# On the additive theory of prime numbers II 

Patrick Cegielski, Denis Richard, Maxim Vsemirnov

## To cite this version:

Patrick Cegielski, Denis Richard, Maxim Vsemirnov. On the additive theory of prime numbers II. 2005, pp.39-47. hal-00096769

HAL Id: hal-00096769

## https://hal.science/hal-00096769

Submitted on 20 Sep 2006

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# On the additive theory of prime numbers II 

Patrick Cegielski $\ddagger$ Denis Richard ${ }^{\S} \&$ Maxim Vsemirnov^

September 20, 2006


#### Abstract

The undecidability of the additive theory of primes (with identity) as well as the theory $\operatorname{Th}\left(\mathbb{N},+, n \mapsto p_{n}\right)$, where $p_{n}$ denotes the $(n+1)$-th prime, are open questions. As a possible approach, we extend the latter theory by adding some extra function. In this direction we show the undecidability of the existential part of the theory $\operatorname{Th}\left(\mathbb{N},+, n \mapsto p_{n}, n \mapsto r_{n}\right)$, where $r_{n}$ is the remainder of $p_{n}$ divided by $n$ in the euclidian division.


## Résumé


#### Abstract

L'indécidabilité de la théorie additive des nombres premiers ainsi que de la théorie $\operatorname{Th}\left(\mathbb{N},+, n \mapsto p_{n}\right)$, où $p_{n}$ désigne le $(n+1)$-ième premier, sont deux questions ouvertes. Nous étendons cette dernière théorie en lui ajoutant une fonction supplémentaire et nous montrons l'indécidabilité de la théorie $\operatorname{Th}\left(\mathbb{N},+, n \mapsto p_{n}, n \mapsto r_{n}\right)$, où $r_{n}$ désigne le reste de $p_{n}$ de la division euclidienne de $p_{n}$ par $n$, et même de sa seule partie existentielle.


Introduction - The additive theory of primes contains longtime open classical conjectures of Number Theory, as famous Goldbach's binary conjecture or Twin PRIMES conjecture, and so on. Some authors provided [BJW,BM,LM] conditional proofs (through Schinzel's Hypothesis [SS]) of the undecidability of the additive theory of primes $\operatorname{Th}(\mathbb{N},+, \mathbb{P})$, where $\mathbb{P}$ is the set of all primes. Weakening the problem by strengthenning this theory, we introduced [CRV] the theory $\operatorname{Th}\left(\mathbb{N},+, n \mapsto p_{n}\right)$, where $p_{n}$ is the $(n+1)$-th prime, and posed the problem of its (un)decidability. As usual for a language containing a function symbol, we suppose it contains identity. Note that $\mathbb{P}$ is existentially definable within $\left\langle\mathbb{N}, n \mapsto p_{n}\right\rangle$, hence $\operatorname{Th}(\mathbb{N},+, \mathbb{P})$ is a subtheory of $\operatorname{Th}\left(\mathbb{N},+, n \mapsto p_{n}\right)$. At the moment, the undecidability of the latter theory is still an open question, and our approach in [CRV] was to consider several approximations of the function $n \mapsto p_{n}$ as, for instance, $n\lfloor\log n\rfloor$ and on this way we showed the undecidability of theories $\operatorname{Th}(\mathbb{N},+, n f(n))$ for a family of functions $f$ including $\lfloor\log \rfloor$ mentioned above. Another approach consists of extending the language $\left\{+, n \mapsto p_{n}\right\}$ to $\left\{+, n \mapsto p_{n}, n \mapsto r_{n}\right\}$, where $r_{n}$ is the remainder of $p_{n}$ divided by $n$. The main result of this paper is the following:

Theorem 1 Multiplication is existentially $\left\langle\mathbb{N},+, \mathrm{n} \mapsto \mathrm{p}_{\mathrm{n}}, \mathrm{n} \mapsto \mathrm{r}_{\mathrm{n}}\right\rangle$-definable at first-order.
This leads to the following (without use of conjectures) result:

