COMMENTATIONES MATHEMATICAE UNIVERSITATIS CAROLINAE

17,3 (1976)

TWIN PRIME PROBLEM IN AN ARITHMETIC WITHOUT INDUCTION

J. MLČEK, Praha

Abstract: We prove that the twin prime problem is undecidable in a first-order arithmetic without induction, stronger than Robinson's arithmetic.

Key words: First-order arithmetic without induction, twin prime problem, undecidable.

AMS: 02H05, 02H15, 10N05 Ref. Ž.: 2.666

Introduction. In this paper we prove that the twin prime problem is undecidable in certain first-order arithmetic Ar without induction.

Moreover, our Ar will be stronger than Robinson's arithmetic (but weaker than Peano one). We will present a parametrical construction of a substructure of a fixed non-standard model $\mathfrak{A}$ of Peano arithmetic. As parameters we will have a submodel of Ar and a non-standard element of $\mathfrak{A}$. The required models are obtained by an appropriate choice of parameters.

§ 0. Preliminaries

0.0.0. Let L be a first-order language with a binary predicate $<$. Let $\varphi(x)$ be a formula of L. We denote by $(\check{\exists} x)\varphi(x)$ the formula $(\forall y)(\exists x)(y< x \ \& \ \varphi(x))$, where y is not a variable of φ . Let $\mathfrak{A}$ and $\mathfrak{B}$ be structures for L. By $\mathfrak{A} \subset \mathfrak{B}$ ($\mathfrak{A} < \mathfrak{B}$) we mean that $\mathfrak{A}$ is a substructure of $\mathfrak{B}$ ($\mathfrak{A}$ is an elementary substructure of $\mathfrak{B}$). The language obtained from L by adding all the names a of individuals a of $\mathfrak{A}$ is denoted by L($\mathfrak{A}$). We expand $\mathfrak{A}$ to a structure $\underline{\mathfrak{A}}$ for L($\mathfrak{A}$) as follows: if $\underline{a}$ is the name of an individual a of $\mathfrak{A}$ then $\underline{\mathfrak{A}}$ assigns a to $\underline{a}$. Let M be a nonempty subset of $\mathfrak{A}$ (where $\mathfrak{A}$ = A is the universe of $\mathfrak{A}$). If there is a substructure of $\mathfrak{A}$ with universe M then it is designated by $\mathfrak{A}/M$.

The expression $\mathfrak{A} \subset \mathfrak{B}$ ($\mathfrak{A} \leq \mathfrak{B}$) stands for 1) $\mathfrak{A} \subset \mathfrak{B}$ ($\mathfrak{A} \prec \mathfrak{B}$), 2), if $a \in A$ and $b \in B$, then $a <^{\mathfrak{B}} b$. ($\mathfrak{B}$ is an (elementary) end-extension of $\mathfrak{A}$.) Writing $\mathfrak{A} \sqsubset \mathfrak{B}$ we mean that $\mathfrak{A} \subseteq \mathfrak{B}$ and $A \neq B$. ($\mathfrak{B}$ is a proper end-extension of $\mathfrak{A}$.) $\mathfrak{A} \prec \mathfrak{B}$ is defined analogously.

0.1.0. The language J of Peano arithmetic P is $\langle 0', +, \cdot, < \rangle$. Let $\mathfrak{N}$ be the standard model of P. For $n \in N$ we denote by n the constant term $0'''\cdots'$, where $'$ is applied n-times.

i,j,k,l,m,n are variables for elements of N.

Remark. We work in the logic with equality.

0.1.1. Let s(i), i = 1,...,5 be symbols such that s(1) is the binary predicate $x \mid y$, s(2) is the unary predicate Prm(x), s(3) is the unary predicate $Prm_2(x)$, s(4) is the binary function e(x,y), and s(5) is the binary function r(x,y).

