A variant of the system PA: with exponentiation instead of addition and multiplication

Dimiter Skordev

Sofia University

skordev@fmi.uni-sofia.bg

Mathematical Logic Colloquium
June 17, 2021

Introduction

On the occasion of a question posed by Vladimir Sotirov, I will consider a variant PA^ of the axiomatic system PA, in which the primitive functions of addition and multiplication are replaced by the function of exponentiation and which is equivalent to PA in terms of interpretation of one system into another.

Peano's axioms and the axioms of PA

Peano's axioms describe a structure that has one constant and one unary operation. If we denote the carrier of the structure, the constant and the unary operation by N, o and $'$, respectively, the axioms are as follows, where M can be any subset of N:

$$\neg(o = x'), \tag{1}$$

$$x' = y' \to x = y, \tag{2}$$

$$o \in M \,\&\, \forall x(x \in M \to x' \in M) \to \forall x(x \in M). \tag{3}$$

The PA system (Peano Arithmetic) assumes, besides o and $'$, also binary operations of addition and multiplication in N, and the axioms are, first, the above ones with the restriction M to be first-order definable, possibly with parameters, in terms of o, $'$, addition, multiplication and equality, and second, the following four:

$$x + o = x, \quad x + y' = (x + y)', \quad x \cdot o = o, \quad x \cdot y' = x \cdot y + x.$$

The standard model of PA: $N = \mathbb{N}$, $o = 0$, $x' = x + 1$, addition and multiplication have their usual sense.

Some known variants of PA

As far as I know, the system PA (with 0 instead of o) is introduced by Hilbert and Bernays in vol. 1 of "Grundlagen der Mathematik" (the system is denoted by (Z) there).
A not significantly different variant of PA is the one, where the first and third of the four additional axioms are replaced by $x + o = x'$ and $x \cdot o = x$, respectively; in its standard model we have $N = \mathbb{N}^+$, $o = 1$ (think that o is an abbreviation of the word "one"). With 1 instead of o and x' written as $S(x)$, this variant is considered in Julia Robinson's article "Definability and decision problems in arithmetic", published in the Journal of Symbolic Logic in 1949. It is indicated there that the addition function could be eliminated because $z = x + y$ is equivalent to

$$(x \cdot z + 1) \cdot (y \cdot z + 1) = (z \cdot z) \cdot (x \cdot y + 1) + 1$$

if $z \neq 0$ (a much more subtle proof is also given that multiplication is first-order definable in terms of the operation $'$ and the divisibility relation).

What about exponentiation in PA?

In the famous 1931 Gödel's paper, a method is developped for the transformation of primitive recursive definitions into explicit ones by appropriately encoding finite sequences of natural numbers. Making use of this method, one can define in PA a ternary relation exp such that the following three statements are theorems of PA:

$$\exp(x, y, s) \,\&\, \exp(x, y, t) \to s = t,$$
$$\exp(x, o, o'), \quad \exp(x, y, z) \to \exp(x, y', z \cdot x).$$

The last two of them, together with the instance of (3) with $M = \{y \mid \exists z \exp(x, y, z)\}$, yield also

$$\forall x \forall y \exists z \exp(x, y, z).$$

Thus PA allows the definition of a binary operation $\uparrow$ such that the following equaltities identically hold:

$$x \uparrow o = o', \; x \uparrow y' = (x \uparrow y) \cdot x.$$

Clearly $x \uparrow y = x^y$ in the standard model of PA (under the stipulation that $0^0 = 1$).

Axioms of the system PA^

We consider a structure with a given carrier N, a constant o, a unary operation $'$ and a binary operation $\uparrow$. The axioms are, first, the statements (1)–(3), where M can be any subset of N, first-order definable, possibly with parameters, in terms of o, $'$, $\uparrow$ and equality, and second, the following three:

$$u \uparrow (v \uparrow o) = u, \tag{4}$$

$$u \uparrow (v \uparrow x') = (u \uparrow (v \uparrow x)) \uparrow v, \tag{5}$$

$$\forall w(w \uparrow x = w \uparrow y) \to x = y. \tag{6}$$

The standard model of PA^: $N = \mathbb{N}$, $o = 0$, $x' = x + 1$, $x \uparrow y = x^y$.