[^0]Corollary $1 \quad \operatorname{Th}_{\exists}\left(\mathbb{N},+, \mathrm{n} \mapsto \mathrm{p}_{\mathrm{n}}, \mathrm{n} \mapsto \mathrm{r}_{\mathrm{n}}\right)$ is undecidable.
Remark Actually all positive integer constants are existentially $\{+, \mathbb{P}\}$-definable in the following manner:

$$
\begin{array}{ll}
x=0 & \Leftrightarrow x+x=x \\
x=1 & \Leftrightarrow \exists y(y=x+x \wedge y \in \mathbb{P}) \\
x=2 & \Leftrightarrow \exists y(y=1 \wedge x=y+y) \\
& \vdots \\
x=n+1 & \Leftrightarrow \exists y \exists z(y=n \wedge z=1 \wedge x=y+z)
\end{array}
$$

As we mentioned above, $\mathbb{P}$ is existentially definable within the language $\left\{+, n \mapsto p_{n}\right\}$, hence all positive integer constants are also existentially $\left\{+, n \mapsto p_{n}\right\}$-definable. Note, that $n\left\lfloor\frac{p_{n}}{n}\right\rfloor=p_{n}-r_{n}$. We intend to define (section 2, see Lemma 3) $\left\lfloor\frac{p_{n}}{n}\right\rfloor$ from + and $n\left\lfloor\frac{p_{n}}{n}\right\rfloor$. Then the strategy will be to define multiplication through the function $n \mapsto c n^{2}$ (where $c$ is a fixed constant), which is to be proved $\left\{+,\left\lfloor\frac{p_{n}}{n}\right\rfloor, n\left\lfloor\frac{p_{n}}{n}\right\rfloor\right\}$-definable. Consequently, multiplication will be existentially $\left\{+, n \mapsto p_{n}, n \mapsto r_{n}\right\}$-definable at first-order.

Remark. In the previous paper [CRV] we consider continuous real strictly increasing functions and their inverses. Since we work with integer parts we have to introduce pseudoinverses of discrete functions. For such a discrete unbounded function $f$ from $\mathbb{N}$ into $\mathbb{N}$, we define its pseudo-inverse $f^{-1}$ from $\mathbb{N}$ into $\mathbb{N}$ by $f^{-1}(n)=\mu m[f(m+1)>n]$, where $\mu$ means "the smallest ... such that". Due to the unboundness of $f$ such an $f^{-1}$ is correctly defined.

## 1) Some preliminary results in Number Theory

Contrarily to what happens with log, the behavior of $\left\lfloor\frac{p_{n}}{n}\right\rfloor$ is a priori irregular but we shall prove it is not too much chaotic. Namely, we prove:

Proposition 1 Let us denote the mapping $n \mapsto\left\lfloor\frac{p_{n}}{n}\right\rfloor$ by $f$.

1) For $m>n$, we have $f(m)-f(n) \geq-1$;
2) For $n \geq 11$, we have $f^{-1}(n+1)-f^{-1}(n)>n$.

Proof 1) We use the following estimates for $p_{n}$ ([RP], p. 249):
$p_{m} \geq m \log m+m \log \log m-1.0072629 m$ for $m \geq 2$;
$p_{m} \leq m \log m+m \log \log m-0.9385 m$ for $m \geq 7022$.
For $m>n \geq 7022$, we have $f(m)-f(n)=\left\lfloor\frac{p_{m}}{m}\right\rfloor-\left\lfloor\frac{p_{n}}{n}\right\rfloor$
$\geq \frac{p_{m}}{m}-\frac{p_{n}}{n}-1 \geq \log \left(\frac{m}{n}\right)-\log \left(\frac{\log m}{\log n}\right)-0.9385+1.0072629-1$.
Hence $f(m)-f(n) \geq-1$ because the sum of the two first terms is positive as is the sum of terms three and four.
If $n<7022$, one may check the desired inequality by a direct computation.
2) Let $m$ be $f^{-1}(n)$. By the very definition of $f^{-1}$, the equality $m=f^{-1}(n)$ is equivalent to the conjunction of the two following conditions:

$$
\left\{\begin{array}{l}
\left\lfloor\frac{p_{m+1}}{m+1}\right\rfloor \geq n+1  \tag{2}\\
\forall k \leq m\left\lfloor\frac{p_{k}}{k}\right\rfloor \leq n
\end{array}\right.
$$

