let us first introduce some auxiliary relations and constants.

LEMMA 3.3. *The relations*

- $[\mathrm{Supp}(x) = \mathrm{Supp}(y)]$, *denoted by* $\mathrm{SameSupp}(x, y)$,
- $[\mathrm{Supp}(x) \subseteq \mathrm{Supp}(y)]$, *denoted by* $\mathrm{InclSupp}(x, y)$,
- $[\mathrm{Supp}(z) = \mathrm{Supp}(x) \cup \mathrm{Supp}(y)]$, *denoted by* $\mathrm{UnionSupp}(x, y, z)$,
- $[x$ *is a prime power*$]$, *denoted by* $\mathrm{PrimePow}(x)$,

are definable in the structure $\langle \mathbb{N}; B_p, \perp\rangle$.

Proof. The relevant definitions are:

$$\begin{aligned}
\mathrm{SameSupp}(x, y) &\Leftrightarrow \forall t(t \perp x \Leftrightarrow t \perp y),\\
\mathrm{InclSupp}(x, y) &\Leftrightarrow \forall t(t \perp y \Rightarrow t \perp x),\\
\mathrm{UnionSupp}(x, y, z) &\Leftrightarrow \forall t(t \perp z \Leftrightarrow (t \perp x \wedge t \perp y)),\\
\mathrm{PrimePow}(x) &\Leftrightarrow \forall y \forall z((\neg x \perp y \wedge \neg x \perp z) \Rightarrow \neg y \perp z). \ \blacksquare
\end{aligned}$$

LEMMA 3.4. *The constants* 2, 4 *and* 8 *are definable in the structure* $\langle \mathbb{N}; B_2, \perp\rangle$.

Proof. By Theorem 3.1(i), for all $\alpha, \beta \in \mathbb{N}$, $\alpha \neq \beta$, we have

$$\mathrm{Supp}(2^\alpha + 1) = \mathrm{Supp}(2^\beta + 1) \Leftrightarrow \begin{cases} \alpha = 1,\ \beta = 3 \text{ or}\\ \alpha = 3,\ \beta = 1.\end{cases}$$

Therefore we can define the set $T = \{3, 9\}$ by the formula

$$\begin{aligned}
T(x) \Leftrightarrow \exists y \exists z(\mathrm{Pow}_2(y) \wedge x = y \sqcup_2 1 \wedge \mathrm{Pow}_2(z) \wedge \neg y = z\\
\wedge\, \mathrm{SameSupp}(x, z \sqcup_2 1)).
\end{aligned}$$

Then we define the set $U = \{2, 8\}$ by the formula

$$U(x) \Leftrightarrow (\mathrm{Pow}_2(x) \wedge \exists y(T(y) \wedge y = x \sqcup_2 1)).$$

The set $V = \{4, 16\}$ can be defined by the formula

$$\begin{aligned}
V(x) \Leftrightarrow (&\mathrm{Pow}_2(x) \wedge \neg y = 1 \wedge \neg U(x)\\
&\wedge \exists y \exists z(U(y) \wedge U(z) \wedge \neg y = z \wedge \mathrm{Supp}(x \sqcup_2 y) = \mathrm{Supp}(x \sqcup_2 z))).
\end{aligned}$$

Then observe that 15 is the only positive integer which is not a prime power and can be written as the sum of 1 and three integers among $\{2, 4, 8, 16\}$. Thus the constant 15 can be defined by the formula

$$\begin{aligned}
x = 15 \Leftrightarrow \neg\, &\mathrm{PrimePow}(x) \wedge \exists y_1 \exists y_2 \exists y_3\\
&(U(y_1) \wedge V(y_2) \wedge (U(y_3) \vee V(y_3))\\
&\wedge \neg y_1 = y_3 \wedge \neg y_2 = y_3 \wedge x = 1 \sqcup_2 y_1 \sqcup_2 y_2 \sqcup_2 y_3).
\end{aligned}$$

This allows us to define the constants 4 and 16 by the formulas

$$x = 4 \Leftrightarrow V(x) \wedge x \sqcap_2 15 = x, \qquad x = 16 \Leftrightarrow V(x) \wedge \neg x = 4.$$

Finally, the integer $1+8+16$ is not coprime to 15, while $1+2+16$ is; thus we define the constants 2 and 8 by the formulas

$$x = 2 \Leftrightarrow U(x) \wedge (1 \sqcup_2 x \sqcup_2 16) \perp 15, \qquad x = 8 \Leftrightarrow U(x) \wedge \neg x = 2. \ \blacksquare$$

We shall use the following corollary of Chebyshev's Theorem:

PROPOSITION 3.5. *For every integer $n \geq 2$ there exists a prime p such that $n \leq p \leq \frac{7}{5}n$.*

Proof. It is proved in [El, p. 21] that there exists a constant $A > 0$ such that for every integer $n \geq 30$,

$$\frac{An}{\log n} \leq \pi(n) \leq \frac{6}{5} \cdot \frac{An}{\log n}.$$

Hence for every integer $n \geq 30$,

$$\begin{aligned}\pi\left(\frac{7}{5}n\right) - \pi(n) &\geq \frac{7}{5} \cdot \frac{An}{\log\left(\frac{7}{5}n\right)} - \frac{6}{5} \cdot \frac{An}{\log n}\\ &\geq \frac{An}{5(\log n)\left(\log n + \log\frac{7}{5}\right)}\left(7\log n - 6\left(\log n + \log\frac{7}{5}\right)\right).\end{aligned}$$

The last expression is strictly positive whenever $n > (7/5)^6$. Since $(7/5)^6 < 30$, this proves that for every $n \geq 30$ there exists a prime p such that $n \leq p \leq \frac{7}{5}n$. The cases $n = 2, \ldots, 29$ are easily checked. $\blacksquare$

LEMMA 3.6. *Let p be a prime greater than 2. The constant p is definable in the structure $\langle \mathbb{N}; B_p, \perp\rangle$.*

Proof. • *First case*: $p = 3$. In this case by Theorem 3.1(i) for every $n \in \mathbb{N}$ we have $\mathrm{Supp}(3^n + 1) = \{2\}$ if and only if $n = 1$. By Theorem 2.3 the constants 1 and 2 are definable in $\langle \mathbb{N}; B_3, \perp\rangle$, and the constant 3 is thus definable in $\langle \mathbb{N}; B_3, \perp\rangle$ by the formula

$$x = 3 \Leftrightarrow (\mathrm{Pow}_3(x) \wedge \mathrm{SameSupp}(x \sqcup_3 1, 2)).$$

• *Second case*: $p > 3$. If we set $n = (p+1)/2$, then the previous proposition ensures us that there exists a prime q such that

$$\frac{p+1}{2} \leq q \leq \frac{7}{5} \cdot \frac{p+1}{2}$$

and $\frac{7}{5}(p+1)/2 < p$ whenever $p \geq 3$. Thus there exists a prime q such that

$$\frac{p+1}{2} \leq q < p.$$

Fix such a q; by Theorem 2.3 the constant $q-1$ is definable in $\langle \mathbb{N}; B_p, \perp\rangle$. Now the set $\mathrm{PredPow}_q = \{(q^n, q^n - 1) : n \geq 1\}$ can be defined by

$$\mathrm{PredPow}_q(x,y) \Leftrightarrow \Big(\mathrm{SameSupp}(x,q) \\ \wedge \bigwedge_{i=1}^{p-1} (x \sqcap_p (p-1) = i \Rightarrow (y \sqcap_p (p-1) = i-1 \wedge x = y \sqcup_p i))\Big).$$

We intend to define the constant q^2, which has only two non-zero digits, namely the 0th and the first; this property will allow us to define p.

