FILOMAT (Niš) 9:3 (1995), 473–481
Algebra, Logic & Discrete Mathematics
Niš, April 14–16, 1995.

INVITED LECTURE

SUBSYSTEMS OF PEANO ARITHMETIC AND CLASSICAL RESULTS OF NUMBER THEORY

C. Dimitracopoulos

ABSTRACT. We discuss problems and results concerning subsystems of first-order Peano Arithmetic, especially concerning the provability of basic theorems of elementary number theory and combinatorics.

Let LA denote the usual first-order language of arithmetic and PA denote Peano's axioms expressed in LA. Subsystems of PA are obtained by rextricting the induction schema or replacing it by a restriction of some other schema.

First we recall the definition of the "arithmetic hierarchy" of formulae of LA.

Definition 1. Let φ be a formula of LA and $n \geq 1$. We say that
(a) φ is Σ_0 or Π_0 or bounded if φ involves bounded quantifiers only, i.e. quantifiers of the form $\forall x \leq y$, $\exists x \leq y$, $\forall x < y$, $\exists x < y$.
(b) φ is Σ_n if φ is of the form $\vec{\exists}\, \vec{\forall} \dots \theta$, where θ is bounded and there exist n alternations of blocks of similar quantifiers in front of θ.
(c) φ is Π_n if $\neg\varphi$ is logically equivalent to a Σ_n formula.

Now we proceed to the precise definition of the subsystems that were first studied.

Definition 2. For $n \geq 0$,
(a) $I\Sigma_n$ denotes PA with induction only for Σ_n formulae with parameters.
(b) $B\Sigma_n$ denotes $I\Sigma_0$ plus the collection schema for Σ_n formulas only, i.e. the schema

$$\forall x < z \exists y \varphi(x,y) \to \exists t \forall x < z \exists y < t \varphi(x,y),$$

where φ is any Σ_n formula with parameters.
(c) $L\Sigma_n$ denotes PA with the induction schema replaced by the least number

schema only for Σ_n formulae with parameters.
$I\Pi_n$, $B\Pi_n$, $L\Pi_n$ are defined similarly.

Remark 1. Strictly speaking, the subsystems defined above include a finite number of axioms expressing commutativity of + and ., associativity of + and ., etc.; these must be added to the usual axioms, because the amount of induction available in some of these systems is not sufficient to prove them.

Relations among the systems we have defined were proved by Paris & Kirby (see [14]) and are summarized as follows.

Theorem 1. *For all $n \geq 0$:*

$$\begin{tikzcd}
I\Sigma_{n+1} \arrow[d, Rightarrow] & & & \\
B\Sigma_{n+1} \arrow[d, Rightarrow] \arrow[r, Leftrightarrow] & B\Pi_n & & \\
I\Sigma_n \arrow[r, Leftrightarrow] & I\Pi_n \arrow[r, Leftrightarrow] & L\Sigma_n \arrow[r, Leftrightarrow] & L\Pi_n .
\end{tikzcd}$$

Furthermore, the converses of the vertical arrows do not hold.

In view of this theorem, the following question was asked in the 1970's:

Main Problem. *What is the weakest subsystem of PA that can serve as a basis for elementary number theory and combinatorics?*

It is not difficult to see that $I\Sigma_1$ is strong enough to serve as a basis; indeed, one can formalize usual proofs so that only induction for Σ_1 formulae is needed. But what happens with the strictly weaker systems $B\Sigma_1$ and $I\Sigma_0$? At this point we need to mention the following result, proved by Paris (see [12]) and, independently, H. Friedman.