For $k \leq 7022$, the maximum of $\frac{p_{k}}{k}$ is attained for $k=7012$ and equal to $\frac{p_{7012}}{7012}<10.102824<$ 11. Consequently, we see that $m=f^{-1}(n) \geq f^{-1}(11) \geq 7022$ and this is the reason why in the hypothesis of Proposition 1, item 2) we assume $n \geq 11$.
To prove the inequality, it is sufficient to prove that for $k=m+n$ we have $\left\lfloor\frac{p_{k}}{k}\right\rfloor \leq n+1$, or in other words,

$$
\begin{equation*}
\frac{p_{k}}{k}<n+2 \tag{3}
\end{equation*}
$$

Note that for $m \geq 7022$, we have by (2):

$$
n+1 \leq\left\lfloor\frac{p_{m+1}}{m+1}\right\rfloor+1 \leq \frac{p_{m+1}}{m+1}+1 \leq \log (m+1)+\log \log (m+1)-0.07<m
$$

Consequently it is sufficient - and actually more convenient - to prove a somehow stronger result, namely the same inequality (3) but for $m \geq 7022$ and $m+1 \leq k \leq 2 m$.
From the second estimate of (1) we have, since $k \geq m \geq 7022$, the following inequalities:

$$
\begin{aligned}
\frac{p_{k}}{k} & <\log k+\log \log k-0.9385 \\
& \leq \log 2 m+\log \log 2 m-0.9385 \\
& =\log m+\log \log m+\log 2+\log \left(1+\frac{\log 2}{\log m}\right)-0.9385
\end{aligned}
$$

using the first estimate of (1) and $\frac{\log 2}{\log m} \leq \frac{\log 2}{\log 7022}$, we have:

$$
\log m+\log \log m-1.0072629 \leq \frac{p_{m}}{m}
$$

consequently:

$$
\frac{p_{k}}{k} \leq \frac{p_{m}}{m}+0.07+\log 2+\log \left(1+\frac{\log 2}{\log 7022}\right) \leq \frac{p_{m}}{m}+1
$$

by an easy computation and finally, due to (2), we obtain $\frac{p_{k}}{k}<n+2$.
Item 1) of previous proposition emphasizes on the fact that $f: n \mapsto\left\lfloor\frac{p_{n}}{n}\right\rfloor$ is "almost" increasing and item 2) shows that the difference $f^{-1}(n+1)-f^{-1}(n)$ is big enough with respect to $n$. This suggests to introduce a new class of functions, containing $f$, for which we prove that the existential part of the theory $\operatorname{Th}(\mathbb{N},+, n \mapsto n f(n))$ is undecidable.

## 2) The class $C\left(k, d, n_{0}\right)$ and some its properties

2.1) The class $C\left(k, d, n_{0}\right)$

Let $k \geq 0$ be a fixed nonnegative integer. We shall say $f$ is $k$-almost increasing if and only if

$$
\begin{equation*}
\forall y \geq x[f(y)-f(x) \geq-k] \tag{4}
\end{equation*}
$$

In this sense 0-almost increasing means increasing (not necessarily strictly) and $n \mapsto\left\lfloor\frac{p_{n}}{n}\right\rfloor$ is 1 -almost increasing (due to Proposition 1).

Still looking at $n \mapsto\left\lfloor\frac{p_{n}}{n}\right\rfloor$, we intend to consider functions whose pseudo-inverse is defined and asymptotically increases quickly enough with respect to its argument. Let us say that $f^{-1}$ has at least ( $1 / d$ )-linear difference, if

$$
\begin{equation*}
\exists n_{0} \in \mathbb{N} \forall n \geq n_{0}\left[f^{-1}(n+1)-f^{-1}(n)>\frac{n}{d}\right] \tag{5}
\end{equation*}
$$

In fact, for $\left\lfloor\frac{p_{n}}{n}\right\rfloor$, the constant $d$ is 1 and $n_{0}=11$, but results and proofs hold for an arbitrary (fixed) $d$.

Now let us definite the class $C\left(k, d, n_{0}\right)$ as the set of functions from $\mathbb{N}$ into $\mathbb{N}$ satisfying conditions (4) of being $k$-almost increasing and (5) of having its pseudo-inverse with an at least $(1 / d)$-linear difference.
In order to prove FUNDAMENTAL LEMMA of section 3 , whose Theorem 1 is a corollary, we show some properties of the class $C\left(k, d, n_{0}\right)$. Firstly, in section 2.2 we present in three lemmas these properties and comment them. Afterwards, in section 2.3, we prove them.