First assume that $q = 2^u - 1$ for some positive integer u. By Theorem 3.1(ii), if $\mathrm{Supp}(q^n - 1) = \mathrm{Supp}(q-1)$ with $n \neq 1$ then $n = 2$. Therefore $q^2 - 1$ is definable in $\langle \mathbb{N}; B_p, \perp\rangle$:

$$x = q^2 - 1 \Leftrightarrow \exists t(\mathrm{PredPow}_q(t,x) \wedge \neg x = q-1 \wedge \mathrm{SameSupp}(x, q-1)).$$

From this we get a definition for q^2 by the formula

$$x = q^2 \Leftrightarrow \bigvee_{i=1}^{p-2} ((q^2-1) \sqcap_p (p-1) = i \wedge x = (q^2-1) \sqcup_p (i+1)).$$

Assume now that $q \neq 2^u - 1$ for every $u \geq 1$. In this case, by Theorem 3.1(ii), for all integers α, β we have

$$\mathrm{Supp}(q^\alpha - 1) = \mathrm{Supp}(q^\beta - 1) \quad \text{if and only if} \quad \alpha = \beta,$$

thus q^2 is the only power of q, say q^n, such that

$$\mathrm{Supp}(q^n - 1) = \mathrm{Supp}(q-1) \cup \mathrm{Supp}(q+1).$$

We have $q < p - 1$, thus by Theorem 2.3 the constant $q + 1$ is definable in $\langle \mathbb{N}; B_p, \perp\rangle$. This leads to the following definition for q^2:

$$x = q^2 \Leftrightarrow \exists y(\mathrm{PredPow}_q(x,y) \wedge \mathrm{UnionSupp}(q-1, q+1, y)).$$

The inequalities

$$\frac{p+1}{2} \leq q < p$$

yield $p < q^2 < p^2$; finally, we can define p by observing that p is the only proper power of p, say p^n, such that $p^n \sqcap_p q^2 \neq 0$:

$$x = p \Leftrightarrow (x \neq 1 \wedge \mathrm{Pow}_p(x) \wedge x \sqcap_p q^2 \neq 0). \ \blacksquare$$

LEMMA 3.7. *For every prime p the relation* $\mathrm{NextPow}_p$ *is definable in the structure* $\langle \mathbb{N}; B_p, \perp\rangle$.

Proof. • *First case*: $p = 2$. Let α, β be two integers greater than or equal to 3. If

$$\mathrm{Supp}(2^\alpha + 2) = \mathrm{Supp}(2^\beta + 1) \cup \{2\}$$

then

$$\mathrm{Supp}(2^{\alpha-1} + 1) = \mathrm{Supp}(2^\beta + 1),$$

which implies, by Theorem 3.1(i), $\alpha - 1 = \beta$. Conversely, if $\alpha - 1 = \beta$ then obviously

$$\mathrm{Supp}(2^\alpha + 2) = \mathrm{Supp}(2^\beta + 1) \cup \{2\}.$$

Therefore a suitable formula for $\mathrm{NextPow}_2(x, y)$ is

$$\begin{aligned}
&\mathrm{NextPow}_2(x, y) \Leftrightarrow \\
&\qquad ((x = 1 \wedge y = 2) \vee (x = 2 \wedge y = 4) \vee (x = 4 \wedge y = 8) \\
&\qquad \vee (\mathrm{Pow}_2(x) \wedge \mathrm{Pow}_2(y) \wedge \neg x = 1 \wedge \neg x = 2 \wedge \neg x = 4 \\
&\qquad \wedge \neg y = 1 \wedge \neg y = 2 \wedge \neg y = 4 \wedge \mathrm{UnionSupp}(x \sqcup_2 1, 2, y \sqcup_2 2))).
\end{aligned}$$

• *Second case*: $p \neq 2$. In this case by Theorem 3.1(i) for all $\alpha, \beta \in \mathbb{N}$ we have

$$\mathrm{Supp}(p^\alpha + p) = \mathrm{Supp}(p^\beta + 1) \cup \{p\} \quad \text{if and only if} \quad \alpha - 1 = \beta.$$

Therefore an appropriate formula for $\mathrm{NextPow}_p(x, y)$ is

$$\mathrm{NextPow}_p(x, y) \Leftrightarrow (\mathrm{Pow}_p(x) \wedge \mathrm{Pow}_p(y) \wedge \mathrm{UnionSupp}(x \sqcup_p 1, p, y \sqcup_p p)). \ \blacksquare$$

THEOREM 3.8. *For every integer $n \geq 2$ the structures $\langle \mathbb{N}; B_n, \perp \rangle$ and $\langle \mathbb{N}; +, \times \rangle$ are inter-definable.*

Proof. By Lemmas 3.7 and 2.4 for every prime p addition is definable in the structure $\langle \mathbb{N}; B_p, \perp \rangle$. Furthermore, by [Ko1], [Be], addition is definable in $\langle \mathbb{N}; B_n \rangle$ whenever $n \geq 2$ is not prime; thus for every integer $n \geq 2$ addition is definable in $\langle \mathbb{N}; B_n, \perp \rangle$. Now by [Wo] multiplication is definable in the structure $\langle \mathbb{N}; +, \perp \rangle$. ∎

COROLLARY 3.9. *For every integer $n \geq 2$ the elementary theory of $\langle \mathbb{N}; B_n, \perp \rangle$ is undecidable.*

4. Definability within $\langle \mathbb{N}; B_n, \mathrm{Sq} \rangle$. Let Sq denote the set of squares. In [Ko2] it was proved that $+$ and $\times$ are definable in the structure $\langle \mathbb{N}; B_2, \mathrm{Sq} \rangle$. We here extend this result to $\langle \mathbb{N}; B_n, \mathrm{Sq} \rangle$ for every integer $n \geq 3$. A first observation is that we only have to define addition, since by [Pu], $\times$ is definable in $\langle \mathbb{N}; +, \mathrm{Sq} \rangle$. Moreover, as noted before, addition is definable in $\langle \mathbb{N}; B_n \rangle$ whenever $n \geq 2$ is not prime ([Ko1], [Be]), thus it is sufficient to prove the result for n prime and greater than or equal to 3.

The following two lemmas specify, for squares with a small number of nonzero digits, their respective position.