Theorem 2. *For $n \geq 0$ and θ a Π_{n+2} sentence: $B\Sigma_{n+1} \vdash \theta \Rightarrow I\Sigma_n \vdash \theta$.*

By the previous theorem and the fact that all basic results of elementary number theory and combinatorics are formalized by Π_2 sentences, studying $I\Sigma_0$ is the same as studying $B\Sigma_1$, as far as our main problem is concerned. Unfortunately, $I\Sigma_0$ seems very weak, since the usual method of coding cannot work in it. To test its strength, the following problems were posed and still remain open:

Problem 1 (Paris). *Does $I\Sigma_0$ prove the MRDP theorem?*

By MRDP theorem we mean the following result of Matijasevič-Robinson-Davis-Putnam (see [10]), which was crucial for the negative solution of Hilbert's 10th problem:

MRDP Theorem. *For every Σ_1 formula $\varphi(\vec{x})$ we can effectively find a polynomial $p \in Z[\vec{x}, \vec{y}]$ such that*

$$N \models \forall\vec{x}[\varphi(\vec{x}) \leftrightarrow \exists\vec{y}(p = 0)],$$

where N denotes the standard model of PA.

Remark 2. Strictly speaking, $p = 0$ stands for $p^+ = p^-$, where $p = p^+ - p^-$ and $p^+, p^- \in N[\vec{x}, \vec{y}]$.

Since the MRDP theorem cannot be expressed as a set of sentences of LA, what is meant in problem 1 is: Can we replace $N \models$ by $I\Sigma_0 \vdash$ in the MRDP theorem?

Problem 2 (Wilkie). *Does $I\Sigma_0$ prove that the set of primes is unbounded?*

Problem 3 (Macintyre). *Does $I\Sigma_0$ prove $PHP\Sigma_0$?*

By $PHP\Sigma_0$ we denote the following schema, which formalizes the pigeonhole principle for Σ_0 maps:

$$\forall x \leq z \exists y < z\varphi(x, y) \rightarrow \exists x_1, x_2 \leq z \exists y < z(x_1 \neq x_2 \wedge \varphi(x_1, y) \wedge \varphi(x_2, y)),$$

where φ is any Σ_0 formula with parameters.

It is widely believed that the answer to all these problems is "no". Concerning Problem 1, this feeling is especially strong, in view of the following observation of A. Wilkie (see [19]):

If $I\Sigma_0$ proves the MRDP theorem, then $NP = co - NP$.

Given the difficulty of working with $I\Sigma_0$, it seemed worthwhile to consider systems strictly between $I\Sigma_0$ and $I\Sigma_1$. Such a system is $I\Sigma_0 + exp$, where exp denotes the axiom $\forall x, y \exists z(z = x^y)$. Here $z = x^y$ is a bounded formula defining the graph of the exponential function in the standard model; the existence of such a formula was first shown by J. Bennett (see [1]). $I\Sigma_0 + exp$ is strictly stronger than $I\Sigma_0$, since the latter can capture functions of polynomial growth only, by the following result of R. Parikh (see [11]).

Theorem 3. *If $I\Sigma_0 \vdash \forall x \exists y \varphi(x, y)$, where φ is Σ_0, then there exists $k \in N$ such that $I\Sigma_0 \vdash \forall x \exists y < x^k + k\ \varphi(x, y)$.*

It is also known that $I\Sigma_0 + exp$ is strictly weaker than $I\Sigma_1$; this holds since the former cannot prove $B\Sigma_1$, essentially by the proof that $I\Sigma_0$ cannot prove $B\Sigma_1$ (see [14]). However, $I\Sigma_0 + exp$ seems to be as strong as $I\Sigma_1$, as far as our main problem is concerned; the idea is that existential quantifiers, unbounded at first sight, are essentially bounded, as long as large numbers exist. For example, it is known that the answer to Problems 1 – 3 is "yes" if we replace $I\Sigma_0$ by $I\Sigma_0 + exp$, i.e. the following hold:

Theorem 4. *$I\Sigma_0 + exp$ proves the MRDP theorem.*

Theorem 5. *$I\Sigma_0 + exp$ proves $PHP\Sigma_0$.*

Theorem 6. *$I\Sigma_0 + exp$ proves that the set of primes is unbounded.*

The first of these results was proved by H. Gaifman and, independently, the author (see [6]) and the second one by the author and J. Paris (see [5]); the proofs of both are based on the fact that inside any $M \models I\Sigma_0 + exp$ one can code finite (in the sense of M), Σ_0 definable sequences of elements of M. Theorem 6 is proved by a straightforward formalization of the usual proof of Euclid's theorem.

