Mathematical Institute
Slovak Academy of Sciences, Bratislava

Preprint 19/1996

Ivan Korec

Definability of arithmetical operations from Pascal's triangle modulo n and arithmetical functions

June 24, 1996

PREPRINT SERIES

DEFINABILITY OF ARITHMETICAL OPERATIONS FROM PASCAL'S TRIANGLE MODULO n AND ARITHMETICAL FUNCTIONS

Ivan KOREC

Abstract. It is proved that for every $n > 1$ the arithmetical operations $+$, $\times$ are definable in the structure $\langle \mathbb{N}; B_n, f \rangle$ where, $B_n(x,y) = \binom{x+y}{x} \operatorname{MOD} n$ and f is one of the following functions: Euler function φ, Carmichael function λ, the sum of divisor function σ, the number of divisors function τ, and the prime counting function π. The same result is proved also for the structure $\langle \mathbb{N}; +, \tau \rangle$.

1. Introduction and notation

$\mathbb{N}$ will denote the set of nonnegative integers and $\mathbb{P}$ the set of primes. The symbols $+$, $\times$ will denote the classical arithmetical operations on the set $\mathbb{N}$, and $\mathbf{s}$ denotes the successor. The operations modulo n will be denoted $\oplus_n$, $\otimes_n$. The quotient and the rest by integer division will be denoted by DIV, MOD, respectively. The symbols $|$, $\perp$ will denote divisibility and coprimeness. We shall also use further classical notation. A symbol for a set $X \subseteq \mathbb{N}^k$ will be used also as a k-ary predicate symbol in the first order formulas; its meaning is fixed. (This is possible because we shall deal with theories of single structures only.)

We shall consider the class of structures of the form $\langle \mathbb{N}; F_1, \dots, F_r, R_1, \dots, R_s \rangle$, r, s finite, where the operations $F_1, \dots, F_r$ and relations $R_1, \dots, R_s$ are *arithmetical*, i.e. first order definable in the structure $\langle \mathbb{N}; +, \times \rangle$. (We shall deal with concrete structures, which will obviously belong to the considered class. No general theory of this class is presented.) The class of such structures is quasi-ordered with respect to first order definability, and the structure $\langle \mathbb{N}; +, \times \rangle$ is its greatest element. For the structures equivalent with $\langle \mathbb{N}; +, \times \rangle$ we shall use the short term "d-strongest", which can be understood as abbreviation for "strongest with respect to first order definability":

Definition 1.1. *A structure $\mathcal{S}$ (from the class mentioned above) will be called d-strongest if the operations $+$, $\times$ on $\mathbb{N}$ are first order definable in $\mathcal{S}$.*

If a structure is d-strongest then its theory contains the true first order arithmetic in a rather direct sense; hence it is undecidable. The converse is not true. The statement "the structure $\mathcal{S}$ is d-strongest" is the strongest undecidability result

---

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

1991 *Mathematics Subject Classification.* Primary 03F30, Secondary 11A25, 11B65.

Key words and phrases. Definability, Undecidable theories, Pascal's triangle, Arithmetic functions.

which can be expected. (Of course, there are structures with harder theories outside of the considered class.)

Classical results of J. Robinson say that $\langle \mathbb{N}; \mathbf{s}, \times \rangle$ and $\langle \mathbb{N}; \mathbf{s}, | \rangle$ are d-strongest. By a result of [Wo] the structure $\langle \mathbb{N}; <, \perp \rangle$ is d-strongest; it is not known whether $\langle \mathbb{N}; \mathbf{s}, \perp \rangle$ is d-strongest, but the problem is equivalent with an interesting number-theoretical conjecture. By [Pu] also the structure $\langle \mathbb{N}; +, \mathrm{Sq} \rangle$, where Sq is the set of squares, is d-strongest; by [Bu] Sq can be replaced by the set of values of any non-linear polynomial with nonnegative integer coefficients.