LEMMA 4.1. *Let p be an odd prime. For all $k, t \in \mathbb{N}$, if $k \neq 2t$ then*

$$(p - 2)p^k + p^{2t} \text{ is a square if and only if } k = 2t + 1.$$

Proof. The "if" part is obvious. For the converse suppose that

$$(p - 2)p^k + p^{2t} = x^2 \tag{1}$$

for some $x \in \mathbb{N}$. Let us first show that $k > 2t$. Otherwise $k < 2t$, and (1) implies

$$p^k[(p-2) + p^{2t-k}] = x^2. \tag{2}$$

Since $p - 2 + p^{2t-k}$ is prime to p, k is even; thus there exist two positive integers j, y such that

$$p - 2 + p^{2j} = y^2. \tag{3}$$

Now p^{2j} and $p^{2j} + 2p^j + 1$ are consecutive squares, and the fact that

$$p^{2j} < p - 2 + p^{2j} < p^{2j} + 2p^j + 1 \tag{4}$$

leads to a contradiction. So $k > 2t$, that is, $k \geq 2t + 1$. It follows that

$$p^{2t}[(p-2)p^{k-2t} + 1] = x^2. \tag{5}$$

Therefore $(p-2)p^{k-2t} + 1$ is a square. Thus we have to show that for all positive integers l, z the equation

$$(p-2)p^l + 1 = z^2 \tag{6}$$

yields $l = 1$. Equation (6) implies $(p-2)p^l \mid z^2 - 1$. Since $p \geq 3$, we have $p^l \mid z - 1$ or $p^l \mid z + 1$. In both cases we have $z \geq p^l - 1$, which implies

$$z^2 \geq p^{2l} - 2p^l + 1. \tag{7}$$

Now $p \geq 3$, so $p^l - 2 - p^{l-1} \geq 0$, which yields $p^{2l} - 2p^l + 1 > p^{2l-1}$. Therefore (6) and (7) lead to $(p-2)p^l + 1 > p^{2l-1}$. This implies $l \geq 2l - 1$, that is, $l \leq 1$ and finally $l = 1$. ∎

LEMMA 4.2. *Let p be an odd prime. For all $j, k \in \mathbb{N}$ such that $j \neq k$, we have the following*:

(i) *if $p = 3$ then ($p^{2j} + p^{2k} + 2p^{2k+1}$ is a square if and only if $j = k+1$ or $j = k - 1$);*

(ii) *if $p > 3$ then ($p^{2j} + p^{2k} + 2p^{2k+1}$ is a square if and only if $j = k+1$).*

Proof. The "if" part is easily checked in both cases. Conversely, assume first that $j < k$. In this case

$$1 + p^{2(k-j)} + 2p^{2(k-j)+1} = y^2 \tag{8}$$

for some positive integer y. Set $l = k - j$. We get

$$1 + p^{2l} + 2p^{2l+1} = y^2. \tag{9}$$

Thus

$$p^{2l}(1 + 2p) = (y-1)(y+1), \tag{10}$$

which yields $p^{2l} \mid y - 1$ or $p^{2l} \mid y + 1$. In both cases $y \geq p^{2l} - 1$, so that $y^2 \geq p^{4l} - 2p^{2l} + 1$. Then from (9) we obtain

$$1 + p^{2l} + 2p^{2l+1} \geq p^{4l} - 2p^{2l} + 1, \tag{11}$$

which implies $1 + 2p \geq p^{2l} - 2$. If $p = 3$ then the previous inequality forces $l = 1$, i.e. $j = k - 1$. If $p > 3$ then $p^{2l} - 2 \geq 5p - 2 > 1 + 2p$, which leads to a contradiction.

Assume now that $j > k$. Set $l = j - k$. In this case

$$1 + p^{2l} + 2p = z^2 \tag{12}$$

for some positive integer z. Now for every $m \in \mathbb{N}$, p^{2m} and $p^{2m} + 2p^m + 1$ are consecutive squares, therefore the only case for which $1 + p^{2l} + 2p$ is a square is $l = 1$, that is, $j = k + 1$. ∎

As in the previous section, we now define $\mathrm{NextPow}_p$ in order to define addition.

Lemma 4.3. *For every prime $p \geq 3$ the relation $\mathrm{NextPow}_p$ is definable in the structure $\langle \mathbb{N}; B_p, \mathrm{Sq}\rangle$.*

Proof. Let $\mathrm{EvenPow}_p$ (respectively OddPow_p) be the set of even (resp. odd) powers of p. These sets are definable by the following formulas:

$$\mathrm{EvenPow}_p(x) \Leftrightarrow (\mathrm{Pow}_p(x) \wedge \mathrm{Sq}(x)),$$
$$\mathrm{OddPow}_p(x) \Leftrightarrow (\mathrm{Pow}_p(x) \wedge \neg\mathrm{Sq}(x)).$$

Let us now define the set $E = \{(p-2)p^k + p^{2t} : k, t \in \mathbb{N} \text{ and } k \neq 2t\}$. A suitable defining formula is

$$E(x) \Leftrightarrow \exists z_1 \exists z_2 (\mathrm{EvenPow}_p(z_1) \wedge \mathrm{OneDig}_p(z_2) \\ \wedge \exists w\, \mathrm{Dig}_p^{p-2}(w, z_2) \wedge x = z_1 \sqcup_p z_2).$$

Now using Lemma 4.1 we can define the set $D_1 = \{(p^{2n}, p^{2n+1}) : n \in \mathbb{N}\}$ by the formula

$$D_1(x,y) \Leftrightarrow \mathrm{EvenPow}_p(x) \wedge \mathrm{OddPow}_p(y) \wedge \exists z (E(z) \wedge \mathrm{Sq}(z) \wedge x \sqsubseteq_p z \wedge y \sqsubseteq_p z).$$

Consider the set $F = \{p^{2j} + p^{2k} + 2p^{2k+1} : j, k \in \mathbb{N} \text{ and } j \neq k\}$. It is definable as follows:

$$F(x) \Leftrightarrow \exists y_1 \exists y_2 \exists y_3 \exists z (\mathrm{EvenPow}_p(y_1) \wedge \mathrm{EvenPow}_p(y_2) \wedge \neg y_1 = y_2 \wedge D_1(y_2, y_3) \\ \wedge \mathrm{OneDig}_p(z) \wedge \exists w\ \mathrm{Dig}_p^2(w,z) \wedge y_3 \sqsubseteq_p z \wedge x = y_1 \sqcup_p y_2 \sqcup_p z).$$

• *First case*: $p > 3$. Let $z \in F$, that is, $z = p^{2j} + p^{2k} + 2p^{2k+1}$ for some $j, k \in \mathbb{N}$, $j \neq k$. By Lemma 4.2(ii), z is a square if and only if $j = k + 1$. This allows us to define $D_2 = \{(p^{2n+1}, p^{2n+2}) : n \in \mathbb{N}\}$ in the following way:

$$D_2(x,y) \Leftrightarrow \mathrm{OddPow}_p(x) \wedge \mathrm{EvenPow}_p(y) \\ \wedge \exists z (F(z) \wedge \mathrm{Sq}(z) \wedge y \sqsubseteq_p z \wedge x \sqsubseteq_p z \wedge \neg D_1(y,x)).$$