Remark. The constant o and the operation $'$ can be eliminated from the signature of PA^, because the following equivalences hold in any model of PA^ thanks to the axioms (4), (5) and (6):

$$z = o \leftrightarrow \forall u \forall v(u \uparrow (v \uparrow z) = u),$$

$$z = x' \leftrightarrow \forall u \forall v(u \uparrow (v \uparrow z) = (u \uparrow (v \uparrow x)) \uparrow v).$$

Characterization of addition and multiplication in the standard model of PA^

The following equivalences hold in the standard model of PA^:

$$z = x + y \leftrightarrow \forall u \forall v (u \uparrow (v \uparrow z) = (u \uparrow (v \uparrow x)) \uparrow (v \uparrow y)),$$
$$z = x \cdot y \leftrightarrow \forall v (v \uparrow z = (v \uparrow x) \uparrow y),$$

Indeed, the equalities in their right-hand sides have the form

$$u^{v^z} = \left(u^{v^x}\right)^{v^y},$$
$$v^z = (v^x)^y,$$

hence they are equivalent to

$$u^{v^z} = u^{v^{x+y}},$$
$$v^z = v^{x \cdot y}.$$

Definition of addition in any model of PA^

Definition 1

$$\mathrm{sum}(x,y,z) \leftrightarrow \forall u \forall v (u \uparrow (v \uparrow z) = (u \uparrow (v \uparrow x)) \uparrow (v \uparrow y)).$$

We prove that

$$\mathrm{sum}(x,y,s)\,\&\,\mathrm{sum}(x,y,t) \rightarrow s = t,$$
$$\forall x \forall y \exists z\, \mathrm{sum}(x,y,z).$$

Definition 2

$$z = x + y \leftrightarrow \mathrm{sum}(x,y,z).$$

We prove that

$$x + o = x, \quad x + y' = (x + y)'.$$

Definition of multiplication in any model of PA^

Definition 3

$$\mathrm{prod}(x, y, z) \leftrightarrow \forall v(v \uparrow z = (v \uparrow x) \uparrow y).$$

We prove that

$$\mathrm{prod}(x, y, s) \,\&\, \mathrm{prod}(x, y, t) \rightarrow s = t,$$
$$\forall x \forall y \exists z \, \mathrm{prod}(x, y, z).$$

Definition 4

$$z = x \cdot y \leftrightarrow \mathrm{prod}(x, y, z).$$

We prove that

$$x \cdot o = o, \quad x \cdot y' = (x \cdot y) + x,$$
$$x \uparrow o = o', \; x \uparrow y' = (x \uparrow y) \cdot x.$$

Proofs for addition (i)

$$\mathrm{sum}(x, y, s) \,\&\, \mathrm{sum}(x, y, t) \to s = t.$$

Proof. Suppose $\mathrm{sum}(x, y, s)$ and $\mathrm{sum}(x, y, t)$, i.e. $u \uparrow (v \uparrow s)$ and $u \uparrow (v \uparrow t)$ equal $(u \uparrow (v \uparrow x)) \uparrow (v \uparrow y)$ for all u and v. Then $u \uparrow (v \uparrow s) = u \uparrow (v \uparrow t)$ for all u and v. A twofold application of axiom (6) yields $s = t$. □

$$\mathrm{sum}(x, o, x).$$

Proof. We have to prove that $u \uparrow (v \uparrow x) = (u \uparrow (v \uparrow x)) \uparrow (v \uparrow o)$ for all u and v, and this statement holds thanks to axiom (4).* □

*Reminder: axiom (4) asserts that always $u \uparrow (v \uparrow o) = u$.

Proofs for addition (ii)

$$\mathsf{sum}(x, y, z) \to \mathsf{sum}(x, y', z')$$

Proof. We will prove the stronger statement that $u \uparrow (v \uparrow z) = (u \uparrow (v \uparrow x)) \uparrow (v \uparrow y)$ implies $u \uparrow (v \uparrow z') = (u \uparrow (v \uparrow x)) \uparrow (v \uparrow y')$. Suppose certain u, v, x, y, z satisfy the first of these equalities. Then

$$\begin{aligned} u \uparrow (v \uparrow z') &= (u \uparrow (v \uparrow z)) \uparrow v \\ &= ((u \uparrow (v \uparrow x)) \uparrow (v \uparrow y)) \uparrow v = (u \uparrow (v \uparrow x)) \uparrow (v \uparrow y') \end{aligned}$$

by a twofold application of axiom (5).* □

*Reminder: axiom (5) asserts that always $u \uparrow (v \uparrow x') = (u \uparrow (v \uparrow x)) \uparrow v$.