In the present paper structures containing $B_n(x,y) = \binom{x+y}{x} \operatorname{MOD} n$ will be considered; the function B_n will be called Pascal's triangle modulo n. Some results concerning such structures are contained in [K2]–[K5], [Be]. For example, if $n > 0$ then $\langle \mathbb{N}; B_n \rangle$ is d-strongest if and only if n is divisible by two distinct primes; otherwise the first order theory of $\langle \mathbb{N}; B_n \rangle$, and even that of of $\langle \mathbb{N}; B_n, + \rangle$, is decidable. For every $n > 1$ the structure $\langle \mathbb{N}; B_n, \times \rangle$ is d-strongest. Also the structure $\langle \mathbb{N}; B_2, \mathrm{Sq} \rangle$, where Sq denote the set of squares was shown to be d-strongest; this result can be extended to arbitrary $n > 1$ instead of 2.

In the present paper we shall deal with the structures containing a Pascal's triangle modulo n and a (more or less) classical arithmetical function or relation. We shall study their elementary theories from decidability and definability point of view.

2. B_n, $+$ AND SQUARES OF PRIMES

Remember briefly several results of [K2] and [K3] about definability in $\langle \mathbb{N}; B_n \rangle$ for n prime: The set Pow_n of powers of n, the n-ary masking relation $\sqsubseteq_n$, the $n$ary carry-free addition $\boxplus_n$, and the constants up to $\lceil n-1 \rceil$ are definable from B_n. (The formula $x \sqsubseteq_n y$ will mean that the n-ary digits of x do not exceed the corresponding n-ary digits of y. The carry-free addition will be used below only with one argument equal to 1.) The usual addition is not definable in $\langle \mathbb{N}; B_n \rangle$. However it is definable in $\langle \mathbb{N}; B_n, \mathbf{s} \rangle$; the function $\mathbf{s}$ can be replaced by the function $\mathit{NextPow}_n$, "next power of n".

Let us denote $\mathrm{SqPow}_n = \{(x, x^2) \mid x \in \mathrm{Pow}_n\}$ the squaring of powers of n and $\mathrm{SqP} = \{(x, x^2) \mid x \in \mathbb{P}\}$ the squaring of primes. We shall show that $\times$ is definable from B_n, $+$ and any of the above relations. The result for SqPow_n is a generalization of Lemma 4.3 in [K3] (which was formulated for $n = 2$); therefore its proof will be only sketched.

Lemma 2.1. *For every $n > 1$ the structure $\langle \mathbb{N}; B_n, +, \mathrm{SqPow}_n \rangle$ is d-strongest.*

Sketch of proof. We ought to define the operation $\times$. We may assume that n is prime. (If n has two distinct prime divisors then by [K2] the operation B_n alone suffices to define both $+$, $\times$. Otherwise we can define B_p and SqPow_p for the prime divisor p of n, and continue with B_p, SqPow_p.) We can code finite sequences of integers, in particular initial segments of the sequence of squares. So we can define the set Sq of squares, and then define $\times$ from $+$ and Sq. The idea of coding is: To construct the code y of a sequence $\mathbf{x} = (x_0, x_1, \ldots, x_k)$, consider $n$ary expansions of all x_i. Then (for all i, j) use the jth digit of x_i as the $2^i \cdot (2j+1)$th digit of y. All digits of y which are not determined in this way will be equal to 0. Notice that

$\mathbf{x}$ consists of consecutive squares if $x_0 = 0$, $x_1 = 1$ and $x_{i+2} + x_i = 2x_{i+1} + 2$ for all $i \leq k-2$; these conditions can be expressed. $\square$

Lemma 2.2. *For every $n > 1$ the structure $\langle \mathbb{N}; B_n, +, \mathrm{SqP} \rangle$ is d-strongest.*