To strengthen the belief that $I\Sigma_0 + exp$ is very strong, Ch. Cornaros and the author obtained (see [4])

Theorem 7. *$I\Sigma_0 + exp$ proves (a version of) the prime number theorem.*

The proof of this result is a modification of Selberg's proof, the two main differences being that

(a) an approximate logarithm function (previously introduced by A. Woods in [20]) is used instead of $log_e x$ and

(b) arguments involving limits have been replaced by inductive ones.

Attempts to solve Problems 2 and 3 led to the study of other systems strictly between $I\Sigma_0$ and $I\Sigma_1$. In connection with Problem 2, A. Woods showed

Theorem 8. *$I\Sigma_0 + PHP\Sigma_0$ proves Sylvester's theorem, i.e. that for any $1 \leq x \leq y$ one of $y+1, ..., y+x$ has a prime divisor $p > x$.*

Let us discuss briefly the idea of his proof. In the usual proof, by considering the largest powers of primes in the prime power decompositions of the numbers $1, \dots, x, y+1, \dots, y+x$, Sylvester showed that if no prime divisor of $y+1, \dots, y+x$ exceeds x then for any function $\xi(x) \geq \pi(x)$ ($=$ number of primes $\leq x$)

$$x!y! \geq (x+y-\xi(x))! \quad (\dagger).$$

But for sufficiently large x and a suitable choice of $\xi(x)$ (†) fails and so the result follows. Woods considered the logarithmic version of (†), using the approximate logarithm function referred to above. Then he "unravelled" (†) to obtain the underlying *comparison map*, the existence of which contradicts $PHP\Sigma_0$ (the "unravelling" was necessary, since it is not known how to define partial sums by a Σ_0 formula in $I\Sigma_0 + PHP\Sigma_0$).

Clearly, we obtain as corollaries of the previous theorem:

(a) the answer to Problem 2 is "yes" if $I\Sigma_0$ is replaced by $I\Sigma_0 + PHP\Sigma_0$

(b) if the answer to Problem 3 is "yes", then the answer to Problem 2 is "yes".

Note that $I\Sigma_0 + PHP\Sigma_0$ is strictly weaker than $I\Sigma_0 + exp$. To see this, let M be a nonstandard model of PA, $a \in M - N$ and K be the substructure of M with universe $\{x \in M : M \models x < a^n \text{ for some } n \in N\}$. Then $K \models I\Sigma_0 + PHP\Sigma_0$ (since $PHP\Sigma_0$ is Π_1 axiomatizable), but clearly $K \not\models exp$.

Another system studied by A. Woods is $I\mathcal{E}^2_*$, which is defined as follows:

Definition 3. Let $\mathcal{E}^2$ be the smallest class of (primitive recursive) functions containing $+$, $\cdot$, all constant functions and closed under substitution and bounded recursion – this class was defined by A. Grzegorczyk (see [7]). $I\mathcal{E}^2_*$ is obtained from $I\Sigma_0$ if we

(a) add a new function symbol to LA, for each $f \in \mathcal{E}^2$,
(b) allow induction for $\mathcal{E}^2_*$ formulae, i.e. bounded formulae of the new language $LA(\mathcal{E}^2)$,
(c) add a defining axiom $DEF(f)$ for each new function symbol f.

Clearly, $I\Sigma_0 \subseteq I\mathcal{E}^2_*$, but it is unknown whether equality holds. It is easy to see that $I\mathcal{E}^2_*$ is contained in an extension by definitions of $I\Sigma_0 + exp$; in fact, this inclusion is strict, since $I\mathcal{E}^2_*$ can only capture functions of polynomial growth (i.e., Theorem 3 can be proved for $I\mathcal{E}^2_*$ instead of $I\Sigma_0$).