Let φ_i, $i = 1,2,3,4,5$ be the following formulas: φ_1 is the formula $(\exists z)(y = x.z)$, φ_2 is the formula $y \mid x \longrightarrow (y = \bar{1} \vee y = x)$, φ_3 is $Prm(x) \,\&\, Prm\,(x + \bar{2})$, φ_4 is $(x > 0 \,\&\, y > \bar{1} \,\&\, y^z \mid x \,\&\, y^{z+1} \nmid x) \vee ((x = 0 \vee y \leq \bar{1}) \,\&\, z = 0)$, φ_5 is $(x > 0 \,\&\, y > \bar{1} \,\&\, (\exists u)(u = e(x,y) \,\&\, x = y^u.z)) \vee$ $\vee ((x = 0 \vee y \leq \bar{1}) \,\&\, z = 0)$.

Remark. By $x \nmid y$ we mean $\neg (x \mid y)$.

Let P designate also the theory obtained from P by adding the functions x^y and the symbols s(i) defined by φ_i, $i = 1,\dots,5$.

0.1.2. Throughout the paper, $\mathfrak{M}_0$, $\mathfrak{A}_0$, $\mathfrak{A}_1$, $\mathfrak{A}$ are non-standard models of P such that

$$\mathfrak{N} \prec \mathfrak{M}_0 \prec \mathfrak{A}_0 \prec \mathfrak{A}_1 \prec \mathfrak{A}$$

and α is a fixed element of $A - A_1$. We use McDowell-Specker's theorem. (See [1].)

If there is no danger of confusion, we write $+, ., <$ etc. instead of $+^{\mathfrak{A}}, .^{\mathfrak{A}}, <^{\mathfrak{A}}$ etc.

Let $\mathfrak{A}^*$ be "integers over $\mathfrak{A}$". $\mathfrak{A}^*$ is an ordered domain. If a, b are elements of A^*, $-a$ designates the inverse element of a. $a - b$ designates $a + (-b)$, and $|a|$ designates absolute value of a. If $b \mid a$, we denote by $\frac{a}{b}$ the element c with $a = b.c$. For $B \subseteq A$, we put $B^- = \{-a;\ a \in B\}$ and $B^* = B^- \cup B$. If $\mathfrak{B} \subseteq \mathfrak{A}$ and $\mathfrak{B} \models x < y \longrightarrow$ $\longrightarrow (\exists z)(z \neq 0 \,\&\, x + z = y)$ then $\mathfrak{B}^* = \mathfrak{A}^*/B$ is a subdomain of $\mathfrak{A}^*$.

§ 1. Arithmetic Ar and some models of it

1.0.0. Ar is a first-order theory with the language

J. The nonlogical axioms of Ar are the following:

(a) $x + 0 = x$ $\qquad$ $x.0 = 0$

$x + y = y + x$ $\qquad$ $x.y = y.x$

$x + (y + z) = (x + y) + z$ $\qquad$ $x.(y.z) = (x.y).z$

$x + y' = (x + y)'$ $\qquad$ $x.y' = x.y + z$

$x.(y + z) = x.y + x.z$

(b) 1) $\neg (x \;\; x)$

2) $x < y \,\&\, y < z \longrightarrow x < z$

3) $x < y \vee x = y \vee y < x$

4) $x < y' \longleftrightarrow x < y \vee x = y$

5) $0 < x \vee 0 = x$

6) $0 < x \longrightarrow (\exists y)(y' = x)$

7) $x < y \longleftrightarrow (\exists z \neq 0)(x + z = y)$

(c) $x < y \,\&\, 0 < u \leq v \longrightarrow x + u < y + v \,\&\, x.u < y.v$

(d) (schema) $\{ \sigma_n ;\ n \in N - \{0\} \}$,

where σ_n is the formula $(\forall x)(\exists y < x)(\exists z < \bar{n})(x + y.\bar{n} + z)$.

1.0.1. Proposition. The following sentences are provable in Ar:

(i) $x \neq 0 \longrightarrow (\exists y)(\forall z)(y < x \,\&\, z < x \longrightarrow z \leq y)$,

(ii) $x < y \longrightarrow x' < y'$,

(iii) $x' = y' \longrightarrow x = y$,

(iv) $x < y \longrightarrow x \neq y$.