Proof. We may assume that n is prime, and we ought to define $\times$. The predicate Pow_n is definable from B_n, and then SqPow_n can be defined by the formula

$$\begin{aligned}\mathrm{SqPow}_n(x,y) \iff & x = 1 \wedge y = 1 \vee x = n \wedge y = n^2 \\ & \vee x > n \wedge y > n^2 \wedge \mathrm{Pow}_n(x) \wedge \mathrm{Pow}_n(y) \wedge \\ & \wedge \forall z, w\big(\mathrm{SqP}(z,w) \implies (z \leq x \iff w \leq y)\big).\end{aligned}$$

The constants n, n^2 can be defined e.g. as $1 + \cdots + 1$. It is important here that there is at most one power of n between any two consecutive primes, and (with one exception) also between their squares. (The exception exists only for $n = 2$ and the primes 2, 3; it is the only reason why the case $x = n$ is considered separately.) The statement is obvious for consecutive primes $p < q$ such that $q^2 < 2p^2$, i.e. for all $p \geq 11$. The remaining cases can be easily considered.

After defining SqPow_n we can apply Lemma 2.1. $\square$

3. B_n AND FOUR CLASSICAL ARITHMETICAL FUNCTIONS

The structures with B_n and one of three multiplicative arithmetical functions φ, σ, τ will be considered there. Moreover, the Carmichael function λ will be similarly considered; it is not multiplicative but its properties are very closed to that of the Euler function φ.

Theorem 3.1. *For every $n > 1$ the structure $\langle \mathbb{N}; B_n, \varphi \rangle$ is d-strongest.*

Proof. We may assume that n is prime. (Otherwise we can define B_p for a prime divisor p of n, and continue with B_p.) By results of [K2] and [K3] we know that (using B_n only) Pow_n and carry-free addition (in $n$ary number system) are definable, and that it suffices to define successor function or $\mathit{NextPow}_n$ or ordering of Pow_n instead of $+$.

Now we can use that $\varphi(n^k) = (n-1) \cdot n^{k-1}$, which enables us to define

$$\begin{aligned}y = \mathit{NextPow}_n(x) \iff & \neg \mathrm{Pow}_n(x) \wedge y = 0 \vee \\ & \vee\ \mathrm{Pow}_n(x) \wedge \mathrm{Pow}_n(y) \wedge x \sqsubseteq \varphi(y).\end{aligned}$$

After that we can define squaring of primes by the formula

$$\mathrm{SqP}(x,y) \iff \mathbb{P}(x) \wedge \varphi(y) + x = y \wedge \forall z\big(\varphi(z) + x = z \implies z \leq y\big).$$

Indeed, take a prime x and consider the equation $\varphi(y) + x = y$. We have to prove that $y = x^2$ is its greatest solution. Let z be its arbitrary solution; obviously $z \geq 2$, and z is composite. If $z = p^k$ for some prime p and $k > 1$ then $p^{k-1} | x$ divides both, z and $\varphi(z)$, hence $p^{k-1} | x$, and then $p = x$, $k - 1 = 1$, i.e. $z = x^2$. If z is not a prime power then $z = z_1 z_2$ for some relatively prime $z_1, z_2 > 1$. Then

$$x = z - \varphi(z) = z - \varphi(z_1) \cdot \varphi(z_2) \geq z - (z_1 z_2 - z_1 - z_2 + 1) = z_1 + z_2 - 1,$$

and hence $z = z_1 z_2 \leq \left(\frac{x+1}{2}\right)^2 < x^2$.

When squaring of primes is defined we can use Lemma 2.1 to define multiplication. $\square$

Now we shall consider *Carmichael function* λ. Remember that $\lambda(n)$ is the smallest positive integer e such that for all x relatively prime to n the congruence $x^e \equiv 1 \pmod{n}$ holds. (We also define $\lambda(0) = 1$.)