## 2.2) Properties of $C\left(k, d, n_{0}\right)$

Lemma 1 For any function $f \in C\left(k, d, n_{0}\right)$ the following items hold:
(i) For any $n \geq n_{0}$, we have $f^{-1}(n+d)-f^{-1}(n)>n$;
(ii) For any $n \geq n_{0}+1$, the set $\{x \in \mathbb{N} \mid f(x)=n\}$ is nonempty;
(iii) For any $n \geq n_{0}+1$, the equality $f(x)=n$ implies

$$
x>\frac{1}{2 d}\left[(n-1)(n-2)-n_{0}\left(n_{0}-1\right)\right] .
$$

Lemma 2 If $f \in C\left(k, d, n_{0}\right)$ and $f(x)=n \geq n_{0}$, then for any $c$ such that $1 \leq c \leq n$, we have:

$$
\begin{equation*}
-k \leq f(x+c)-f(x) \leq k+d \tag{6}
\end{equation*}
$$

Lemma 3 For any $f \in C\left(k, d, n_{0}\right)$, let $x_{0}=f^{-1}\left(2+4 d+n_{0}^{2}+k\right)$.
Consider $\tilde{f}:\left[x_{0}+1,+\infty[\cap \mathbb{N} \longrightarrow \mathbb{N}\right.$ with $\tilde{f}(x)=f(x)$. Then $\tilde{f}$ is existentially definable at first-order within $\langle\mathbb{N},+, 1, x \mapsto x f(x)\rangle$.

Remarks 1) Item (i) of Lemma 11 provides a linear lower bound of values of $f^{-1}$ when difference of arguments is the parameter $d$ of the considered class.
Item (ii) of the same lemma insure that $f$ is asymptotically onto, and item (iii) gives a quadradic lower bound for solutions of the equation $f(x)=n$, that we need in section 3 .
2) Actually, as the reader will see within the proof, Lemma 1 does not use condition (4) of being $k$-almost increasing.
3) Lemma 2 provides asymptotical bounds for the difference of two values of $f$ with arguments taken in a short interval with respect to the values of these arguments. Refering to the previous Lemma 11 we see that $n$ is at most $\sqrt{2 d x+n_{0}^{2}}+2$.
4) Lemma 3 generalizes the situation of the main result of the previous paper [CRV] of the same authors when $\lfloor\log n\rfloor$ was "extracted", i.e. defined, from + and $n\lfloor\log n\rfloor$.

## 2.3) Proofs of the three Lemmas

Proof of Lemma 1 (i) By condition (5):

$$
\begin{aligned}
f^{-1}(n+d)-f^{-1}(n)= & {\left[f f^{-1}(n+d)-f^{-1}(n+d-1)\right] } \\
& +\left[f^{-1}(n+d-1)-f^{-1}(n+d-2)\right] \\
& +\ldots \\
& +\left[f^{-1}(n+1)-f^{-1}(n)\right] \\
> & \frac{n+d-1}{d}+\frac{n+d-2}{d}+\ldots+\frac{n}{d} \\
> & n .4
\end{aligned}
$$

(ii) If there was no $x$ such that $f(x)=n$, we would have $f^{-1}(n)=f^{-1}(n-1)$. But $f^{-1}(n)>f^{-1}(n-1)$ according to condition (5).
(iii) By definition of $f^{-1)}$, we have: $x>f^{-1}(n-1)$.