1.0.2. Let Ar designate also the theory obtained from Ar by adding the symbols s(i) defined by φ_i , $i = 1,2,3$.

1.1.0. Let $\mathfrak{M}_1$ be a model of Ar such that

$$\mathfrak{A}_0 \subseteq \mathfrak{M}_1 \subseteq \mathfrak{A}_1$$

Let $s \in A_0$.

We define, for $i = 0,1$,

$M_{1i}[s] = \{\alpha^k a_k + \dots + \alpha a_1 + a_0;\ k \in N - \{0\},\ a_1, \dots$
$\dots, a_k \in M_1^*,\ a_k > 0,\ a_0 \in M_i^*,$
there exists an $e \in A_0 - N$ such that $s^e \mid^{\mathfrak{M}_1^*} a_1, \dots$
$\dots, s^e \mid^{\mathfrak{M}_1^*} a_k\}$,
$M_{1i}(s) = M_{1i}[s] \cup M_i$.

Lemma. Let $a \in M_{1i}$, $i = 0,1$. Then there is precisely one $k \in N$ and $a_1, \dots, a_k \in M_1^*$, $a_k > 0$, $a_0 \in M_i^*$ such that

$$a = \alpha^k a_k + \dots + \alpha a_1 + a_0.$$

Proof is obvious.

Notation. For $a \in M_{1i}[s]$, $i = 0,1$, we denote by $v(a)$ the standard number k and by $a_1, \dots, a_k$ elements of M_1^*, $a_k > 0$, and a_0 element of M_i^* such that $a = \alpha^k a_k + \dots$ $\dots + \alpha a_1 + a_0$.

Lemma. $M_{1i}(s)$ is the universe of a substructure of $\mathfrak{A}$ $i = 0,1$.

Proof. Let $a, b \in M_{1i}[s]$. Obvously $a' \in M_{1i}[s]$. Let $v(a) \leq v(b)$. For $0 \leq i \leq v(a)$ we have $(a+b)_i = a_i + b_i$, for $v(a) < i \leq v(b)$ we have $(a+b)_i = b_i$. There is an $e \in A_0 - N$ such that $s^e \mid^{\mathfrak{M}_1^*} a_i$, $i = 1, \dots, v(a)$, $s^e \mid^{\mathfrak{M}_1^*} b_i$, $i = 1, \dots, v(b)$. Consequently, $a + b \in M_{1i}[s]$. We also have $(a.b) = \sum_{k+\ell=i} a_k b_\ell$; for $i \geq 1$ we have $s^e \mid^{\mathfrak{M}_1^*} \sum_{k+\ell=1} a_k b_\ell$. Thus, $a.b \in M_{1i}[s]$. Similarly for $a \in M_i$ and $b \in M_{1i}[s]$ etc.

1.1.1. We put $\mathfrak{M}_{1i}(s) = \mathfrak{A}/M_{1i}(s)$, $i = 0,1$. We write $\mathfrak{M}_{1i}$ for $\mathfrak{M}_{1i}(s)$, $i = 0,1$.