Theorem 3.2. *For every $n > 1$ the structure $\langle \mathbb{N}; B_n, \lambda \rangle$ is d-strongest.*

Proof. We can use the same considerations as in the proof of the previous theorem. It is important that $\lambda(n) \leq \varphi(n)$ for all $n \in \mathbb{N}$, with equality for all prime powers. $\square$

Theorem 3.3. *For every $n > 1$ the structure $\langle \mathbb{N}; B_n, \sigma \rangle$ is d-strongest.*

Proof. Similarly as in above theorems we may assume that n is a prime. We can define the ordering of powers of n by the formula

$$x \leq_{\mathrm{Pow}_n} y \iff \mathrm{Pow}_n(x) \wedge \mathrm{Pow}_n(y) \wedge x \sqsubseteq \sigma(y).$$

This suffice to define $+$. Now we can define squaring of primes by the formula

$$\mathrm{SqP}(x, y) \iff \mathbb{P}(x) \wedge y + x + 1 = \sigma(y) \wedge \forall z\big(z + x + 1 = \sigma(z) \implies z \leq y\big).$$

Indeed, take any prime x and consider the equation $y + x + 1 = \sigma(y)$. We have to prove that $y = x^2$ is its greatest solution; it is oviously a solution. Let z be its arbitrary solution; obviously $z \geq 2$, and z is composite. If z is not a prime square then z has at least one pair of distinct proper divisors with product z, and hence $\sigma(z) > z + 2\sqrt{z} + 1$. Then $2\sqrt{z} < x$, which implies $z < x^2$. If z is a prime square we obtain $z = x^2 = y$.

It remains to use Lemma 2.1 as above. $\square$

Theorem 3.4. *For every $n > 1$ the structure $\langle \mathbb{N}; B_n, \tau \rangle$ is d-strongest.*

Proof. We shall often use that x is a nonzero square if and only if $\tau(x)$ is odd. Indeed, the divisors of x distinct from $\sqrt{x}$ can be partitioned into pairs with product x, and $\sqrt{x}$ is a divisor of x iff x is a square.

If n is composed we can define $+$ (without using τ). Then we can define the set of squares by

$$\mathrm{Sq}(x) \iff \exists y\big(\tau(x) = y + y + 1\big),$$

and Sq, $+$ suffice to define $\times$. So we may assume that n is prime. For $n = 2$ we can define Sq by

$$\mathrm{Sq}(x) \iff x = 0 \vee 1 \sqsubseteq_2 \tau(x),$$

and by [K3] B_2, Sq suffice to define $+$, $\times$. Let n be an odd prime from now on. We can define the set $\mathrm{TPow}_n = \{2x \mid x \in \mathrm{Pow}_n\}$ by

$$\mathrm{TPow}_n(x) \iff \exists! y\big(y \neq 0 \wedge y \neq x \wedge y \sqsubseteq_n x\big).$$

Notice that $\{\tau(x) \mid x \in \mathrm{TPow}_n\}$ consists of all positive even numbers. Therefore we can define

$$\mathrm{Sq}(x) \iff \neg\exists y\big(\mathrm{TPow}_n(y) \wedge \tau(x) = \tau(y)\big).$$

Now B_n and Sq suffice to define $+$ and $\times$. $\square$

The above proof contains also the proof of:

Theorem 3.5. *For every $n > 1$ the structure $\langle \mathbb{N}; +, \tau \rangle$ is d-strongest.*

4. B_n AND THE PRIME COUNTING FUNCTION π

In this section we shall define $+$ at first. Then we shall define "approximate squaring" using the idea that if x is sufficiently big then the density of primes in a suitable neighborhood of x^α is α-times smaller than the density of primes in a neighborhood of x. We shall not use the idea immediately for $\alpha = 2$, but only for $\alpha < \frac{4}{3}$; the reason is in the assumptions of the used theorem on the number of primes in short intervals. We have to multiply three suitable (rational) α to obtain the exponent 2. In this stage only π and $+$ will be used. Further, we use Pow_n (definable from B_n) and "approximate squaring" to define the (exact) squaring of powers of n. After that, we will be able to define multiplication.

