WHAT ARE WEAK ARITHMETICS?

Patrick CEGIELSKI* Denis RICHARD†

Contents

*LACL - IUT - route forestière HURTAULT - F-77300 FONTAINEBLEAU - cegielski@univ-paris12.fr
†LLAIC1 - IUT Dépt. Informatique - B.P. 86 - F-63172 AUBIÈRE cedex - richard@llaic.u-clermont1.fr

I. - An attempt to define Weak Arithmetics from the *Journées sur les Arithmétiques Faibles*

It is amusing, indeed astonishing, that no-one among a community of about one hundred computer scientists, logicians and mathematicians organizing meetings twice a year for almost ten years[1] has thought it advisable properly and precisely to define the field of research one usually calls *Weak Arithmetics.* In my opinion, everybody, within this group, brought to it his own interest and wondered at not having to justify the relevance of Weak Arithmetics. In discussions by ourselves, it appears that this relevance is intuitively founded on a common field of mathematical interest, a common set of questions and logical methods to investigate problems, and a general culture within computer science. Basically, a scientist interested in Weak Arithmetics knows some mathematical logic, likes PEANO Arithmetic and the two GÖDEL Theorems, works or has been working on decision problems, on algorithms and their complexities, and uses all kinds of abstract machines. Through these machines Weak Arithmetics are strongly influenced by the computer-dominated modern world. The Weak Arithmetics scientist is not a professional mathematician who studies numbers (using such tools as algebraic methods, complex analysis and algebraic geometry) but is often (or always in some areas) in contact with Number Theory. Therefore it is difficult to give a precise definition of Weak Arithmetics as a discipline in the same way as - say - Model Theory. Nevertheless we can nowadays consider the list of lectures and talks given from JAF1 to JAF17, in order to determine the main directions and themes provided by the participants at those events. One can distinguish four groups of lectures which the reader can find in the Annex.

Theme 1.- *Construction of Nonstandard Models of first-order Arithmetics in order to investigate:*

1) *axiomatizations of subtheories of* PEANO *Arithmetic (denoted PA) in which induction schemata are restricted to a special subset of formulas;*

2) *complexities of the considered subtheories, especially for developing polynomial time algorithms.*

This theme is closely linked, on the one hand, to the study of induction schemata which are respectively called logarithmic, open, parameter free, Δ_k-induction, etc., and, on the other hand, to the BUSS Arithmetic. In this theme, logicians try to construct (nonstandard) models having specific properties (for example an ordered field without an integer part (BOUGHATTAS)). One tries also to prove (or disprove) some axiomatizability properties such as the fact that open-induction in normal rings is not finitely axiomatisable (BOUGHATTAS). Algorithmic and Complexity theories are also connected to this theme because computability in polynomial time corresponds to some specific axiomatisations one can characterize: for instance P. PUDLAK, TAKEUTI and KRAJICEK proved the equivalence between the provability in bounded arithmetic of the collaps of the strict *polynomial time hierarchy and the finite axiomatizability of the arithmetical theory in the language of addition, multiplication and* $x^{\lceil \log x \rceil}$ *with induction schemata restricted to* Σ_0*-formulas.*
The lively style of the preface by J.P. RESSAYRE provides a precise and well-documented presentation, the deep links between nonstandard models, axiomatizability and algorithmic complexity. So on this matter, we refer to his text.
Another illustration of this theme is bounded arithmetics, which were introduced by BUSS within a first-order logical language which we denote $L(BA)$. This language contains the