1.1.2. Theorem. Let $n \mid s$ for every $n \in N$. Then $\mathfrak{M}_{1i}(s) \models Ar$, $i = 0,1$.

Proof. We have $\mathfrak{M}_{1i} \subseteq \mathfrak{A}$. Only the axioms (b6), (b7) and the schema (d) are not general closures of open formulas and, consequently it suffices to prove that $\mathfrak{M}_{1i}$ is a model of these axioms. Obviously $\mathfrak{M}_{1i} \models$ (b6). We will prove $\mathfrak{M}_{1i} \models$ (b7). Let $a, b \in M_{1i}[s]$ and $a < b$. Thus $v(a) \leq v(b)$. If $v(a) = v(b)$, put $j = \max\{i;\ a_i \neq b_i\}$. If $b_j - a_j < 0$, then we have $\alpha^j(b_j - a_j) + \ldots + (b_0 - a_0) \leq$ $\leq -\alpha^j + \alpha^{j-1}|b_{j-1} - a_{j-1}| + \ldots + |b_0 - a_0| \leq -$ $- \alpha^j + \alpha^{j-1}.j.\max\{|b_i - a_i|\ ;\ i = 0,\ldots, j-1\} < 0$. Thus $b_j - a_j > 0$. On the other hand, if $v(a) < v(b)$ then obviously $b - a \in M_{1i}[s]$. Thus $\mathfrak{M}_{1i} \models$ (b7). It remains to prove the schema (d). Let $n \in N$, $n > 0$, $a \in M_{1i}[s]$, $k =$ $= v(a)$. There are $\tilde{a}_0 \in M_i^*$, $\tilde{\tilde{a}}_0 \in M_i^*$ such that $0 \leq \tilde{\tilde{a}}_0 < n$ and $a_0 = n.\tilde{a}_0 + \tilde{\tilde{a}}_0$.

Put $b = \alpha^k . \frac{a_k}{n} + \ldots + \alpha . \frac{a_1}{n} + \tilde{a}_0$. There exists an $e \in A_0 - N$ such that $s^e \mid^{\mathfrak{M}_1^*} a_i,\ \frac{a_i}{n} \in M_1^*$ and $s^{e-1} \mid^{\mathfrak{M}_1^*} \frac{a_i}{n}$, $i = 1,\ldots,k$. Consequently, $b \in M_{1i}[s]$. Evidently $a = n.b + \tilde{\tilde{a}}_0$. Hence $\mathfrak{M}_{1i} \models \sigma_n$.

1.2.0. Let $M \subseteq |\mathfrak{A}|$, $a \in M$. We say that a is decomposable in M if there are $b, c \in M$ such that $a = b.c$.

1.2.1. Lemma. Let $a \in M_{1i}[s]$, $a_0 \in \{-1, 1\}$, $v(a) \geq 2$. Then a is decomposable in $M_{1i}[s]$, $i = 0,1$.

Proof. $a_0 = 1$. Let $d, e \in A_0 - N$, $e < d$, $\hat{a}_i \in M_1^*$, $a_i =$ $= \hat{a}_i . s^{d+e}$, $i = 1,\ldots,k$, $k = v(a)$. Let $x_0 = y_0 = 1$, $x_1 =$ $= s^e$ and $y_{i+1} = a_{i+1} - y_i . s^e$ if $0 \leq i < k-1$ and $y_{k-1} =$ $= \hat{a}_k . s^d$.

Obviously, $\frac{y_i}{s^e} \in M_1^*$, $i = 1,\dots,k-1$. Thus, $y = \alpha^{k-1}.y_{k-1} + \dots + 1 \in M_{1i}[s]$, $x = \alpha.s^e + 1 \in M_{1i}[s]$. We have $(x.y)_0 = 1$, $(x.y)_i = y_i + s^e y_{i-1} = a_i - y_{i-1}.s^e + y_{i-1}.s^e = a_i$ for $i = 1,\dots,k-1$ and $(x.y)_k = s^e y_{k-1} = a_k$. Consequently, $a = x.y$. Analogously for $a_0 = -1$.

1.2.2. Lemma. Let $a \in M_{1i}[s]$, $b \in M_i$, $i = 0,1$.

(i) If $\mathfrak{M}_{1i} \models \underline{b} \mid \underline{a}$ then $\mathfrak{M}_1^* \; \underline{b} \mid \underline{a}_j$, $j = 0,\dots,v(a)$.

(ii) If $b \mid s$ and $\mathfrak{M}_i^* \models \underline{b} \mid \underline{a}_0$ then $\mathfrak{M}_{1i} \models \underline{b} \mid \underline{a}$.

Proof. (i) If $a = b.c$ and $c \in M_{1i}[s]$, then $a_i = b.c_i$, $i = 0,1,\dots,v(a)$.