As in (i), we have:

$$
\begin{aligned}
f^{-1}(n-1)-f^{-1}\left(n_{0}\right)= & {\left[f^{-1}(n-1)-f^{-1}(n-2)\right] } \\
& +\ldots \\
& +\left[f^{-1}\left(n_{0}+1\right)-f^{-1}\left(n_{0}\right)\right] \\
> & \frac{n-2}{d}+\frac{n_{0}}{d}+\ldots+\frac{n}{d} \\
= & \frac{(n-2)(n-1)-n_{0}\left(n_{0}+1\right)}{2 d} .
\end{aligned}
$$

and the result.
Proof of Lemma 2 The left-hand side of the inequality is an immediate consequence of the very definition of a $k$-almost increasing function. For proving the right-hand side, note that, using $k$-almost increasing property of $f$ together with $f(x)=n$, we obtain:

$$
\max _{y \leq x} f(y) \leq f(x)+k=n+k
$$

so that $f^{-1}(n+k) \geq x$, by the definition of $f^{-1}$. By previous Lemma 11, item (i) and the latter inequality, we have:

$$
f^{-1}(n+k+d)>f^{-1}(n+k)+n+k \geq x+n+k \geq x+n \geq x+c
$$

since $1 \leq c \leq n$. Using again the definition of $f^{-1}$, we see that $f(x+c) \leq n+k+d=$ $f(x)+k+d$ and we are done.

Proof of Lemma 3 To define $\tilde{f}$ within the structure $\langle\mathbb{N},+, x \mapsto x f(x)\rangle$ we shall make use of the inequality:

$$
0 \leq f(x)<x
$$

together with the remainder of $f(x)$ modulo $x+1$, which we must define in the considered structure.

Fact 1.- $f(x)<x$.
By the definition of $f^{-1}$, we have $f\left(x_{0}+1\right)>k+2+4 d+n_{0}^{2}$ and by the $k$-almost increasing property we deduce, for $x \geq x_{0}+1$,

$$
\begin{equation*}
n=f(x) \geq f\left(x_{0}+1\right)-k>2+4 d+n_{0}^{2} \tag{7}
\end{equation*}
$$

Hence $\frac{n-2}{2 d}>2$.
From (7), we obtain $n>n_{0}+1$ so that by Lemma 1. item (iii), we have:

$$
x>\frac{1}{2 d}\left[(n-1)(n-2)-n_{0}\left(n_{0}-1\right)\right],
$$

hence:

$$
x>2(n-1)-\frac{n_{0}\left(n_{0}-1\right)}{2 d}>2(n-1)-n_{0}^{2}=n+\left(n-2-n_{0}^{2}\right)>n=f(x)
$$

Fact2.- We have:

$$
\begin{equation*}
f(x) \equiv(x+1) f(x+1)_{5}-x f(x)(\bmod x+1) \tag{8}
\end{equation*}
$$

It is sufficient to note that $(x+1) f(x+1)-x f(x)=f(x)+(x+1)[f(x+1)-f(x)]$.
We are still unable to define general congruences, fortunately here the difference $|f(x+1)-f(x)|$ is bounded, namely,

$$
\begin{equation*}
|f(x+1)-f(x)| \leq k+d \tag{9}
\end{equation*}
$$

due to Lemme 2, with $c=1$. This suggests to introduce the notion of a restricted congruence, namely, for $a, b, m$ in $\mathbb{N}$ and some fixed integer $c$, we define $a \equiv_{c} b(\bmod m)$ by:

$$
\bigvee_{h=0}^{c}\{[a=b+\underbrace{m+\cdots+m}_{\mathrm{h} \text { times }}\urcorner \vee[b=a+\underbrace{m+\cdots+m}_{\mathrm{h} \text { times }}]\} .
$$

Obviously, the first-order latter formula is expressible within the structure $\langle\mathbb{N},+\rangle$, since $c$ is fixed. The congruence (8) and inequality (9) provide together the following restricted congruence:

$$
f(x) \equiv_{k+d}(x+1) f(x+1)-x f(x)(\bmod x+1),
$$

which is a definition of $f(x)$ within $\langle\mathbb{N},+, 1, x \mapsto x f(x)\rangle$ since $1 \leq f(x)<x$. Finally, we provide explicitely an existential first-order definition of $f$, namely:

$$
\begin{gathered}
{\left[x>x_{0} \wedge y=f(x)\right] \leftrightarrow} \\
\{x>x_{0} \wedge y \leq x \wedge \bigvee_{h=0}^{k+d}[(y+x f(x)=(x+1) f(x+1)+\underbrace{(x+1)+\cdots+(x+1)}_{\text {h times }}) \\
\vee((x+1) f(x+1)=y+x f(x)+\underbrace{(x+1)+\cdots+(x+1)}_{\text {h times }})]\} .
\end{gathered}
$$

## 3) Fundamental Lemma and the proof of the Main Theorem

In order to prove the undecidability of $\operatorname{Th}\left(\mathbb{N}, n \mapsto p_{n}, n \mapsto r_{n}\right)$, we prove a more general result, namely:

Lemma 4 (Fundamental Lemma) For any $f \in C\left(k, d, n_{0}\right)$ [see §2], multiplication is existentially $\{+, 1, x \mapsto x f(x)\}$-definable at first-order.