[1]The first "Journées sur les Arithmétiques Faibles" had been held in june 1990 at the "École Normale Supérieure de Lyon"

symbols of successor, addition, multiplication, 0, $\lfloor(x/2)\rfloor$, length of x, that is to say $\lceil(\log_2(x+1))\rceil$, the function $2^{|x|\cdot|y|}$, identity and natural order. In this language, BUSS defines a special induction-schemata on certain subset of formulas providing a Weak Arithmetical theory S such that a subset A of N is P if and only if it is S-provably $NP \cap (Co - NP)$. In so doing, BUSS provides a promising method to prove a set A is P since, according to this result, it is sufficient to prove it is both NP and $Co - NP$ in some explicitly known and specific (weak) theory. About this result, P. CEGIELSKI wrote: *Practically, if we know it is both NP and $Co - NP$, then the method used to prove this result certainly is not too complex and the demonstration can be formalized in such a theory. However, up to now, no set has been shown in P by such a method. The reason is that bounded arithmetics are still not widely developed. For instance we do not know which classical theorems of Number Theory are true in these Weak Arithmetics. The length of proof of any classical theorem increases greatly with weakness of the arithmetical theory in which this proof takes place. For instance, a proof of* DIRICHLET *theorem on (infinity of) primes in arithmetical sequences in primitive recursive arithmetic PRA is one hundred pages long. Such results would help to apply* BUSS'(results).

Theme 2.- *Definability and decidability of weak substructures of the Standard Model of* PEANO.

The general framework of definability is presented in a detailed way in the survey carried out by P. CEGIELSKI in the ANNALS of MATHEMATICS and ARTIFICIAL INTELLIGENCE, vol. 16 n^{os}1.4 (1996). For a structure M, we denote by DEF(M) the set of constants, functions and relations which are first-order definable within M. Following CHURCH and TURING's proof in 1936 that the theory of natural integers equipped with addition and multiplication and identity is not decidable, we obtain a method for proving the undecidability of the theory of a structure M which consists in showing $\mathrm{DEF}(M) = \mathrm{DEF}(N, +, \times, =)$. The set $\mathrm{DEF}(N, +, \times, =)$ is well-known and K. GÖDEL proved it contains any relation we can define by recursion (with some particular set of natural functions as primitives) so that , if M is a sub-structure of the standard model, then the inclusion of DEF(M) into $\mathrm{DEF}(N, +, \times, =)$ is trivial. One of the most famous questions to have been solved in the framework of arithmetical definability is HILBERT's tenth problem; It asks for an algorithm to determine whether a given diophantine equation has a solution or, in other words whether there exists a program such that given a polynomial $P(x_1, \ldots, x_n)$ with integer coefficients as input, we can obtain as output the set, possibly empty, of integer solutions of $P(x_1, \ldots, x_n) = 0$. In 1970, I. MATIASSEVITCH proved the key-results leading to a negative answer to this problem: exponentiation is definable by a diophantine equation, i.e. by a Σ_1-formula within PEANO Arithmetic. Of course, this result was obtained after years of research and collaboration with M. DAVIS, H. PUTNAM, J. ROBINSON who provide many classical theorems and conjectures. Due to this cooperation, in the definability area we refer to as the MDRP (for MATIASSEVITCH-DAVIS-ROBINSON-PUTNAM) theorem the fact that every Σ_1-formula is equivalent to a Diophantine formula. The key-points of this famous proof of the negative solution of the tenth-HILBERT problem belong to arithmetical coding and definability:

- It is possible *to code* the process of register machines by the masking relation $r \rightharpoondown s$ between the integers r and s given in their binary expansion; more precisely, we say that s masks r if and only if when 0 appears as a digit in the binary expansion of s then 0 also appears as the digit of the same rank in the binary expansion of r;
- (A corollary of LUCAS' Theorem) the miracle is that $r \rightharpoondown s$ if and only if $\binom{r}{s} \equiv 1 \pmod 2$, which means that one can completely *describe in the language of first-order arithmetic not only the operation* of a register machine, but also that of a normal computer as well;
- the description, via first-order arithmetical formulas describing the operating cycles, of a register machine, can finally be rewritten as a conjunction of diophantine equations; this is due to arithmetical properties such as, for instance, the *exponential growth* of the sequence of the solutions $x_a(n)$ and $y_a(n)$ to the PELL-FERMAT equation $x^2 - \sqrt{a^2-1}y^2 = 1$.