(ii) We have $\frac{s}{b} \in A_0$, and hence $\frac{a_i}{b} \in M_1^*$, $i = 1,\dots,v(a)$. Since $\frac{a_0}{b} \in M_1^*$, the statement follows.

§ 2. The consistency of Ar with $\neg(\check{\exists} x)\mathrm{Prm}(x)$ and with $(\check{\exists} x)\mathrm{Prm}(x) \;\&\; \neg(\check{\exists} x)\mathrm{Prm}_2(x)$

The models in question are $\mathfrak{M}_{10}(s)$ with $\mathfrak{M}_1 = \mathfrak{A}_1$.

2.0.0. Theorem. $\mathrm{Ar} \cup \{\neg(\check{\exists} x)\mathrm{Prm}(x)\}$ is consistent.

Proof. Let $L \in A_0 - M_0$, $s = L!$. We prove that $\mathfrak{M}_{10} = \mathfrak{M}_{10}(s)$ (with $\mathfrak{M}_1 = \mathfrak{A}_1$) is the required model. First, $s \in A_0$ and for every standard n we have $n \mid s$. Thus, $\mathfrak{M}_{10}(s) \models \mathrm{Ar}$ follows by 1.1.2.

Let $a \in M_{10}[s]$, $v(a) \geq 2$. If $a_0 = \pm 1$, then $\mathfrak{M}_{10} \models \neg \mathrm{Prm}(a)$ follows from 1.2.1. If $a_0 = 0$ then evidently $\mathfrak{M}_{10} \models \neg \mathrm{Prm}(\underline{a})$. If $a_0 \notin \{0,+1,-1\}$, then $|a_0| \in M_0$ and $|a_0| \mid^{\mathfrak{M}_{10}} a$ (this follows from $|a_0| \mid s$ and (ii) of 1.2.2). Consequently, $a \in M_{10}[s]$ and $v(a) \geq 2$ implies

$\mathfrak{M}_{10} \models \underline{a} < x \rightarrow \neg\, Prm(x)$.

Now, we will prove the consistency of Ar with

$$(\check{\exists} x)Prm(x) \;\&\; \neg\, (\check{\exists} x)Prm_2(x).$$

2.1.0. As it is well known,

(i) $P \vdash Prm(p) \& p \mid x.y \longrightarrow p \mid x \vee p \mid y$,

(ii) $P \vdash Prm(p) \& p \nmid z \& z \mid p^x.y \longrightarrow z \mid y$.

2.1.1. Let $p \in M_0 - N$ be prime, $L \in A_0 - M_0$ and

$$s = r(L!,p).$$

(For the definition of r see 0.1.1.)

<u>Lemma</u>. If $d \in M_0$ and $d > 1$, then $r(d,p) \mid s$.

Proof. We first prove that $c \in M_0$ and $p \nmid c$ implies $c \mid s$. This follows from (ii) of 2.1.0 using $c \mid L!$ and $L! = p^{e(L!,p)}.s$.

We have $r(d,p) < d$, hence $r(d,p) \in M_0$ and $p \nmid r(d,p)$. Consequently, $r(d,p) \mid s$.

As a consequence we obtain immediately!

<u>Corollary</u>. For every standard n, $n \mid s$.

2.1.2. Let $\mathfrak{M}_1 = \mathfrak{A}_1$.

$\mathfrak{M}_{10}(s) \models$ Ar follows from 1.1.2 by Corollary from 2.1.1.

<u>Theorem.</u> (1) $\mathfrak{M}_{10}(s) \models (\check{\exists} x)Prm(x)$,

(2) $\mathfrak{M}_{10}(s) \models \neg\, (\check{\exists} x)Prm_2(x)$.