This leads to the following definition for $\mathrm{NextPow}_p$:

$$\mathrm{NextPow}_p(x,y) \Leftrightarrow D_1(x,y) \vee D_2(x,y).$$

• *Second case*: $p=3$. Let $z \in F$, say $z = 3^{2j} + 3^{2k} + 2\cdot 3^{2k+1}$ for some $j,k \in \mathbb{N}$, $j \neq k$. By Lemma 4.2(i), z is a square if and only if $j = k+1$ or $j = k-1$. Thus we can define the set $G = \{(3^{2m}, 3^{2n}) : |m-n| = 1\}$ by the formula

$$\begin{aligned} G(x,y) \Leftrightarrow\ & \mathrm{EvenPow}_3(x) \wedge \mathrm{EvenPow}_3(y) \\ & \wedge \neg x = y \wedge \exists z(F(z) \wedge \mathrm{Sq}(z) \wedge x \sqsubseteq_3 z \wedge y \sqsubseteq_3 z). \end{aligned}$$

Now consider

$$\mathrm{SeqEvenPow}_3 = \Big\{(x,t) : x = \sum_{i=0}^{n} 3^{2i} \text{ and } t = 3^{2n} \text{ for some } n \in \mathbb{N}\Big\};$$

this set, using G, is definable as follows:

$$\begin{aligned} &\mathrm{SeqEvenPow}_3(x,t) \Leftrightarrow \\ &\quad (\forall z((\mathrm{Pow}_3(z) \wedge z \sqsubseteq_3 x) \Rightarrow (\mathrm{EvenPow}_3(z) \wedge \mathrm{Dig}_3^1(z,x))) \\ &\quad \wedge 1 \sqsubseteq_3 x \wedge \mathrm{EvenPow}_3(t) \wedge t \sqsubseteq_3 x \wedge \exists u(G(t,u) \wedge \neg u \sqsubseteq_3 x) \\ &\quad \wedge \forall v \forall w((\mathrm{EvenPow}_3(v) \wedge v \sqsubseteq_3 x \wedge \neg v = t \wedge G(v,w)) \Rightarrow w \sqsubseteq_3 x)). \end{aligned}$$

Thanks to this set we can define

$$\mathrm{NextEvenPow}_3 = \{(3^{2n}, 3^{2n+2}) : n \in \mathbb{N}\}$$

by the formula

$$\begin{aligned} \mathrm{NextEvenPow}_3(x,y) \Leftrightarrow\ & \exists u \exists v(\mathrm{SeqEvenPow}_3(u,x) \\ & \wedge \mathrm{SeqEvenPow}_3(v,y) \wedge v = u \sqcup_3 y). \end{aligned}$$

We finally define $\mathrm{NextPow}_3$ in the following way:

$$\mathrm{NextPow}_3(x,y) \Leftrightarrow D_1(x,y) \vee \exists z(D_1(z,x) \wedge \mathrm{NextEvenPow}_3(z,y)). \ ■$$

THEOREM 4.4. *For every integer $n \geq 2$ the structures $\langle \mathbb{N}; B_n, \mathrm{Sq}\rangle$ and $\langle \mathbb{N}; +, \times\rangle$ are inter-definable.*

Proof. From Lemma 4.3 and Theorem 2.4 it follows that for every prime p addition is definable in the structure $\langle \mathbb{N}; B_p, \mathrm{Sq}\rangle$. Since by [Ko1], [Be], addition is definable in $\langle \mathbb{N}; B_n\rangle$ whenever $n \geq 2$ is not prime, this proves that for every integer $n \geq 2$ addition is definable in the structure $\langle \mathbb{N}; B_n, \mathrm{Sq}\rangle$. Then by [Pu] multiplication is definable in the structure $\langle \mathbb{N}; +, \mathrm{Sq}\rangle$. ■

COROLLARY 4.5. *For every integer $n \geq 2$ the elementary theory of $\langle \mathbb{N}; B_n, \mathrm{Sq}\rangle$ is undecidable.*

5. Definability within $\langle \mathbb{N}; B_n, \mathrm{SQ}_n\rangle$. In the last section we proved that adding the set of squares to the language $\{B_n\}$ suffices to define addition and multiplication, and therefore leads to the undecidability of the corresponding theory. We now study the situation obtained by adding a fragment of the squaring function to $\{B_n\}$.

For every integer $n \geq 2$, let SQ_n denote the restriction of the squaring function to powers of n. In [Ko2] the following two results were proved:

(i) Multiplication is definable in the structure $\langle \mathbb{N}; B_2, +, \mathrm{SQ}_2 \rangle$. Thus the elementary theory of this structure is undecidable.

(ii) Neither $+$ nor $\times$ are definable in the structure $\langle \mathbb{N}; B_2, \mathrm{SQ}_2 \rangle$.

We prove below that (i) holds if 2 is replaced by any integer greater than 1. Since addition is definable in $\langle \mathbb{N}; B_n \rangle$ whenever $n \geq 2$ is not prime, this will imply that for every nonprime integer $n \geq 2$ the elementary theory of $\langle \mathbb{N}; B_n, \mathrm{SQ}_n \rangle$ is undecidable. On the other hand, we show, using Feferman–Vaught results on generalized powers, that for every prime p the elementary theory of $\langle \mathbb{N}; B_p, \mathrm{SQ}_p \rangle$ is decidable.

Let us first consider the structure $\langle \mathbb{N}; B_n, +, \mathrm{SQ}_n \rangle$ for $n \geq 2$. We shall make use of the following theorem due to Villemaire [Vi], which is a first-order version of results of Thomas [Th]. For every integer $n \geq 2$, let us denote by V_n the function which maps every positive integer x to the greatest power of n dividing x.

THEOREM 5.1 (Villemaire). *Let $n \geq 2$, and let f be a function from* Pow_n *to* Pow_n *which has the following properties*:

(1) *For every $i \in \mathbb{N}$, $f(n^{i+1}) \geq n f(n^i)$ (f is strictly increasing)*;

(2) *There exists $d \in \mathbb{N}$ such that for every $i \in \mathbb{N}$ there exists an integer m such that $i \leq m \leq i + d$ and*

$$f(n^{m+1}) \geq n^2 f(n^m).$$

Then multiplication is definable in the structure $\langle \mathbb{N}; +, V_n, f \rangle$.

THEOREM 5.2. *For every integer $n \geq 2$ multiplication is definable in* $\langle \mathbb{N}; B_n, +, \mathrm{SQ}_n \rangle$.