Lemma 4.1. *For every $n > 1$ addition is definable in the structure $\langle \mathbb{N}; B_n, \pi \rangle$*

Proof. Similarly as above, we may assume that n is a prime, and it suffices to define the successor $\mathbf{s}$. By [K2] the n-ary masking relation $\sqsubseteq_n$, and the constants up to $\lceil n-1 \rceil$ are definable from B_n. The constant n can be defined by

$$x = n \iff \mathrm{Pow}_n(x) \wedge x \neq 1 \wedge \pi(x) \sqsubseteq_n \lceil n-1 \rceil.$$

(The last part can be replaced by $\exists y, z\big(\pi(x) = B_n(y, z)\big)$.) Then the successor can be defined as follows

$$y = \mathbf{s}(x) \iff x = \lceil n-1 \rceil \wedge y = n \vee x \neq y \wedge \exists z\big(\pi(z) = x \wedge \pi(z \boxplus_n 1) = y\big).$$

(For $n = 2$ we can replace the carry-free addition $\boxplus_n$ by the lattice operation $\sqcup_n$ derived from $\sqsubseteq_n$.) Notice that the case $x = \lceil n-1 \rceil$ had to be considered separately because the addition $\lceil n-1 \rceil + 1 = n$ is not carry-free. $\square$

Now we shall need some special results about distribution of primes. To formulate them we shall use the notations $O()$ and $o()$ in their usual sense from mathematical analysis. We shall also use $\pi(x)$ for arbitrarily real x in the obvious way. The summation index p will range over primes. The following results can be found in [Ka, p. 111-112, 102].

Theorem 4.2. (i) *Let $h \geq x^{0.75} \exp\left(\ln^{0.8} x\right)$ and $x, y \geq x_0 > 0$. Then for some $c_2 > 0$ it holds*

$$\sum_{x < p \leq x+h} \ln p \;=\; h \;+\; O\Big(h \cdot \exp\left(-\ln^{0.1} x\right)\Big), \tag{4.2.1}$$

$$\pi(x) \;=\; \int_2^x \frac{\mathrm{d}\,t}{\ln t} \;+\; O\Big(x \cdot \exp\Big(-c_2 \frac{\ln x}{\ln\ln x}\Big)^{0.6}\Big). \tag{4.2.2}$$

We need not so strong results; estimates with e.g. $O\big(h \cdot \ln^{-5} x\big)$ and $O\big(x \cdot \ln^{-5} x\big)$ would suffice for us instead of those in the theorem.

Theorem 4.3. *Let $1 < \alpha < \frac{4}{3}$ and let the function F_α be defined by*

$$F_\alpha(x) = \min\big\{y \in \mathbb{N} \mid \pi(y+\lfloor 2\alpha\pi(x)\rfloor)-\pi(y) \le \pi(x+\pi(x))+\pi(x-\pi(x))\big\}. \tag{4.3.1}$$

Then there is $x_0 = x_0(\alpha)$ such that for all $x \ge x_0$

$$|F_\alpha(x) - x^\alpha| \le \frac{x^\alpha}{\ln x}. \tag{4.3.2}$$

Proof. Notice before the proof that Theorem 4.3 uses the idea from the introduction of the present section. We need an interval of a length h containing x and an interval of length approximately αh containing $y \approx x^\alpha$. To apply (4.2.1) for y instead of x we need h sufficiently large. On the other, to estimate properly density of primes near x we need h small (but not too small) with respect to x. The choice $h = 2\pi(x)$ would satisfy both requirements (the constant 2 is used only to avoid fractions in some places). The formula (4.2.1) could be applied also for the interval containing x, but a better estimation can be obtained by (4.2.2). Further, it is suitable when x is the center of the interval associated to it. Position of y in its interval is not so important because the interval is relatively much shorter.