Proof. (1) (a) Let $a = \alpha^k a_k + a_0 \in M_{10}[s]$, $a_k \in M_1$, $a_0 \in M_0$, $Prm(a_0)$ and $a_0 \nmid a_k$. We prove that a is not decomposable in $M_{10}[s]$. If $a = x.y$ and $x, y \in M_{10}[s]$, then $k \geq 2$, $v(x) + v(y) = k$ and $x_0.y_0 = a_0$. Let $|x_0| = 1$, $|y_0| = a_0$. If $j < v(y)$ and $a_0 \mid y_i$, $i = 0,\dots,j$, then $a_0 \mid y_{j+1}$ follows from $0 = a_{j+1} = \sum_{m+n=j+1} x_m \cdot y_n$. Thus $a_0 | a_k$ follows from $a_k = x_{v(x)} \cdot y_{v(y)}$, which is a contradiction.

(b) If $e \in A_0 - N$, then we have $\mathrm{Prm}^{\mathfrak{M}_{10}} (\alpha^k s^e + p)$.

Proof. $\alpha^k s^e + p$ is not decomposable in $M_{10}[s]$ by (a). Let $1 < b$, $b \in M_0$ and $b \,|^{\mathfrak{M}_{10}}\, \alpha^k s^e + p$. Thus $b | s^e$ and $b | p$ and, consequently, $b = p$. Finally, $p | s$ follows from $p | s^e$, which is a contradiction.

Clearly, $a \in M_{10}[s]$ implies $\alpha^{v(a)+1} s^e + p > a$, which finished the proof of (1).

We will prove (2). Let $a \in M_{10}[s]$, $v(a) \geq 2$.

(a) If $a_0 = 0$, then $\neg \mathrm{Prm}^{\mathfrak{M}_{10}}(a)$ follows from $s^e \,|^{\mathfrak{M}_{10}}\, a$ for some $e \in A_0 - N$.

(b) If $|a_0| = 1$, then $\neg \mathrm{Prm}^{\mathfrak{M}_{10}}(a)$ follows by 1.2.1.

(c) If $|a_0| > 1$, and $r(|a_0|, p) \neq 1$, then $\neg \mathrm{Prm}^{\mathfrak{M}_{10}}(a)$.

Proof. $r(|a_0|, p) | s$ follows from $r(|a_0|, p) \in M_0$ by using lemma in 2.1.1. Thus $r(|a_0|, p) \,|^{\mathfrak{M}_{10}}\, a$ follows from (ii) of 1.2.2.

(d) Let $|a_0| > 1$, $r(|a_0|, p) = 1$. Let t be such that $|a_0| = p^t$.

(d1) If $a_0 > 1$, then $r(|a_0|, p) \neq 1$ and $\neg \mathrm{Prm}^{\mathfrak{M}_{10}}(a + 2)$ follows from (c).

(d2) If $a_0 = -2$, then $(a + 2)_0 = 0$ and $\neg \mathrm{Prm}^{\mathfrak{M}_{10}}(a + 2)$ follows from (a).

(d3) If $a_0 = -3$, then $|(a + 2)_0| = 1$ and $\neg \mathrm{Prm}^{\mathfrak{M}_{10}}(a + 2)$ follows from (b).

(d4) If $a_0 < -3$, then $|(a + 2)_0| > 1$. Let $r(|a_0 + 2|, p) = 1$. Then there exists a $\tilde{t}$ with $|a_0 + 2| = p^{\tilde{t}}$. Thus $|a_0| - |a_0 + 2| = 2 = p^{\tilde{t}} \cdot (p^{t-\tilde{t}} - 1)$, which is a contradiction.

Thus $r(|a_0 + 2|,p) \neq 1$ and $\neg \mathrm{Prm}^{\mathfrak{M}_{10}}(a + 2)$ follows from (c).

Consequently, $\neg \mathrm{Prm}_2^{\mathfrak{M}_{10}}(a)$ follows from (a),(b),(c),(d).

Let $a \in M_{10}[s]$, $v(a) \geq 2$. Since $\mathfrak{M}_{10} \models \underline{a} < x \longrightarrow \neg \mathrm{Prm}_2(x)$, the proof is completed.