Proof. Since for every $i \in \mathbb{N}$, $\mathrm{SQ}_n(n^{i+1}) = n^2 \mathrm{SQ}_n(n^i)$, it follows that the function SQ_n satisfies conditions (1) and (2) of the previous theorem. Thus it remains to prove that V_n is definable in $\langle \mathbb{N}; B_n, +, \mathrm{SQ}_n \rangle$. A suitable definition is

$$\begin{aligned} y = V_n(x) \Leftrightarrow (\neg x = 0 \wedge \mathrm{Pow}_n(y) \wedge \neg\, \mathrm{Dig}_n^0(y, x) \\ \wedge \forall z((z < y \wedge \mathrm{Pow}_n(z)) \Rightarrow \mathrm{Dig}_n^0(z, x))). \end{aligned}$$

COROLLARY 5.3. *For every nonprime integer $n \geq 2$ the elementary theory of $\langle \mathbb{N}; B_n, \mathrm{SQ}_n \rangle$ is undecidable.*

Proof. This follows from Theorem 5.2 and the fact that addition is definable in $\langle \mathbb{N}; B_n \rangle$ whenever $n \geq 2$ is not prime ([Ko1], [Be]). ∎

We now study the expressive power of $\langle \mathbb{N}; B_p, \mathrm{SQ}_p \rangle$ for p prime. The following theorem specifies the result (ii) of the beginning of the section.

THEOREM 5.4. *For every prime p, neither $+$ nor $\times$ are definable in $\langle \mathbb{N}; B_p, \mathrm{SQ}_p \rangle$.*

Proof. The argument is almost the same as in [Ko2]. Let φ be the permutation of Pow_p defined by

$$\begin{cases} \varphi(p^{2^i}) = p^{3\cdot 2^i} & \text{for every } i \in \mathbb{N}, \\ \varphi(p^{3\cdot 2^i}) = p^{2^i} & \text{for every } i \in \mathbb{N}, \\ \varphi(p^i) = p^i & \text{for every } i \notin \{3\cdot 2^j : j \in \mathbb{N}\} \cup \{2^j : j \in \mathbb{N}\}. \end{cases}$$

Now let $\overline{\varphi}$ be the function defined by

$$\overline{\varphi}\Big(\sum_{i=0}^{k} a_i p^i\Big) = \sum_{i=0}^{k} a_i \varphi(p^i) \text{ for all } n \in \mathbb{N} \text{ and } a_i \in \{0,1,\ldots,p-1\},\ 0 \le i \le k.$$

It follows from Lucas' Theorem that for all $x, y \in \mathbb{N}$,

$$B_p(x,y) = B_p(\overline{\varphi}(x), \overline{\varphi}(y)).$$

Moreover, $\overline{\varphi}(z) = z$ for every $z \in \{0,1,\ldots,p-1\}$. Hence $\overline{\varphi}$ preserves B_p. It is easily checked that $\overline{\varphi}$ preserves SQ_p too. Therefore $\overline{\varphi}$ is an automorphism of the structure $\langle \mathbb{N}; B_p, \mathrm{SQ}_p \rangle$. Now

$$\overline{\varphi}(p-1) + \overline{\varphi}(1) = p - 1 + 1 = p \ne p^3 = \overline{\varphi}(p-1+1)$$

and

$$\overline{\varphi}(p^2) \cdot \overline{\varphi}(p) = p^6 \cdot p^3 = p^9 \ne p = \overline{\varphi}(p^2 \cdot p).$$

Thus $\overline{\varphi}$ preserves neither $+$ nor $\times$. ■

In the sequel p will denote a prime number. We now proceed to show that the elementary theory of $\langle \mathbb{N}; B_p, \mathrm{SQ}_p \rangle$ is decidable.

For technical reasons we shall consider, instead of $\langle \mathbb{N}; B_p, \mathrm{SQ}_p \rangle$, the structure $\langle \mathbb{N}; B'_p, \mathrm{SQ}'_p \rangle$, where:

- B'_p is the graph of B_p.
- $\mathrm{SQ}'_p = \{(p^i, p^{2i}) : i \ge 1\} \cup \{(1,p)\}$.

B_p is obviously definable in $\langle \mathbb{N}; B'_p, \mathrm{SQ}'_p \rangle$; moreover, SQ_p is definable in $\langle \mathbb{N}; B'_p, \mathrm{SQ}'_p \rangle$ by the formula

$$y = \mathrm{SQ}_p(x) \Leftrightarrow ((x = 1 \wedge y = 1) \vee (\neg x = 1 \wedge \mathrm{SQ}'_p(x,y))).$$

Thus if we show that the elementary theory of $\langle \mathbb{N}; B'_p, \mathrm{SQ}'_p \rangle$ is decidable, then so will be the elementary theory of $\langle \mathbb{N}; B_p, \mathrm{SQ}_p \rangle$.

We shall use the notion of generalized power, which was introduced by Feferman and Vaught [FV].

For every set B, denote by $\mathcal{P}_{\mathrm{f}}(B)$ the set of finite subsets of B. If A is a (nonempty) set, e is an element of A, and B is a set, we denote by $A_e^{(B)}$ the set of functions f from B to A such that $\{b : b \in B \wedge f(b) \ne e\}$ is finite.

Definition 5.5. Let A, B be nonempty sets, e be an element of A, $\mathcal{L}_A$, $\mathcal{L}_B$ be first-order languages, and $\mathcal{A} = \langle A; \mathcal{R}_A \rangle$, $\mathcal{B} = \langle \mathcal{P}_{\mathrm{f}}(B); \mathcal{R}_B \rangle$ be an $\mathcal{L}_A$-structure and $\mathcal{L}_B$-structure, respectively. Let R be a relation with arity k over $A_e^{(B)}$. We say that R is *accessible* in $(\mathcal{A}, \mathcal{B})$ if and only if there exist an $\mathcal{L}_B$-formula $G(X_1, \ldots, X_l)$ and l $\mathcal{L}_A$-formulas with k free variables $F_1, \ldots, F_l$ such that:

(i) $\mathcal{A} \not\models F_i(e, e, \ldots, e)$ for every $i \in \{1, \ldots, l\}$.

(ii) For every k-tuple $(f_1, \ldots, f_k)$ of $A_e^{(B)}$, $R(f_1, \ldots, f_k)$ holds if and only if

$$\mathcal{B} \models G(T_1, \ldots, T_l)$$

where

$$T_i = \{x \in B : \mathcal{A} \models F_i(f_1(x), \ldots, f_k(x))\} \text{ for every } i \in \{1, \ldots, l\}.$$

(The condition (i) ensures that $T_1, \ldots, T_l$ are finite sets.)

Definition 5.6. With the above notations, if $\mathcal{R}$ is a set of relations over $A_e^{(B)}$, we say that the structure $\langle A_e^{(B)}; \mathcal{R} \rangle$ is a *generalized power* of $\mathcal{A}$ relative to $\mathcal{B}$ if every relation of $\mathcal{R}$ is accessible in $(\mathcal{A}, \mathcal{B})$.