As shown by Y. Matiyasevich, the existential true theory of numbers is exactly the set of arithmetical relations, which are definable by diophantine equations. Therefore the negative solution of the 10 -th Hilbert's problem [MY] implies the following corollary.

Corollary 2 The existential theory $\mathrm{Th}_{\exists}(\mathbb{N},+, 1, x \mapsto x f(x))$ is undecidable.
Proof of Lemma 6 It suffices to show that for some constants $c$ and $n_{1}$ the function $n \mapsto c n^{2}$ from $\left[n_{1},+\infty[\cap \mathbb{N}\right.$ into $\mathbb{N}$ is $\{+, 1, x \mapsto x f(x)\}$-definable. More precisely, we shall take $c=5 d$ and $n_{1}=2+5 d+n_{0}^{2}$. Consider $n \geq n_{1}$. Since $n_{1}>n_{0}+1$, we can apply Lemma 11, item (ii), proving there exists $x$ such that $f(x)=5 d n$. Let $x_{0}$ be the same as in Lemma 3, namely $x_{0}=f^{-1}\left(2+4 d+n_{0}^{2}+k\right)$. Let us show $x>x_{0}$. Otherwise $x \leq x_{0}$, so that by the $k$-almost increasing property $f(x) \leq f\left(x_{0}\right)-k$, implying, by the definitions of $f^{-1}$ and $x_{0}$,

$$
f(x) \leq 2+4 d+n_{0}^{2}+k-k_{6}<n_{1}<5 d n_{1} \leq 5 d n=f(x),
$$

which is impossible.
Note that $5 d n$ is $\{+\}$-definable as the sum of $5 d$ terms equal to $n$ ( $d$ is a fixed constant). Now thanks to Lemma 3, an $x$ such that $f(x)=5 d n$ is $\{+, 1, x \mapsto x f(x)\}$-definable.
On the other hand:
$(x+n) f(x+n)-x f(x)=(x+n)[f(x+n)-f(x)]+n f(x)=(x+n)[f(x+n)-f(x)]+5 d n^{2}$.
By Lemma 2 applied to $c=n$, we have $|f(x+n)-f(x)| \leq k+d$, so that:

$$
\begin{equation*}
5 d n^{2} \equiv_{k+d}(x+n) f(x+n)-x f(x)(\bmod x+n) . \tag{10}
\end{equation*}
$$

According to Lemma 1 and item (iii) since $f(x)=5 d n$ and $5 d n>n_{1}>n_{0}+1$ the inequalities $n \geq n_{1}>n_{0}^{2}$ and:

$$
\begin{align*}
x+n & >\frac{(5 d n-1)(5 d n-2)}{2 d}-\frac{n_{0}\left(n_{0}-1\right)}{2 d}+n \\
& >\frac{25 d^{2} n^{2}-15 n d}{2 d}>5 d n^{2} \tag{11}
\end{align*}
$$

hold.
Using (10) and (11), a similar argument as in Lemma 3 shows that the function $n \mapsto$ $5 d n^{2}=c n^{2}$ with domain $\left[n_{1},+\infty[\cap \mathbb{N}\right.$ is existentially $\{+, 1, x \mapsto x f(x)\}$-definable. By a routine argument, multiplication is clearly existentially $\{+, 1, x \mapsto x f(x)\}$-definable.

Proof of the Main-Theorem We remind the reader that 1 was existentially $\{+, \mathbb{P}\}$ and $\left\{+, n \mapsto p_{n}\right\}$-defined in the introduction.
We also noted that $n\left\lfloor\frac{p_{n}}{n}\right\rfloor=p_{n}-r_{n}$ and $n \mapsto n\left\lfloor\frac{p_{n}}{n}\right\rfloor$ belongs to $C(1,1,11)$, the latter due to Proposition 11, $\S 1$. Then Fundamental Lemma can be applied and multiplication is existentially $\left\{+, n \mapsto p_{n}, n \mapsto r_{n}\right\}$-definable.