A by-product of this is the possibility of first-order defining the set of prime as the set of positive value $P(\mathbb{N}^n) \cap \mathbb{N}$ of a certain polynomial P due to J.P. JONES and al...

In the present theme, usually we consider an arithmetical substructure M of the standard model and we try to prove that either the whole arithmetical standard model is definable within M, or M is *decidable* and in this case we investigate the complexity of the considered structure. This is not an alternative: there are *undecidable weak substructure of* PEANO *where addition and multiplication are not simulteneously definable and which are undecidable.* The problem of definability which is the main topic of theme 2 goes back to Number Theory questions raised a long time ago, as we shall show in part II below. Arithmetical definability is closely related to Number Theory and, in a sense, sheds new light on its classical results. In part II of the present preface, we intend to develop on an example having historical roots going back a century before the second main theme of Weak Arithmetics, namely the problem of mutual definability of arithmetical relations within first-order Number Theory. Undecidability is a corollary of definability of addition and multiplication in the framework of PEANO Arithmetic. Weak Arithmetics therefore also include arithmetical decision problems such as decidable extensions of PRESBURGER (additive) arithmetic and SKOLEM (multiplicative) arithmetic. The decision problem for additive prime number theory is adressed both within Number Theory and the Theory of Automata. There are conditional results in this field (mostly due to A. WOODS) under SHINZEL's Hypothesis on primes, and absolute results recently proved by CEGIELSKI, RICHARD and VSMIRNOV. The study of the set RUD of rudimentary predicates (GRZEGORCZYK and ESBELIN) is linked both to BUSS Arithmetics, and to algorithmic and Spectra problems which concern the set of cardinalities of the finite models of a given first-order formula. It is worth noting that rudimentary predicates extend to real analysis and to the problem of speeding up software used in computer science and numerical analysis. In our somewhat arbitrary classification, we put RUD in a special theme with the study of the problem of spectra (finite models), arithmetisation of graphs and GRZEGORCZYK hierarchy.

Theme 3.- *Abstract Machines, Automata and Words.*
Any program in a specified language which we use in a computer has a corresponding abstract machine, for instance a TURING machine. Actually, we can formalize any program because with addition and multiplication we can define (or simulate) all recursive schemata. Now if we consider only some Weak Arithmetic (for instance PRESBURGER Arithmetic) then a corresponding abstract machine computing functions and relations definable in this theory, or in a model of this one, is of course weaker than a TURING Machine (for instance it can be an automat on for PRESBURGER Arithmetic). In this way, it is natural to associate abstract machines (Automata, Push Down Automata, Cellular Automata, BELTIUKOV Machines, Alternating TURING Machines, etc) with different weak arithmetical theories and to the models we investigate. During the JAF, many machines, algorithms and the objects they represent were presented. Of course, the *words* - arguments which these machines use - with the different meaning we give to this notion in computer science, were studied. To this theme also belong general coding theory and all problems of weak arithmetical structures consisting of the usual integers with pairing functions (such as CANTOR pairing polynomial) or codings of n-tuples (using for example the well-known β-function of GÖDEL). Machines as tools for solving problems of definability or decidability were used by I. KOREČ, A. BÈS, V. BRUYÈRE, C. MICHAUX, J.E. PIN, J. TOMASIK, etc. Machines are not only tools but are themselves the objects of investigation such as for instance the smallest universal TURING Machines (M. MARGENSTERN and PAVLOTSKAIA), or the MATIASSEVITCH machines introduced to solve problems of trace monoid (A. MUSCHOLL, Y. MATIASSEVITCH). Results on these machines are due to O. TEYTAUD and A. BÈS. The problem of determining whether counting is possible with a given abstract machine is closely connected to question of complexity hierarchies as in the case of the GRZEGORCZYK hierarchy. Automata trees and modular counting were developed by H.A. ESBELIN and R. ESPEL LLIMA. In the framework of infinite games and particularly on Borelsets, J. DUPARC, J.P. RESSAYRE, O. FINKEL refer to automata but this is considered to be on the boundary between Weak Arithmetics and Set Theory.
We have seen that Weak Arithmetics cover two main themes (Axiomatizibility and Complexity in Subtheories of PEANO Arithmetic on the one hand, and Arithmetical Definability and Decidability on the other). We have also noted that Abstract Machines underlie our investigations and thus become another theme of studies within the framework of Weak Arithmetics. Nevertheless these three areas do not exhaust the topics presented by par-

ticipants of the JAF. We list some recurrent questions and some new concepts in the last section of this part.