By exploiting the availability of "census functions" of $\mathcal{E}^2_*$-definable sets in $I\mathcal{E}^2_*$, i.e. the ability to count the number of elements of any $\mathcal{E}^2_*$-definable set by means of a function in $\mathcal{E}^2$, A. Woods proved (see [20])

Theorem 9. *$I\mathcal{E}^2_*$ proves $PHP\mathcal{E}^2_*$, where $PHP\mathcal{E}^2_*$ denotes the pigeonhole principle schema for $\mathcal{E}^2_*$ formulae.*

As a consequence of Theorems 8 and 9, Problem 2 has a positive answer if $I\Sigma_0$ is replaced by $I\mathcal{E}^2_*$.

Now we turn our attention to subsystems of $I\mathcal{E}^2_*$, studied by A. Berarducci & B. Intrigila (see [2]) and Ch. Cornaros (see [3]). Each one of these systems includes $I\Sigma_0$ and is included in $I\mathcal{E}^2_*$, but it is unknown whether any of these inclusions are proper.

Berarducci and Intrigila considered combinatorial principles provable in $I\mathcal{E}^2_*$; we will refer to only two, i.e. $weak - PHP\Sigma_0$ and $EQ\Sigma_0$.

Definition 4. (a) $Weak - PHP\Sigma_0$ is the following schema

$$\begin{aligned}(1+\varepsilon)z > z \wedge \quad & \forall x < (1+\varepsilon)z\ \exists y < z\ \varphi(x,y) \rightarrow \\ & \exists x_1, x_2 < (1+\varepsilon)z\ \exists y < z(x_1 \neq x_2 \wedge \varphi(x_1,y) \wedge \varphi(x_2,y)),\end{aligned}$$

where φ is any Σ_0 formula with parameters and $\varepsilon > 0$ is any rational number.
(b) $EQ\Sigma_0$ (equipartition principle for Σ_0 relations) tis the following schema

$\forall z$ "if $\varphi(x,y)$ defines an equivalence relation on z such that every equivalence class
has exactly n elements, then $n \mid z$",

where φ is any Σ_0 formula and $n \in N$.

It should be noted that $weak - PHP\Sigma_0$ had been previously considered by J. Paris, A. Wilkie and A. Woods (see [14]) and that Theorem 9 clearly implies that $I\mathcal{E}^2_* \vdash weak - PHP\Sigma_0$.

Using Theorem 9, Berarducci and Intrigila obtained

Theorem 10. *$I\mathcal{E}^2_*$ proves $EQ\mathcal{E}^2_*$, where $EQ\mathcal{E}^2_*$ is as before, but considering $\mathcal{E}^2_*$ formulae instead of Σ_0 ones.*

They also showed that the following hold:

Theorem 11. *$I\Sigma_0 + weak - PHP\Sigma_0$ proves Lagrange's theorem, i.e. that every integer is the sum of four squares.*

Theorem 12. *$I\Sigma_0 + EQ\Sigma_0$ proves the "complementary conditions" of the quadratic reciprocity law, i.e. that for any odd prime p:*
(a) -1 is a quadratic residue $modp$ iff $p \equiv 1 mod4$
(b) 2 is a quadratic residue $modp$ iff $p \equiv \pm 1 mod8$.

Theorem 13. *$I\Sigma_0 + EQ\Sigma_0$ proves that a prime number is the sum of two squares iff it is of the form $4n + 1$.*

For the proofs they used the multiplicative property of Legendre's symbol $(\frac{x}{p})$ (p an odd prime) and some group-theoretical considerations – the usual proofs are based on Euler's criterion $(\frac{x}{p}) \equiv x^{p-1/2} modp$, but it is unknown whether this is provable in the theories considered.

Cornaros, continuing the work of Berarducci and Intrigila, proved

Theorem 14. *$I\mathcal{E}^2_*$ proves the quadratic reciprocity law, i.e. that for any odd primes p, q:*

$$(\tfrac{p}{q})(\tfrac{q}{p}) = (-1)^{(p-1)(q-1)/2}.$$

His proof is based on the usual one and exploits the the fact that $\prod_{0\leq x\leq y,\varphi(x)} f(x) modp$ and $\sum_{0\leq x\leq y} f(x)$ are $\mathcal{E}^2$ functions, for any $f \in \mathcal{E}^2$ and any $\mathcal{E}^2_*$ formula φ.

He also attempted to prove the following conjecture of A. Woods (see [20]).