Theorem 5.7 (Feferman–Vaught [FV]). *With the above notations, if the elementary theories of $\mathcal{A}$ and $\mathcal{B}$ are decidable and $\mathcal{C}$ is a generalized power of $\mathcal{A}$ relative to $\mathcal{B}$ then the elementary theory of $\mathcal{C}$ is decidable.*

Let us denote by $\ll$ the binary relation over $\mathcal{P}_{\mathrm{f}}(\mathbb{N})$ defined by: $X \ll Y$ if and only if X, Y are nonempty sets and $\mathrm{Sup}(X) < \mathrm{Sup}(Y)$. We shall prove that the structure $\langle \mathbb{N}; B_p', \mathrm{SQ}_p' \rangle$ is isomorphic to a generalized power of $\langle \mathbb{N}; B_p, + \rangle$ relative to $\langle \mathcal{P}_{\mathrm{f}}(\mathbb{N}); \subseteq, \ll \rangle$.

For every $x \in \mathbb{N}$, let $f_x : \mathbb{N} \to \mathbb{N}$ be the function defined as follows: assume that

$$x = \sum_{i=0}^{k} a_i p^i, \qquad \text{where } a_i \in \{0, 1, \ldots, p-1\},\ 0 \le i \le k;$$

then

$$f_x(0) = a_0 p^0 + \sum_{i=0}^{\lfloor \log_2(k) \rfloor} a_{2^i} p^{i+1}$$

and for every positive integer n,

$$f_x(n) = \sum_{i=0}^{\lfloor \log_2(k/(2n+1)) \rfloor} a_{(2n+1)2^i} p^i$$

where $\lfloor r \rfloor$ denotes the integer part of r. It is easily checked that the function $\varphi : \mathbb{N} \to \mathbb{N}_0^{(\mathbb{N})}$ which maps every $x \in \mathbb{N}$ to f_x is 1-1 and onto.

Consider the structure $\langle \mathbb{N}_0^{(\mathbb{N})}; \widetilde{B}_p', \widetilde{\mathrm{SQ}}_p' \rangle$, where

$$\mathbb{N}_0^{(\mathbb{N})} \models \widetilde{B}_p'(x, y, z) \quad \text{if and only if} \quad \mathbb{N} \models B_p'(\varphi^{-1}(x), \varphi^{-1}(y), \varphi^{-1}(z))$$

and

$$\mathbb{N}_0^{(\mathbb{N})} \models \widetilde{\mathrm{SQ}}'_p(x,y) \quad \text{if and only if} \quad \mathbb{N} \models \mathrm{SQ}'_p(\varphi^{-1}(x), \varphi^{-1}(y))$$

for all $x, y, z \in \mathbb{N}_0^{(\mathbb{N})}$. This structure is clearly isomorphic to $\langle \mathbb{N}; B'_p, \mathrm{SQ}'_p \rangle$.

We intend to prove that $\langle \mathbb{N}_0^{(\mathbb{N})}; \widetilde{B}'_p, \widetilde{\mathrm{SQ}}'_p \rangle$ is a generalized power of $\langle \mathbb{N}; B_p, + \rangle$ relative to $\langle \mathcal{P}_{\mathrm{f}}(\mathbb{N}); \subseteq, \ll \rangle$. For this we have to show that the relations $\widetilde{\mathrm{SQ}}'_p$ and $\widetilde{B}'_p$ are accessible in $(\langle \mathbb{N}; B_p, + \rangle, \langle \mathcal{P}_{\mathrm{f}}(\mathbb{N}); \subseteq, \ll \rangle)$.

We first introduce several relations and functions over $\mathcal{P}_{\mathrm{f}}(\mathbb{N})$.

LEMMA 5.8. *The following relations and functions over* $\mathcal{P}_{\mathrm{f}}(\mathbb{N})$ *are definable in the structure* $\langle \mathcal{P}_{\mathrm{f}}(\mathbb{N}); \subseteq, \ll \rangle$:

- $[X$ *is empty*$]$, *denoted by* $\mathrm{Empty}(X)$;
- $[X$ *is a singleton*$]$, *denoted by* $\mathrm{Singl}(X)$;
- *the singleton* $\{0\}$, *denoted by* Zero;
- *the function denoted by* $Y = \mathrm{Succ}(X)$, *which maps every singleton* $X = \{n\}$ *to* $Y = \{n+1\}$ $(n \in \mathbb{N})$;
- *the function denoted by* $Y = \mathrm{Sup}(X)$, *which maps every nonempty set* X *with maximal element* n *to the singleton* $Y = \{n\}$.

Proof. The corresponding definitions are:

$$\begin{aligned}
\mathrm{Empty}(X) &\Leftrightarrow (\forall Y (X \subseteq Y));\\
\mathrm{Singl}(X) &\Leftrightarrow (\neg\, \mathrm{Empty}(X) \wedge \forall Y (Y \subseteq X \Rightarrow (\mathrm{Empty}(Y) \vee X = Y)));\\
X = \mathrm{Zero} &\Leftrightarrow (\mathrm{Singl}(X) \wedge \forall Y (\neg Y \ll X));\\
Y = \mathrm{Succ}(X) &\Leftrightarrow (\mathrm{Singl}(X) \wedge \mathrm{Singl}(Y) \wedge X \ll Y \wedge \neg \exists Z (X \ll Z \wedge Z \ll Y));\\
Y = \mathrm{Sup}(X) &\Leftrightarrow (\neg\, \mathrm{Empty}(X) \wedge \mathrm{Singl}(Y) \wedge \forall Z (X \ll Z \Leftrightarrow Y \ll Z)). \ \blacksquare
\end{aligned}$$

LEMMA 5.9. *The relation* $\widetilde{\mathrm{SQ}}'_p$ *is accessible in* $(\langle \mathbb{N}; B_p, + \rangle, \langle \mathcal{P}_{\mathrm{f}}(\mathbb{N}); \subseteq, \ll \rangle)$.

Proof. Let x, y be two integers with respective p-ary expansions $x = [x_k \ldots x_1 x_0]_p$ and $y = [y_k \ldots y_1 y_0]_p$. Then $\widetilde{\mathrm{SQ}}'_p(f_x, f_y)$ holds if and only if both x and y have a single nonzero digit, say x_i and y_j, each being equal to 1, and either $i = 0$ and $j = 1$, or $i > 0$ and $j = 2i$. These conditions can be expressed in the following (equivalent) way: there exists $n \in \mathbb{N}$ such that $f_x(n) = p^l$, $f_y(n) = p^{l+1}$ for some $l \in \mathbb{N}$, and $f_x(n') = f_y(n') = 0$ whenever $n' \neq n$. This yields the following description of $\widetilde{\mathrm{SQ}}'_p$:

Consider

$$F_1(u,v): \quad \neg(u = 0 \vee v = 0)$$

and

$$F_2(u,v): \quad \mathrm{NextPow}_p(u,v).$$

F_1 and F_2 can be seen as $\{B_p,+\}$-formulas (since $\mathrm{NextPow}_p$ is easily definable in $\langle\mathbb{N};B_p,+\rangle$). Then consider

$$G(T_1,T_2):\quad \mathrm{Singl}(T_1)\wedge T_1\subseteq T_2.$$

$G(T_1,T_2)$ can be seen as a $\{\subseteq,\ll\}$-formula (by Lemma 5.8). From the above remark it is clear that $\widetilde{\mathrm{SQ}}'_p(f_x,f_y)$ holds if and only if $G(T_1,T_2)$ does, with

$$T_i=\{n\in\mathbb{N}:\langle\mathbb{N};B_p,+\rangle\models F_i(f_x(n),f_y(n))\}\quad\text{ for every } i\in\{1,2\}. \ \blacksquare$$

LEMMA 5.10. *The relation $\widetilde{B}'_p$ is accessible in $(\langle\mathbb{N};B_p,+\rangle,\langle\mathcal{P}_{\mathrm{f}}(\mathbb{N});\subseteq,\ll\rangle)$.*

Proof. Let x,y be two integers with respective p-ary expansions $x=[x_k\ldots x_1x_0]_p$ and $y=[y_k\ldots y_1y_0]_p$. By Lucas' Theorem,

$$\begin{aligned}
B_p(x,y)&=\prod_{i=0}^{k}\binom{x_i+y_i}{x_i}\ \mathrm{MOD}\ p\\
&=\binom{x_0+y_0}{x_0}\prod_{i=0}^{\lfloor\log_2(k)\rfloor}\binom{x_{2^i}+y_{2^i}}{x_{2^i}}\\
&\quad\times\prod_{j=1}^{\lfloor(k-1)/2\rfloor}\ \prod_{i=0}^{\lfloor\log_2(k/(2j+1))\rfloor}\binom{x_{(2j+1)2^i}+y_{(2j+1)2^i}}{x_{(2j+1)2^i}}\ \mathrm{MOD}\ p\\
&=B_p(f_x(0),f_y(0))\prod_{j=1}^{\lfloor(k-1)/2\rfloor}B_p(f_x(j),f_y(j))\ \mathrm{MOD}\ p\\
&=\prod_{j=0}^{\lfloor(k-1)/2\rfloor}B_p(f_x(j),f_y(j))\ \mathrm{MOD}\ p.
\end{aligned}$$

This identity allows us to split the computation of $B_p(x,y)$ into a finite number of computations of $B_p(f_x(j),f_y(j))$, which we then multiply modulo p.

Consider the following $\{B_p,+\}$-formulas:

$$\begin{aligned}
&F_1(x,y,z): && x\neq 0\vee y\neq 0,\\
&F_2^i(x,y,z): && (x\neq 0\vee y\neq 0)\wedge B_p(x,y)=i\quad (i=0,1,\ldots,p-1),\\
&F_3(x,y,z): && z\neq 0,\\
&F_4^j(x,y,z): && z=j\quad (j=1,\ldots,p-1).
\end{aligned}$$

We now find a $\{\subseteq,\ll\}$-formula F which describes the computation of $B_p(x,y)$. The idea is to introduce p finite sets $Y_0,Y_1,\ldots,Y_{p-1}$ which encode the computation of $\prod_{j=0}^{\lfloor(k-1)/2\rfloor}B_p(f_x(j),f_y(j))$ modulo p, in the following way:

• If $B_p(f_x(\lfloor (k-1)/2 \rfloor), f_y(\lfloor (k-1)/2 \rfloor)) = h$ then $\lfloor (k-1)/2 \rfloor \in Y_h$, and $\lfloor (k-1)/2 \rfloor \notin Y_i$ for every $i \neq h$.

• For every $j < \lfloor (k-1)/2 \rfloor$, if $j+1 \in Y_l$ and $B_p(f_x(j), f_y(j)) = m$ then $j \in Y_{lm \,\mathrm{MOD}\, p}$, and $j \notin Y_i$ for every $i \neq lm$ MOD p.

This means that for every $j \leq \lfloor (k-1)/2 \rfloor$, $j \in Y_l$ if and only if l equals the partial product $\prod_{i=j}^{\lfloor (k-1)/2 \rfloor} B_p(f_x(i), f_y(i))$ MOD p. Thus one sees that at the end of the computation, the value of $B_p(x,y)$ will be the (unique) integer l such that $0 \in Y_l$. These ideas lead to the following definition for F:

$$
\begin{aligned}
&F(T_1, T_2^0, T_2^1, \ldots, T_2^{p-1}, T_3, T_4^1, T_4^2, \ldots, T_4^{p-1}) : \\
&\quad (\mathrm{Empty}(T_1) \Rightarrow (\mathrm{Singl}(T_3) \wedge \mathrm{Zero} \subseteq T_4^1)) \\
&\quad \wedge \neg \, \mathrm{Empty}(T_1) \Rightarrow \exists Y_0, Y_1, \ldots, Y_{p-1} \\
&\quad \Big(\mathrm{Sup}(Y_0, Y_1, \ldots, Y_{p-1}) = \mathrm{Sup}(T_1) \\
&\quad \wedge \bigwedge_{i=0}^{p-1} (\mathrm{Sup}(T_1) \subseteq T_2^i \Leftrightarrow \mathrm{Sup}(T_1) \subseteq Y_i) \\
&\quad \wedge \forall Z \Big((\mathrm{Singl}(Z) \wedge Z \ll \mathrm{Sup}(T_1)) \Rightarrow \\
&\quad \Big(\neg Z \subseteq T_1 \Rightarrow \bigwedge_{i=0}^{p-1} (\mathrm{Succ}(Z) \subseteq Y_i \Leftrightarrow Z \subseteq Y_i) \Big) \\
&\quad \wedge \Big(Z \subseteq T_1 \Rightarrow \bigwedge_{0 \leq i,j \leq p-1} ((\mathrm{Succ}(Z) \subseteq Y_i \wedge Z \subseteq T_2^j) \Leftrightarrow Z \subseteq Y_{ij \,\mathrm{MOD}\, p}) \Big) \Big) \\
&\quad \wedge \bigwedge_{j=1}^{p-1} (\mathrm{Zero} \subseteq Y_j \Rightarrow (\mathrm{Singl}(T_3) \wedge \mathrm{Zero} \subseteq T_4^j)) \\
&\quad \wedge \mathrm{Zero} \subseteq Y_0 \Rightarrow \mathrm{Empty}(T_3) \Big).
\end{aligned}
$$

Finally, one checks that for all $x, y, z \in \mathbb{N}$, $\widetilde{B}'_p(f_x, f_y, f_z)$ holds if and only if $F(\ldots)$ does, with

$$T_i = \{ n \in \mathbb{N} : \langle \mathbb{N}; B_p, + \rangle \models F_i(f_x(n), f_y(n), f_z(n)) \} \quad \text{for every } i \in \{1, 3\}$$

and

$$T_2^i = \{ n \in \mathbb{N} : \langle \mathbb{N}; B_p, + \rangle \models F_2^i(f_x(n), f_y(n), f_z(n)) \} \quad (i = 0, 1, \ldots, p-1),$$
$$T_4^j = \{ n \in \mathbb{N} : \langle \mathbb{N}; B_p, + \rangle \models F_4^j(f_x(n), f_y(n), f_z(n)) \} \quad (j = 1, \ldots, p-1). \ \blacksquare$$

From Lemmas 5.9 and 5.10 we now deduce the following:

COROLLARY 5.11. *The structure* $\langle \mathbb{N}_0^{(\mathbb{N})}; \widetilde{B}'_p, \widetilde{\mathrm{SQ}}'_p\rangle$ *is a generalized power of* $\langle \mathbb{N}; B_p, +\rangle$ *relative to* $\langle \mathcal{P}_{\mathrm{f}}(\mathbb{N}); \subseteq, \ll\rangle$.