Other Themes.-
a) *Graphs, Spectra and RUD*;
b) *Elementary proofs of classical Number Theory results, Arithmetical Proof Theory;*
c) *Functional Programing and Recursivity*;
d) *General Logic*;
e) *Applied Algorithmics.*

Theme a) refers to Finite Models and to the FAGIN conjecture which is also linked to RUD according to some results of A. WOODS. The notion of Graph is central and its arithmetisation addresses this question within Weak Arithmetics. In the present issue there is an arithmetisation of the four-colour problem due to Y. MATIASSEVITCH.

Theme b) stems from the work ERDÖS and SELFRIDGE who were the first to ask for what they called elementary proofs (*i.e.* in the framework of real analysis instead of complex analysis) of results such as the DIRICHELET Theorem on the infinity of primes in arithmetical sequences. Logicians such as TAKAEUTI, KREISEL and SIMPSON (with his reverse mathematics) have contributed to the subject but in a general way. P. CEGIELSKI and O. SUDAC have constructed proofs for specific classical theorems (such as the Prime Number Theorem of DE LA VALLÉE POUSSIN). They have also constructed some first order denumerable structures modelling a version of PEANO Analysis to provide proofs within PEANO Arithmetic models or even within the standard model of weaker arithmetical theories (*e.g.* PRA, the Primitive Recursive Arithmetic). It is clear that this work should be continued in order to strengthen the tools developed by BUSS.

Theme c) is clearly within the scope of Weak Arithmetics wherein one attempts to reconstruct a missing induction or recursive schemata. In Functional Programming also attempts to avoid recursion and recursive definition. For example L. COLSON demonstrates that roughly speaking primitive recursive algorithms are not optimal in terms of complexity.

Theme d) is mainly concerned with NEZONDET's p-destinies which are a general tool founded on trees for deciding closed sentences when applied to theories consisting of a set of sentences in a relational language which have a bounded number of quantifiers. This a promising new method which, for example gives rise to many interesting questions in Number Theory (GUILLAUME, JELEI YIN, RICHARD).

Theme e) could be considered to be the future of Weak Arithmetics in Informatics. A considerable proportion of software relies on algorithms which derive from numerical analysis however, due to the undecidability of the real zero, many of these programs have to be written within the framework of the standard model $\mathbb{Z}$ of integers. This is particularly the case in discrete geometry, computer imagery and artificial vision where faster computation with increasing precision is constantly demanded. Some structure such as the natural integers with the mappings ceiling and floor is necessary to describe digital planes and their algorithms of connectivity, or to perform ray tracing and so on. Here the blend of Number Theory, Logical Arithmetic and Computer Science (automata and chips) which make up Weak Arithmetics has been applied effectively and will become more and more useful.