Conjecture. *$I\Sigma_0(\pi) + DEF(\pi)$ proves that the set of primes is unbounded, where $I\Sigma_0(\pi) + DEF(\pi)$ is the subsystem of $I\mathcal{E}^2_*$ if we allow only one new function symbol π corresponding to the usual function $\pi(x)$ = number of primes $\leq x$.*

Cornaros showed that adding π and one more new function symbol to LA suffices, namely

Theorem 15. *$I\Sigma_0(\pi, K)+DEF(\pi)+DEF(K)$ proves Bertrand's postulate, where K is a new function symbol corresponding to the usual function $K(x) = \sum_{0<n\leq x} log_e n$.*

For the proof, an approximate logarithm function is used again and care is taken to define other functions involved in the usual proof, e.g. $\psi(x)$, in a $\Sigma_0(\pi, K)$ manner.

Next, we discuss problems and results concerning the system $I\Sigma_0 + \Omega_1$, where Ω_1 denotes the axiom $\forall x \exists y (y = x^{[log_2 x]})$. By Theorem 3, $I\Sigma_0$ is strictly weaker than $I\Sigma_0+\Omega_1$. To see that $I\Sigma_0+\Omega_1$ is strictly weaker than $I\Sigma_0+exp$, it suffices to consider the structure with universe $\{x \in M : M \models x < a^{[log_2 a]^n}$ for some $n \in N\}$, for an arbitrary nonstandard $M \models PA$ and $a \in M - N$.

Let us see what is known about Problems 1 − 3 if $I\Sigma_0$ is replaced by $I\Sigma_0 + \Omega_1$.

(a) The feeling is that Problem 1 again has a negative solution. Indeed, Wilkie's observation shows that if $I\Sigma_0 + \Omega_1$ proves the MRDP theorem, then $NP = co - NP$.

(b) By using ingenious coding techniques, Paris, Wilkie and Woods showed (see [15])

Theorem 16. *$I\Sigma_0 + \Omega_1$ proves $weak - PHP\Sigma_0$.*

(c) Again in [15] one finds

Theorem 17. *$I\Sigma_0 + \Omega_1$ proves that the set of of primes is unbounded.*

Actually this can be improved to

Theorem 18. *$I\Sigma_0 + \Omega_1$ proves Sylvester's theorem.*

This follows from Theorem 16 and the fact that Woods's proof of Theorem 8 really uses $weak - PHP\Sigma_0$, not $PHP\Sigma_0$.

We continue with a short discussion of a very weak subsystem of $I\Sigma_0$. This is denoted by $IOpen$ and is obtained from $I\Sigma_0$ if we allow induction for open formulae only. The study of free-variable systems was first advocated by T. Skolem (see [17]). Shepherdson obtained (see [16])

Theorem 19. *$IOpen$ does not prove any of the following:*
(a) $x^2 \neq 2y^2 \vee x = 0$
(b) $x^3 + y^3 \neq z^3 \vee xyz = 0$
(c) the set of primes is unbounded.

By part (a) of this theorem and the fact that $I\Sigma_0$ proves $\forall x, y(x^2 \neq 2y^2 \vee x = 0)$, it follows that $IOpen$ is strictly weaker than $I\Sigma_0$.

To prove this theorem, Shepherdson constructed a recursive nonstandard model M of $IOpen$, in which (a)-(c) fail, as follows:
The universe of M is the set of all polynomials of the form

$$a_p X^{p/q} + a_{p-1} X^{(p-1)/q} + \cdots + a_1 X^{1/q} + a_0,$$

where $p, q \in N$, $q > 0$, $a_p, \ldots, a_1$ are real algebraic, $a_p > 0$ if $p > 0$, a_0 is an integer and is ≥ 0 if $p = 0$. Successor, addition, etc., are defined in the obvious way; by taking X to be "infinitely large", one can make M into a discretely ordered semi-ring.