Let x be sufficiently large so that Theorem 4.2 can be applied. (E.g., we need to arrange $\pi(x) \ge y \exp\big(\ln^{0.8} y\big)$ for $y = x^\alpha$.) We have:

$$\begin{aligned}
\pi\big(x+\pi(x)\big) - \pi\big(x-\pi(x)\big) &= \int_{x-\pi(x)}^{x+\pi(x)} \frac{\mathrm{d}\,t}{\ln t} + O\Big(x\exp\big(-\frac{c_2}{2}\sqrt{\ln x}\big)\Big) = \\
&= \int_{-\pi(x)}^{\pi(x)} \frac{\mathrm{d}\,t}{\ln(x+t)} + O\Big(\frac{x}{\ln^5 x}\Big) = \int_{-\pi(x)}^{\pi(x)} \frac{\mathrm{d}\,t}{\ln x + \frac{t}{x} + O\big(\frac{t^2}{x^2}\big)} + O\Big(\frac{\pi(x)}{\ln^4 x}\Big) = \\
&= \int_{-\pi(x)}^{\pi(x)} \Big(\frac{1}{\ln x} - \frac{t}{x\ln^2 x} + O\Big(\frac{t^2}{x^2\ln^2 x}\Big)\Big)\mathrm{d}\,t + O\Big(\frac{\pi(x)}{\ln^4 x}\Big) = \\
&= \Big(\frac{t}{\ln x} - \frac{t^2}{2x\ln^2 x} + O\Big(\frac{t^3}{x^2\ln^2 x}\Big)\Big)\Big|_{-\pi(x)}^{\pi(x)} + O\Big(\frac{\pi(x)}{\ln^4 x}\Big) = \\
&= \frac{2\pi(x)}{\ln x} + O\Big(\frac{\pi^3(x)}{x^2\ln^2 x}\Big) + O\Big(\frac{\pi(x)}{\ln^4 x}\Big) = \frac{2\pi(x)}{\ln x}\cdot\Big(1 + O\Big(\frac{1}{\ln^3 x}\Big)\Big).
\end{aligned}$$

For every y, $x \le y \le x^\alpha \cdot (1 - \frac{1}{\ln x})$ we have

$$\begin{aligned}
\pi\big(y + 2\alpha\cdot\pi(x)\big) - \pi(y) &\ge \frac{\sum\limits_{y<p\le y+2\alpha\cdot\pi(x)} \ln p}{\ln y} = \\
&= \frac{2\alpha\cdot\pi(x) + O\big(\pi(x)\cdot\exp(-\ln^{0.1} y)\big)}{\alpha\ln x + \ln\big(1 - \frac{1}{\ln x}\big)} = \\
&= \frac{2\alpha\cdot\pi(x) + O\big(\frac{\pi(x)}{\ln^3 x}\big)}{\alpha\ln x - \frac{1}{\ln x} + O\big(\frac{1}{\ln^2 x}\big)} = \frac{2\alpha\cdot\pi(x)\cdot\big(1 + O\big(\frac{1}{\ln^3 x}\big)\big)}{\alpha\ln x\cdot\big(1 - \frac{1}{\alpha\ln^2 x} + O\big(\frac{1}{\ln^3 x}\big)\big)} = \\
&= \frac{2\pi(x)}{\ln x}\cdot\Big(1 + \frac{1}{\alpha\ln^2 x} + O\Big(\frac{1}{\ln^3 x}\Big)\Big) > \pi\big(x+\pi(x)\big) - \pi\big(x - \pi(x)\big).
\end{aligned}$$

The same inequality can be proved also for $y < x$, although some details must be modified. (For e.g. $y > \pi(x)$ the above computation remains valid in essential; for still smaller y the statement becomes easier. However, these technical details can be omitted at all if we arrange $F_\alpha(x) > x$ directly in the definition of F_α.) Hence we have $F_\alpha(x) \ge x^\alpha \cdot \bigl(1 - \frac{1}{\ln x}\bigr)$.