II. - An illustration of a definability problem is Weak Arithmetics definability: the WOODS-ERDÖS conjecture

The question of *whether first-order arithmetic on the set of nonnegative integers is definable in terms of the successor function S and the coprimeness predicate* $\perp$ is a typical problem of Weak Arithmetics and perhaps, historically speaking, one of the first to be posed in this modern framework. It was raised in 1949 by Julia ROBINSON in her thesis, when she investigated the axiomatizability of different theories of elementary structures on numbers. More precisely, Julia ROBINSON stated: *We might also try to improve the theorem by replacing divisibility by the relation of relative primeness. However I have not been able to determine whether $\bullet$ is arithmetically definable in terms of $\perp$ and S or even in terms of $\perp$ and $+$.* This question, and some others of the same nature such as the definability of all arithmetical relations in terms of addition and coprimeness, were neglected for decades. In the eighties, Alan WOODS, returned to these problems. He was the first to realize that the question of definability within mathematical logic is equivalent to the following conjecture of Number Theory: *there is an integer k such that for every pair (x, y) of integers, the equality $x = y$ holds if and only if $x + i$ and $y + i$ have the same prime divisors for $0 \leq i \leq k$.* This number-theoretical form of Julia ROBINSON's question is itself very closely linked to some open questions proposed by Paul ERDÖS and for which he had conjectured a positive answer. In the book by Richard GUY entilted *Unsolved Problems of Number Theory*, the question is attributed to Alan WOODS, but due to its close relation with conjectures of ERDÖS which were known to A. WOODS, this conjecture is known as the WOODS-ERDÖS conjecture, or WE or WE(k) if it is necessary to state the parameter k. Indeed, WE is a weakening of the following conjecture of P. ERDÖS: ERDÖS *asks if there are infinitely many* 4*-tuples* (m, k, n, l) such that $(m+1)(m+2)\ldots(m+k)$ and $(n+1)(n+2)\ldots(n+l)$ with $k \geq l \geq 3$ can contain the same prime factors. *For example* 2.3.4.5.6.7.8.9.10 *and* 14.15.16 *or* 48.49.50, *also* 2.3.4.5.6.7.8.9.10.11 *and* 98.99.100. For $k = l \geq 3$ he conjectures that there are only finitely many. ERDÖS' interest is the relationship between prime divisors and consecutive integers is supported by many other papers. Weak Arithmetic, combines a Number-Theoretoc pointof view with approchies based on mathematical Logic and concept of definability in a fashion particulary appropriate to the investigation of the WE-conjecture.

II-1 The Number Theoretical approach to WE.

The problem of finding a local characterization of an integer a by its prime divisors and by the prime divisors of $a - 1$ (or $a + 1$) - which actually is a problem of definability - was raised by famous mathematicians many years ago. The fundamental result on this question is due to ZSIGMONDY and was rediscovered and generalized by BIRKHOFF and VANDIVER twelve years later. They showed that, except for 2 and 8, each power u of a prime number p is characterized by p and the prime divisors of $u + 1$. An analogue of the previous result dealing with $x^n + y^n$ has been proved by LUCAS and generalized by CARMICHAEL.
Another Classical result closely related to WE is due to C. STØRMER who showed the following:
Let $\mathrm{p}_1, \ldots, \mathrm{p}_\mathrm{n}$ *be distinct prime numbers and* K, $\alpha_1, \ldots, \alpha_\mathrm{n}$ *be nonnegative integers. For* $1 \leq \mathrm{i} \leq \mathrm{n}$, *let us put* $\varepsilon_\mathrm{i} = 1$ *if* α_i *is odd,* $\varepsilon_\mathrm{i} = 2$ *if* α_i *is even and set* $\mathrm{D} = \mathrm{K}.\mathrm{p}_1^{\epsilon_1} \ldots \mathrm{p}_\mathrm{n}^{\epsilon_\mathrm{n}}$.
If $\mathrm{x}^2 - 1 = \mathrm{K}.\mathrm{p}_1^{\alpha_1} \ldots \mathrm{p}_\mathrm{n}^{\alpha_\mathrm{n}}$ *then* x *is the fundamental solution of the* PELL-FERMAT *equation* $\mathrm{x}^2 - \mathrm{Dy}^2 = 1$*;*
If $\mathrm{x}(\mathrm{x}+1) = \mathrm{K}.\mathrm{p}_1^{\alpha_1} \ldots \mathrm{p}_\mathrm{n}^{\alpha_\mathrm{n}}$ *then* $2\mathrm{x} + 1$ *is the fundamental solution of the* PELL-FERMAT *equation* $\mathrm{x}^2 - 4\mathrm{Dy}^2 = 1$.
Now, we define $SUPP(n)$ as the set of the prime divisors of n. From this result, the following:

(i) *If* E *is a set of* n *distinct prime integers, there are at most* 2^n *nonnegative integers satisfying the condition* $\mathrm{SUPP}(\mathrm{x}(\mathrm{x}+1)) \subset \mathrm{E}$, *so that, for any nonnegative integer* a, *the set* ST(a) *of nonnegative integers* b *such that*

$$\mathrm{SUPP}\ (\mathrm{a}) = \mathrm{SUPP}(\mathrm{b}) \ \text{ and } \ \mathrm{SUPP}(\mathrm{a}+1) = \mathrm{SUPP}(\mathrm{b}+1) \ \textit{is also finite.}$$

(ii) *The nonnegative integers* x *and* y *are equal if and only if the following conditions are simultaneously satisfied:*

1) SUPP(x - 1) = SUPP(y - 1) and SUPP(x + 1)=SUPP(y + 1);

2) *for all prime numbers* p *in* SUPP($x^2 - 1$) *(or in* SUPP($y^2 - 1$)) *the* exponent *of* p *in the factorisation of* x + 1 *(resp.* x - 1*) has the same parity as in the factorisation of* y + 1 *(resp.* y - 1*).*

Recently, number theoretists such as M. LANGEVIN, R. BALASUBRAMANIAN, T.N. SHOREY and M. WALDSCHMIDT have investigated bounds and inequalities which permit the location of integers in N according to the relationship of their supports. In this direction, LANGEVIN provides a fundamental result he calls the *reduction lemma.* To present it, we introduce his notation:

SUPP$(x) = \{p \in \mathbb{N} : p$ *is prime and* $p|x\}$?
$u(n)$ is *the product of the primes in* SUPP(n);
$P(n)$ is *the greatest prime in* SUPP(n);
$w(n)$ is *the cardinality of* SUPP(n);
$u(n;k)$ is *the product of all primes in* SUPP$((n+1)(n+2)\ldots(n+k))$;
$v(n;k) = P((n+1)(n+2)\ldots(n+k))$.

Reduction Lemma. (LANGEVIN). *Let* x *and* y *be positive integers. In each group labelled* (i), (ii), (iii), (iv), *the conditions given are equivalent:*

(i) u(y +i) = u(x + i) *for* $1 \leq$ i $\leq$ k (condition H_1(k));
u(x,k) = u(y,k) | (y - x) (condition H_5(k)).

(ii) u(y + i) | u(x + i) *for* $1 \leq$ i $\leq$ k (condition H_2(k));
u(x,k) | (y -x) (condition H_3(k));
u(y,k) = gcd ((y - x),u(x,k)) (condition H_4(k)).

(iii) P(y + i) | (x + i) *for* $1 \leq$ i $\leq$ k (condition H_6(k));
v(y,k) | (y - x) (condition H_7(k)).

(iv) P(y + i) = P(x + i) *for* $1 \leq$ i $\leq$ k (condition H_8(k));
v(y,k) = v(x,k) | (y - x) (condition H_9(k)).

We note that condition $H_1(k)$ is the very hypothesis of WE. These conditions show how close the links are between the languages of successor and coprimeness on one hand and successor and divisibility on the other hand.

Beginning with the results on inequalities, we first mention a fundamental result of M. LANGEVIN who proved that for $0 < x < y$, if SUPP(x) = SUPP(y) then $|y - x| > [\log(x + y)]^{1/6}$.

This inequality was improved upon by R. BALASUBRAMANIAN, T.N. SHOREY and M. WALDSCHMIDT who proved that for x, y, k *being nonnegative integers satisfying* 0<x<y *and* k $\geq$ 1 *and* H_1(k) *of the previous reduction lemma:*