Many other authors studied $IOpen$, among which A. Wilkie ([19]), L. Van den Dries ([18]) and A. Macintyre & D. Marker ([9]), obtaining very interesting results. We mention only one result from [9], namely

Theorem 20. *$IOpen$ does not prove Lagrange's theorem.*

Most proofs in [9], including the proof of the previous result, involve constructions of models by unions of chains arguments and repeated use of purely algebraic constructions.

Let us finish with a remark: Most of the systems we have defined in this paper have been studied extensively from more than one viewpoints, but we have been concerned only with results associated to the main problem stated at the beginning. For information concerning other viewpoints, we urge the interested reader to consult A. Macintyre's excellent survey of the subject ([8]).

References

[1] J. Bennett: *On Spectra*, Ph. D. thesis, Princeton University, 1962.

[2] A. Berarducci & B. Intrigila: *Combinatorial principles in elementary number theory*, Ann. Pure Appl. Logic **55** (1991), 35 – 50.

[3] Ch. Cornaros: *On Grzegorczyk Induction*, Ann. Pure Appl. Logic .. (1995), ...

[4] Ch. Cornaros & C. Dimitracopoulos: *The prime number theorem and fragments of PA*, Arch. Math. Logic **33** (1994), 265 – 281.

[5] C. Dimitracopoulos & J. Paris: *The pigeonhole principle and fragments of arithmetic*, Z. Math. Logik Grundlag. Math. **32** (1986), 73 – 80.

[6] H. Gaifman & C. Dimitracopoulos: *Fragments of Peano's arithmetic and the MRDP theorem*, Logic and Algorithmic, Monograph. Enseign. Math. **30** (1982), 187 – 206.

[7] A. Grzegorczyk: *Some classes of recursive functions*, Rozprawy Mat. IV (1953), 1 – 45.

[8] A. Macintyre: *The strength of weak systems*, Proc. of the 11th Wittgenstein Symposium, Kirchberg/Wechsel (Austria), Hölder-Pichler-Tempsky, Wien, 1987, 43 – 59.

[9] A. Macintyre & D. Marker: *Primes and their residue rings in models of open induction*, Ann. Pure Appl. Logic **43** (1989), 57 – 77.

[10] Y. V. Matijasevič: *Enumerable sets are diophantine* (Russian), Dokl. Akad. Nauk SSSR **191** (1970), 279 – 282. English translation: Soviet Math. Doklady **11** (1970), 354 – 357.

[11] R. Parikh: *Existence and feasibility in arithmetic*, J. Symbolic Logic **36** (1971), 494 – 508.

[12] J. Paris: *Some conservation results for fragments of arithmetic*, Lecture Notes in Math. **890** (1981), 251 – 262.

[13] J. Paris & C. Dimitracopoulos: *Truth definitions for Δ_0 formulae*, Logic and Algorithmic, Monograph. Enseign. Math. **30** (1982), 317 – 329.

[14] J. Paris & L. A. S. Kirby: *Σ_n-Collection schemas in arithmetic*, Logic Colloquium '77, North-Holland, 1978, 199 – 209.

[15] J. B. Paris, A. J. Wilkie & A. R. Woods: *Provability of the pigeonhole principle and the existence of infinitely many primes*, J. Symbolic Logic **53** (1988), 1235 – 1244.

[16] J. Shepherdson: *A non-standard model for a free variable fragment of number theory*, Bull. Polish Acad. Sci. Math. **12** (1964), 79 – 86.

[17] Th. Skolem: *Peano's axioms and models of arithmetic*, Mathematical interpretations of formal systems, Amsterdam, 1955, 1 – 14.

[18] L. Van den Dries: *Some model theory and number theory for models of weak systems of arithmetic*, Lecture Notes in Math. **834** (1980), 346 – 362.

[19] A. J. Wilkie: *Some results and problems on weak systems systems of arithmetic*, Logic Colloquium '77, North-Holland, 1978, 285 – 296.

[20] A. R. Woods: *Some problems in logic and number theory* and their connections, Ph. D. thesis, Manchester University, 1981.

Department of Methodology, History and Philosophy of Science,
University of Athens, 37, J. Kennedy Str., 161 21 Kaisariani, Greece.
E-mail address: `cdimitr@atlas.uoa.ariadne-t.gr`