Similarly for $y = x^\alpha \cdot (1 + \frac{1}{\ln x})$ we have

$$\begin{aligned}
\pi\bigl(y + 2\alpha \cdot \pi(x)\bigr) - \pi(y) &\le \frac{\sum\limits_{y<p\le y+2\alpha\cdot\pi(x)} \ln p}{\ln(y + 2\alpha\cdot\pi(x))} = \\
&= \frac{2\alpha\cdot\pi(x) + O\bigl(\pi(x)\cdot\exp(-\ln^{0.1} y)\bigr)}{\alpha \ln x + \ln\bigl(1 + \frac{1}{\ln x}\bigr) + \ln\bigl(1 + \frac{2\alpha\cdot\pi(x)}{y}\bigr)} = \dots = \\
&= \frac{2\pi(x)}{\ln x}\cdot\Bigl(1 - \frac{1}{\alpha\ln^2 x} + O\Bigl(\frac{1}{\ln^3 x}\Bigr)\Bigr) < \pi\bigl(x+\pi(x)\bigr) - \pi\bigl(x - \pi(x)\bigr),
\end{aligned}$$

and hence $F_\alpha(x) < x^\alpha \cdot \bigl(1 + \frac{1}{\ln x}\bigr)$. (It was important here that $\frac{2\alpha\cdot\pi(x)}{y}$ is smaller than $\frac{1}{\ln^3 x}$.) $\square$

Lemma 4.4. (i) *For every rational $\alpha > 1$ the function α from (4.3.1) is definable in $\langle\mathbb{N}; +, \pi\rangle$.*

(ii) *For all sufficiently large x we have*

$$\Bigl| F_{\frac{14}{11}}\bigl(F_{\frac{11}{9}}\bigl(F_{\frac{9}{7}}(x)\bigr)\bigr) - x^2 \Bigr| \le \frac{4x^2}{\ln x}. \tag{4.4.1}$$

Proof. Let $\alpha = \frac{p}{q}$. At first notice that the function $f(x) = \lfloor \alpha x \rfloor$ is definable:

$$y = \lfloor \alpha x \rfloor \iff q\cdot y \le px \wedge px < q\cdot(y+1);$$

here qy abbreviates $y + \cdots + y$ (q-times), and similarly for px, $q\cdot(y+1)$. Then F_α can be defined by:

$$\begin{aligned}
y = F_\alpha(x) \iff\ & \pi\bigl(y + \lfloor\alpha\cdot 2\pi(x)\rfloor\bigr) + \pi\bigl(x - \pi(x)\bigr) \le \pi(y) + \pi\bigl(x + \pi(x)\bigr) \wedge \\
& \wedge (\forall z < y)\Bigl(\pi\bigl(z + \lfloor\alpha\cdot 2\pi(x)\rfloor\bigr) + \pi\bigl(x - \pi(x)\bigr) > \pi(z) + \pi\bigl(x + \pi(x)\bigr)\Bigr).
\end{aligned}$$

(It remains to eliminate minus signs in $x - \pi(x)$, what is easy; e.g., we can use a bounded variable u for the expression, and ask $u + \pi(x) = x$.)

To prove (4.4.1) denote

$$\gamma = \frac{14}{11}, \qquad \beta = \frac{11}{9}, \qquad \alpha = \frac{9}{7}, \qquad y = F_\alpha(x), \qquad z = F_\beta(y).$$

Notice $\alpha\beta\gamma = 2$ and $1 < \alpha, \beta, \gamma < \frac{4}{3}$, hence we may use (4.3.2), which gives

$$y = x^\alpha\cdot(1 + o(1)), \qquad z = x^{\alpha\beta}\cdot(1 + o(1)), \qquad F_\gamma(z) = x^2\cdot(1 + o(1)).$$