§ 3. <u>The consistency of Ar with</u> $(\check{\exists} x)\mathrm{Prm}_2(x)$

3.0.0. At first we are going to construct a model $\mathfrak{M}_1$. Let $\beta \in A_1 - A_0$ be prime, $L \in A_0 - N$ and $s = L!$. Put $M' = \{\beta . a_1 + a_0;\ a_1 > 0,\ a_1 \in A_1,\ a_0 \in A_0^*$ and there is an $e \in A_1 - N$ with $s^e \mid a_1\}$,

and

$$M_1 = M' \cup A_0.$$

<u>Lemma</u>. If $a \in M'$, then there is exactly one $a_1 \in A_1$ and $a_0 \in A_0^*$ such that $a = \beta . a_1 + a_0$ and $a_1 > 0$.

Proof is obvious.

<u>Notation</u>. For $a \in M'$, we denote a_0, a_1 the elements of A_1^* such that $a_1 > 0$, $a_0 \in A_0^*$ and $a = \beta . a_1 + a_0$.

<u>Lemma</u>. M_1 is the universe of a substructure of $\mathfrak{A}_1$.

3.0.1. Put $\mathfrak{M}_1 = \mathfrak{A}_1 / M_1$.

<u>Lemma</u>. (0) $\mathfrak{A}_0 \subseteq \mathfrak{M}_1 \subset \mathfrak{A}_1$,

(1) $\mathfrak{M}_1 \models \mathrm{Ar}$,

(2) there is a $c \in M'$ such that $\mathfrak{M}_1 \models \mathrm{Prm}_2(\underline{c})$.

Proof: (0) obvious. (1) can be proved similarly as Theorem 1.1.2. (2): First, we shall prove the following statements:

(a) $a \in M'$ and $n \in N$ imply $n \mid a_1$ and $\frac{a}{n} 1 \notin N$. (Obvious.)

(b) If $a \in M'$, $b \in A_0$, then $b \mid a_1$ and $b \mid a_0$ follows from $b \mid^{\mathfrak{M}_1} a$.

(c) If $a, b \in M'$, $a.b = \beta^2.u + v$ and $v \in A_0^*$, $a_1, b_1 \in A_0$, then $a_1b_0 + b_1a_0 = 0$. (Indeed, we have $\beta.a_1b_1 + a_1b_0 + b_1a_0 = \beta.u$. Thus $\beta \mid a_1b_0 + b_1a_0$ and $a_1b_0 + b_1a_0 = 0$ follows from $a_1.\mid b_0\mid + b_1.\mid a_0\mid < \beta$.)

(d) If $a = \beta^2.u + v$, $a \in M'$, $u, v > 0$ and $u, v \in A_0$, then a is not decomposable in M'. (Let $x, y \in M'$ and $x.y = a$. Hence $v = x_0y_0$ and, consequently $sign(x_0) = sign(y_0)$.

If $x_1, y_1 \in A_0$, then $x_1y_0 + y_1x_0 = 0$ follows from (c). Thus $x_1, y_1 \in A_0$ implies $sign(x_0) \neq sign(y_0)$, a contradiction.

We have $\beta.u = \beta.x_1y_1 + x_1y_0 + y_1x_0$. If $x_1 \notin A_0$ and $sign(x_0) = 1$, then, obviously, $u \notin A_0$, a contradiction. We shall prove that $u \notin A_0$ follows from $x_1 \notin A_0$ and $sign(x_0) = -1$. We have $x_1.\mid y_0\mid < x_1.\beta$, $y_1.\mid x_0\mid < y_1.\beta$. Thus $\beta.(x_1 + y_1) > x_1.\mid y_0\mid + y_1.\mid x_0\mid$, and consequently

$$u > x_1y_1 - (x_1 + y_1) = (x_1.\frac{y_1}{2} - x_1) + (y_1.\frac{x_1}{2} - y_1) >$$

$$> x_1 + y_1 \notin A_0 .$$ ($2\mid y_1, 2\mid x_1$ and $\frac{x_1}{2} > 2$, $\frac{y_1}{2} > 2$ follows from (a).) The statement (d) is proved.