Proofs for multiplication (i)

$$\mathrm{prod}(x, y, s) \,\&\, \mathrm{prod}(x, y, t) \to s = t.$$

Proof. Suppose $\mathrm{prod}(x, y, s)$ and $\mathrm{prod}(x, y, t)$, i.e. $v \uparrow s = (v \uparrow x) \uparrow y$ and $v \uparrow t = (v \uparrow x) \uparrow y$ for all v. Then $v \uparrow s = v \uparrow t$ for all v, hence $s = t$ by axiom (6). □

$$\mathrm{prod}(x, o, o).$$

Proof. We have to prove that $v \uparrow o = (v \uparrow x) \uparrow o$ for all v. This statement holds thanks to axiom (6) and the fact that

$$u \uparrow (v \uparrow o) = u, \;\; u \uparrow ((v \uparrow x) \uparrow o) = u$$

for all u and v by axiom (4). □

Proofs for multiplication (ii)

$$\text{prod}(x, y, z) \to \text{prod}(x, y', z + x).$$

Proof. We will prove the stronger statement that $v \uparrow z = (v \uparrow x) \uparrow y$ implies $v \uparrow (z + x) = (v \uparrow x) \uparrow y'$. Suppose certain v, x, y, z satisfy the first of these equalities. Then

$$\begin{aligned} w \uparrow (v \uparrow z + x)) &= (w \uparrow (v \uparrow z)) \uparrow (v \uparrow x) \\ &= (w \uparrow ((v \uparrow x) \uparrow y)) \uparrow (v \uparrow x) = w \uparrow ((v \uparrow x) \uparrow y' \end{aligned}$$

for all w according to the definition of sum and axiom (5). The needed conclusion follows by axiom (6). □

Proofs for exponentiation (i)

$$x \uparrow o = o'.$$

Proof. By axioms (5) and (4),

$$w \uparrow (v \uparrow o') = (w \uparrow (v \uparrow o)) \uparrow v = w \uparrow v$$

for all v and w, hence

$$v \uparrow o' = v$$

for all v. Making use of axiom (4) again, we see that

$$v \uparrow (x \uparrow o) = v \uparrow o'$$

for all v and x, hence $x \uparrow o = o'$ for all x. □

Proofs for exponentiation (ii)

$$x \uparrow y' = (x \uparrow y) \cdot x.$$

Proof. We have to prove that

$$\mathrm{prod}(x \uparrow y, x, x \uparrow y'),$$

i.e. $v \uparrow (x \uparrow y') = (v \uparrow (x \uparrow y)) \uparrow x)$ for all v, and this equality follows from axiom (5). □

Independence of axioms (1) and (2)

The above proofs do not use axioms (1) and (2).

Each of the axioms (1) and (2) is independent from the other axioms of PA^.

Proof. The independence of axiom (1) can be shown by considering a structure with one-element carrier. To show the independence of axiom (2), we will concider the structure with carrier $\{0, 1\}$ such that

$$o = 0,\ 0' = 1' = 1,\ x \uparrow y = \max(x, 1 - y).$$

Axioms (1) and (3) are evidently satisfied. The verification of (4) is easy: since always $v \uparrow o = 1$, the equality $u \uparrow (v \uparrow o) = 0$ holds iff $u = 0$. The validity of (5) can be seen as follows:

$$u \uparrow (v \uparrow x') = 0 \leftrightarrow u = 0 \,\&\, v \uparrow x' = 1 \leftrightarrow u = 0 \,\&\, v = 1,$$
$$(u \uparrow (v \uparrow x)) \uparrow v = 0 \leftrightarrow u \uparrow (v \uparrow x) = 0 \,\&\, v = 1 \leftrightarrow u = 0 \,\&\, v = 1.$$

Axiom (6) holds because $0 \uparrow 0 \neq 0 \uparrow 1$. □

A PA^-characterization of the sequence of the prime numbers

Let $p_0, p_1, p_2, \ldots$ be the sequence $2, 3, 5, \ldots$ of the consecutive prime numbers. Next statement leads to a PA^-characterization of this sequence, more direct than the one obtained by translation of its PA-characterization based on primitive recursiveness.

The natural numbers m and n satisfy the condition $p_m = n + 1$ iff $n + 1$ is a prime number and a natural number x exists such that we get a one-to-one correspondence between the prime numbers p not exceeding n and the natural numbers less than m by considering, for each of the numbers p in question, the maximal natural number k such that p^k is a divisor of $x + 1$.

Proof of the statement. If $p_m = n + 1$ then, for instance, the number

$$\prod_{i<m} p_i^i - 1.$$

can be taken as x. The converse direction is trivial. □

Thank you very much
for the attention!