Now we can estimate (for sufficiently large x):

$$\begin{aligned}
\left|F_\gamma(z)-x^2\right| &\le \left|F_\gamma(z)-z^\gamma\right| + \left|F_\beta^\gamma(y)-\left(y^\beta\right)^\gamma\right| + \left|F_\alpha^{\beta\gamma}(x)-\left(x^\alpha\right)^{\beta\gamma}\right| \le \\
&\le \left|F_\gamma(z)-z^\gamma\right| + \gamma(y^\beta)^{\gamma-1}\cdot(1+o(1))\cdot\left|F_\beta(y)-y^\beta\right| + \\
&\qquad + \beta\gamma(x^\alpha)^{\beta\gamma-1}\cdot(1+o(1))\cdot\left|F_\alpha(x)-x^\alpha\right| \le \\
&\le \frac{z^\gamma}{\ln z} + \gamma y^{\beta\gamma-\beta}\cdot(1+o(1))\cdot\frac{y^\beta}{\ln y} + \beta\gamma x^{\alpha\beta\gamma-\alpha}\cdot(1+o(1))\cdot\frac{x^\alpha}{\ln x} \le \\
&\le \left(\frac{1}{\gamma}+\frac{\gamma}{\beta}+\beta\gamma+o(1)\right)\cdot\frac{x^2}{\ln x} \le \frac{4x^2}{\ln x}.
\end{aligned}$$

□

Lemma 4.5. *For every $n<1$ the operation $\times$ is definable in $\langle\mathbb{N}; B_n, +, \pi\rangle$.*

Proof. Let us define

$$H(x) = F_{\frac{14}{11}}\left(F_{\frac{11}{9}}\left(F_{\frac{9}{7}}(x)\right)\right)$$

Choose an integer x_0 such that (4.4.1) holds; we may assume $x_0 > \exp(12)$. Then for all $x \ge x_0$ we have $\frac{2}{3} < \frac{H(x)}{x^2} < \frac{4}{3}$. Using H and x_0 we can define the relation SqPow_n (squaring of powers of n) by

$$\begin{aligned}
\mathrm{SqPow}_n(x,y) \iff\ & \mathrm{Pow}_n(x) \wedge \mathrm{Pow}_n(y) \wedge \\
& \wedge \big(x=1 \wedge y=1 \vee x=n \wedge y=p^2 \vee \cdots \vee \\
& \qquad \vee x \ge x_0 \wedge 2y < 3H(x) \wedge 3H(x) < 4y\big),
\end{aligned}$$

where "…" stands instead of all other cases with $x<x_0$, and multiplication by 2, 3, 4 means the repeated. Now we can apply Lemma 2.2. □

Remark: If we want to write the defining formula (and not only to prove that it exists) we must know x_0 effectively.

Theorem 4.6. *For every $n>1$ the structure $\langle\mathbb{N}; B_n, \pi\rangle$ is d-strongest.*

Proof. It suffices to combine the results above: We can define + by Lemma 4.4, and then × by Lemma 5.5. □

References

[BJW] P. T. Bateman, C. G. Jockusch, A. R. Woods, *Definability and undecidability of theories with a predicate for primes*, Journal of Symbolic Logic **58** (1993), no. 2, 672-687.

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

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

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

[Ka] A. A. Karatsuba, *Foundations of the analytical number theory (in Russian)*, "Nauka", Moscow, 1983.

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

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

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

[K4] ______, *Decidable and undecidable theories of generalized Pascal triangles*, General Algebra and Discrete Mathematics, Potsdam, Sept. 27 – Okt. 1, 1993 (K. Denecke, O. Lüders, eds.), Heldermann-Verlag, Berlin, 1995, pp. 169–179.

[K5] ______, *Elementary theories of structures containing generalized Pascal triangles modulo a prime*, Discrete Mathematics and Applications, Blagoevgrad/Predel, Sept. 12-16, 1994 (S. Shtrakov and Iv. Mirchev, eds.), Blagoevgrad, 1995, pp. 91-102.

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

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

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

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

E-mail address: korec@savba.sk

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

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

Tel./Fax (+421 7) 5249 7316

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

Tel./Fax (+421 95) 6228291

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

Latest preprints of the series:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(continued on inside back cover)