Let $e \in A_0 - N$, $u = \beta^2 s^e + s^e - 1$. We prove $Prm_2^{\mathfrak{M}_1}(u)$. Note that us is not decomposable in M (this follows from (d) and $s^e \in A_0$). If $a > 1$, $a \in A_0$ and $\mathfrak{M}_1 \models a \mid u$, then $a \mid \beta.s^e$ and $a \mid s^e - 1$. β is prime, thus $a \mid s^e$ follows by using (ii) of 2.1.0, a contradiction. We have $Prm^{\mathfrak{M}_1}(u)$. Case $u + 2$ can be proved like the case u. Clearly, $u \in A_0$ and u is the required element c.

3.1.0. Let $\mathfrak{M}_1$, s be as in 3.0.0. We have $\mathfrak{M}_{11}(s) \models$ Ar.

<u>Theorem</u>. $\mathfrak{M}_{11}(s) \models (\check{\exists} x)\mathrm{Prm}_2(x)$.

Proof. (a) Let $a \in M_{11}[s]$, $v(a) = k$, $a_{k-1} = a_{k-2} = \dots = a_1 = 0$, $\mathrm{Prm}^{\mathfrak{M}_1}(a_0)$ and $a_0 \nmid^{\mathfrak{M}_1} a_k$. Then $\mathrm{Prm}^{\mathfrak{M}_{11}}(a)$.

We shall first prove that a is not decomposable in $M_{11}[s]$.

Contrarywise, assume that $a = x.y$ and $x, y \in M_{11}[s]$. Then $x_0.y_0 = a_0$ and $v(x) + v(y) = k$. Let $|x_0| = 1$, $|y_0| = a_0$. Thus $a_0 \mid^{\mathfrak{M}_1^*} y_0$. Let $j < v(y)$ and $a_0 \mid^{\mathfrak{M}_1^*} y_i$, $i = 0,1,\dots,j$. $|y_{j+1}| = |\sum_{m+n=j} x_{m+1}y_n|$ follows from $0 = \sum_{m+n=j+1} x_m y_n$, and consequently $a_0 \mid^{\mathfrak{M}_1^*} y_{j+1}$. Thus $a_0 \mid^{\mathfrak{M}_1^*} y_i$, $i = 0,\dots,v(y)$. We have $a_k = x_{v(x)} \cdot y_{v(y)}$. Consequently, $a_0 \mid^{\mathfrak{M}_1} a_k$, a contradiction.

Let $b \in M_1$, $b > 1$ and $b \mid^{\mathfrak{M}_{11}} a$. Then $b \mid^{\mathfrak{M}_1} a_k$ and $b \mid^{\mathfrak{M}_1} a_0$. Thus $b = a_0$, a contradiction.

(b) Let $e \in A_0 - N$, $p \in M_1 - A_0$ with $\mathrm{Prm}_2^{\mathfrak{M}_1}(p)$ (by using (2) of 3.0.1). $p \nmid^{\mathfrak{M}_1} s^e$ and $p + 2 \nmid^{\mathfrak{M}_1} s^e$ follows from $s^e \in A_0$. Let $c(k) = \alpha^k s^e + p$, $k \in N$ and $k \geq 1$. $\mathrm{Prm}_2^{\mathfrak{M}_{11}}(c(k))$ follows from a. Clearly, if $a \in M_{11}[s]$, then $a < c(v(a) + 1)$, and hence the proof is completed.

References

[1] J.L. BELL and A.B. SLOMSON: Models and ultraproducts, NHPC 1969.

[2] A. MOSKOWSKI: Sentences undecidable in formalized arithmetic, NHPC 1952.

[3] J.R. SHOENFIELD: Mathematic Logic, Addison-Wesley 1967.

Matematický ústav
Karlova universita
Sokolovská 83, 18600 Praha 8
Československo

(Oblatum 6.4. 1976)