Conclusion: Our main result is absolute in the sense that does not depend on any conjecture. In order to shed more light on the considered theories $\mathrm{Th}_{\ni}(\mathbb{N},+, \mathbb{P})$ and $\mathrm{Th}_{\exists}\left(\mathbb{N}, n \mapsto p_{n}, n \mapsto r_{n}\right)$, we recall a conditional result of A . Woods. Let us recall that Dickson's conjecture [DL] claims that if $a_{1}, a_{2}, \ldots a_{n}, b_{1}, b_{2}, \ldots b_{n}$ are integers with all $a_{i}>0$ and

$$
\forall y \neq 1 \exists x\left[y \nmid \prod_{1 \leq i \leq n}\left(a_{i} x+b_{i}\right)\right]
$$

then there exist infinitely many $x$ such that $a_{i} x+b_{i}$ are primes for all $i$. Let us call $D C$ this conjecture, then A. Woods proved [WA]:
If $D C$ is true then the existential theory $\mathrm{Th}_{\exists}(\mathbb{N},+, \mathbb{P})$ is decidable.
Now, the question is to know whether there is a gap between $\operatorname{Th}_{\exists}\left(\mathbb{N},+, n \mapsto p_{n}, n \mapsto r_{n}\right)$ or whether they are exactly the same. In the case of equality between these two theories, $D C$ is false (and hence Schinzel's hypothesis on primes, whose $D C$ is the linear case, is also false).

Open problem: Is $\mathrm{Th}_{\exists}(\mathbb{N},+, \mathbb{P})$ equal to $\mathrm{Th}_{\exists}\left(\mathbb{N},+, n \mapsto p_{n}, n \mapsto r_{n}\right)$ ?

## References

[BJW] P.T. Bateman, C.G. Jockusch and A.R. Woods, Decidability and Undecidability of theories with a predicate for the prime, Journal of Symbolic Logic, vol. 58, 1993, pp.672-687.
[BM] Maurice Boffa, More on an undecidability result of Bateman, Jockusch and Woods, Journal of Symbolic Logic, vol. 63, 1998, p.50.
[CRV] Patrick Cegielski, Denis Richard \& Maxim Vsemirnov, On the additive Theory of Prime Numbers I, Proceedings of CSIT'2003 (Computer Science and Information Technologies), September 22-26, 2003, Yerevan, Armenia, 459 p., pp. 80-85.
[DL] L.E. Dickson, A new extension of Dirichlet's theorem on prime numbers, Messenger of Mathematics, vol. 33 (1903-04), pp. 155-161.
[LM] T. Lavendhomme \& A. Maes, Note on the undecidability of $\left\langle\omega,+, P_{m, r}\right\rangle$, Definability in arithmetics and computability, 61-68. Cahier du Centre de logique, Belgium, 11 (2000).
[MY] Yuri Matiyasevich, Hilbert's tenth Problem, The MIT Press, Foundations of computing, 1993, XXII+262p.
[RP] Paul Ribenboim, The new book of Prime records, Springer, 1996, XIV+541p.
[SS] A. Schinzel \& W. Sierpieńsky, Sur certaines hypothses concernant les nombres premiers, Acta Arithmetica, vol. 4, 1958, 185-208 and 5, 1959, 259.
[WA] Alan Woods, Some problems in logic and number theory, and their connection, Ph.D. thesis, University of Manchester, Manchester, 1981.


[^0]:    ${ }^{\ddagger}$ LACL, UMR-FRE 2673, Université Paris 12, IUT Route Forestière Hurtault F-77300 Fontainebleau, - Email: cegielski@univ-paris12.fr
    ${ }^{\text {§ }}$ LLAIC1 Université d'Auvergne, IUT Informatique, B.P. 86, F-63172 Aubière Cedex - Email: richard@iut.u-clermont1.fr
    ${ }^{\text {TS Steklov Institute of Mathematics (POMI), } 27 \text { Fontanka St Petersburg, 191011, Russia }}$

    - Email: vsemir@pdmi.ras.ru