LEMMA 5.12. *The elementary theory of* $\langle \mathcal{P}_{\mathrm{f}}(\mathbb{N}); \subseteq, \ll\rangle$ *is decidable.*

Proof. By [Ko3] the elementary theory of $\langle \mathbb{N}; B_2, +\rangle$ is decidable. Consider the relation $x \prec y$ over $\mathbb{N}$ which holds if and only if there exists $i \in \mathbb{N}$ such that $x < 2^i \le y$. Using $+$ and Pow_2 one easily defines $\prec$ in $\langle \mathbb{N}; B_2, +\rangle$. Furthermore, $\sqsubseteq_2$ is definable in $\langle \mathbb{N}; B_2, +\rangle$. It follows that the elementary theory of $\langle \mathbb{N}; \sqsubseteq_2, \prec\rangle$ is decidable. Now let $h : \mathbb{N} \to \mathcal{P}_{\mathrm{f}}(\mathbb{N})$ be the function which maps every integer $n = \sum_{j=0}^{k} 2^{i_j}$ (with i_j pairwise distinct) to $h(x) = \{i_0, i_1, \ldots, i_k\}$. h is obviously 1-1 and onto; moreover, one checks that for all $n, n' \in \mathbb{N}$, $n \sqsubseteq_2 n'$ if and only if $h(n) \subseteq h(n')$, and $n \prec n'$ if and only if $h(n) \ll h(n')$. Therefore the structures $\langle \mathbb{N}; \sqsubseteq_2, \prec\rangle$ and $\langle \mathcal{P}_{\mathrm{f}}(\mathbb{N}); \subseteq, \ll\rangle$ are isomorphic, from which the result follows. ∎

THEOREM 5.13. *For every prime p the elementary theory of* $\langle \mathbb{N}; B_p, \mathrm{SQ}_p\rangle$ *is decidable.*

Proof. By Corollary 5.11 the structure $\langle \mathbb{N}_0^{(\mathbb{N})}; \widetilde{B}'_p, \widetilde{\mathrm{SQ}}'_p\rangle$ is a generalized power of $\langle \mathbb{N}; B_p, +\rangle$ relative to $\langle \mathcal{P}_{\mathrm{f}}(\mathbb{N}); \subseteq, \ll\rangle$. By [Ko3] and Lemma 5.12 the last two structures have decidable elementary theories, thus by Theorem 5.7 the same holds for $\langle \mathbb{N}_0^{(\mathbb{N})}; \widetilde{B}'_p, \widetilde{\mathrm{SQ}}'_p\rangle$. Now this structure is isomorphic to $\langle \mathbb{N}; B'_p, \mathrm{SQ}'_p\rangle$, which has therefore a decidable elementary theory, and the result follows from the fact that B_p and SQ_p are definable in this structure. ∎

Acknowledgements. The authors wish to thank the anonymous referee for many valuable corrections and suggestions.

References

[BJW] P. T. Bateman, C. G. Jockusch and, A. R. Woods, *Decidability and undecidability with a predicate for the primes*, J. Symbolic Logic 58 (1993), 672–687.

[Be] A. Bès, *On Pascal triangles modulo a prime power*, Ann. Pure Appl. Logic 89 (1997), 17–35.

[Bo] B. A. Bondarenko, *Generalized Pascal Triangles and Pyramids, their Fractals, Graphs and Applications*, "Fan", Tashkent, 1990 (in Russian).

[BHMV] V. Bruyère, G. Hansel, C. Michaux and R. Villemaire, *Logic and p-recognizable sets of integers*, Bull. Belg. Math. Soc. Simon Stevin 1 (1994), 191–238.

[Ce] P. Cegielski, *Definability, decidability, complexity*, Ann. Math. Artificial Intelligence 16 (1996), 311–342.

[Di] L. E. Dickson, *History of the Theory of Numbers*, Vol. I, Chelsea, New York, 1952, Ch. IX.

[El] W. and F. Ellison, *Prime Numbers*, Hermann, Paris, 1985.

[FV] S. Feferman and R. L. Vaught, *The first order properties of products of algebraic systems*, Fund. Math. 47 (1959), 57–103.

[Fi] N. J. Fine, *Binomial coefficients modulo a prime*, Amer. Math. Monthly 54 (1947), 589–592.

[Ko1] I. Korec, *Definability of arithmetic operations in Pascal triangle modulo an integer divisible by two primes*, Grazer Math. Ber. 318 (1993), 53–62.

[Ko2] —, *Structures related to Pascal's triangle modulo 2 and their elementary theories*, Math. Slovaca 44 (1994), 531–554.

[Ko3] —, *Elementary theories of structures containing generalized Pascal triangles modulo a prime*, in: Proc. 5th Conf. on Discrete Mathematics and Applications (Blagoevgrad/Predel, 1994), S. Shtrakov and I. Mirchev (eds.), Blagoevgrad, 1995, 91–102.

[Lu] E. Lucas, *Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier*, Bull. Soc. Math. France 6 (1878), 49–54.

[MMT] R. McKenzie, J. Mycielski and D. Thompson, *On boolean functions and connected sets*, Math. Systems Theory 5 (1971), 259–270.

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

[Ri] D. Richard, *All arithmetical sets of powers of primes are first-order definable in terms of the successor function and the coprimeness predicate*, Discrete Math. 53 (1985), 221–247.

[Ro] J. Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic 14 (1949), 98–114.

[Si] D. Singmaster, *Notes on binomial coefficients III—Any integer divides almost all binomial coefficients*, J. London Math. Soc. (2) 8 (1974), 555–560.

[Th] W. Thomas, *A note on undecidable extensions of monadic second order successor arithmetic*, Arch. Math. Logik Grundlagenforsch. 17 (1975), 43–44.

[Vi] R. Villemaire, *Joining k- and l-recognizable sets of natural numbers*, in: Proc. 9th Sympos. Theoretical Aspects of Computer Science STACS'92 (Paris), Lecture Notes in Comput. Sci. 577, Springer, 1992, 83–94.

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

Université Paris 7
Equipe de Logique URA 753
2, place Jussieu
75251 Paris Cedex 05, France
E-mail: bes@logique.jussieu.fr

Mathematical Institute
Slovak Academy of Sciences
Štefánikova 49
81473 Bratislava, Slovakia
E-mail: korec@savba.sk

Received 7 November 1996;
in revised form 27 July 1997