1) *There exists an effectively computable absolute positive constant* C *such that:*

$$y-x > (k \log\log y)^{C.k(\log\log y)(\log\log\log y)} \text{ for } y > 27;$$

2) *There exists an effectively computable absolute positive constant* D *such that:*

$$\log x > D(\log(k))^2 (\log(\log(k))) \text{ for } k > 3.$$

3) *There exists an effectively computable absolute positive constant* E *such that:*

$$y-x > \exp(E.k(\log(k))^2(\log(\log(k))^{-1} \text{ for } k > 3.$$

Importance of the Woods-Erdös conjecture

Beyond its intrinsic interest both to Mathematical Logic (more precisely for arithmetical definability and axiomatizability) and Number Theory, the attempt to prove or disprove the questions of J. ROBINSON, A. WOODS and P. ERDÖS, gains in importance if we realize how strong the links are between WE and other classical conjectures of Number Theory. In the same paper by LANGEVIN, the following results were proved:

Let k *be the parameter appearing in the* WOODS-ERDÖS *conjecture* WE(k).

1) *If there is an absolute constant* C *such that for any pair* (x,y) *of positive integers the condition* $x^3 \neq y^2$ *implies:*

$$|x^3 - y^2| > [\max(x^3, y^2)]^C \text{ (HALL's conjecture).}$$

then the answer to WE *is positive.*

2) *Moreover, under the same hypothesis* $x^3 \neq y^2$ *above, if we can prove*

$$|x^3 - y^2| > [\max(x^3, y^2)]^{1/6},$$

then the answer to WE(k) *is positive with* $k \geq 16$ *modulo a finite set of exceptions.*

3) *If for every positive real* ε*, there exists a constant* D *such that for any pair* (a,b) *of positive integers we have;*

$$u(a + b)ab > D(a + b)/(\gcd(a,b)^{1-\varepsilon} \text{ ((a-b-c)-}\textit{conjecture}\text{)},$$

then the answer to WE(k) *is positive with* $k \geq 3$ *modulo a finite set of exceptions.*

We note that as a result of conclusions 2) and 3) the above theorem is a *negative answer to WE would refute both* HALL *'s conjecture*, and the so-called OESTERLÉ-MASSER *'s conjecture* (also called the *a-b-c-conjecture*).

There are still other relationships of WE to questions recently answered by Capi Corrales RODRIGÀNEZ and René SCHOOF about the characterization of x by supports of $x^n - 1$, for infinitely many positive n this was also a question posed by ERDÖS. Maxim VSMIRNOV (unpublished) has a proof of the characterization of integers by finitely many supports. Ten years ago, we asked *whether* $SUPP(x^{2^n} - 1) = SUPP(y^{2^n} - 1)$ *for all* $n \in \mathbb{N}$ *implies* $x = y$ and we gave a proof due to A. SCHINZEL of the fact that the (*a-b-c*)-conjecture implies a positive answer to our question. In the section devoted to the logical approach to WE, we present an analogue of these results within the frame-work of definability, when we prove that $\mathrm{DEF}(\mathbb{N}, =, +, \times) = \mathrm{DEF}(\mathbb{N}, S, \perp, \mathrm{POW})$.

II-2 Logical approach to WE.

To place the logical approach to WE in a more general and historical setting, it is worth pointing out that arithmetical definability goes back to Kurt GÖDEL who proved that the structure $\langle \mathbb{N}, =, +, \times \rangle$ is *closed under primitive recursion.* In order to appreciate the power of this result, consider the effort required to obtain a direct first-order definition of exponentiation, or of the natural enumeration of prime integers, from equality, addition and multiplication. Another interesting aspect of GÖDEL's result is that *there exist arithmetical structures which are not closed under primitive recursion*:

- addition does not belong to $\mathrm{DEF}(\mathbb{N}, =, S)$ as shown by LANGFORD in 1926;
- multiplication does not belong to $\mathrm{DEF}(\mathbb{N}, =, +)$ as shown by PRESBURGER in 1929.

Defining addition and multiplication from some *a priori* weaker languages of arithmetic is not always easy but is sometimes possible. A classical example is the language $\{S, \times\}$ which defines all arithmetical relations. A. TARSKI provided a first-order $\langle S, \times \rangle$-definition of addition from the following equivalence:

$$(xz + 1)(yz + 1) = [z^2(xy + 1)] + 1 \textit{ if and only if } (x = y = z = 0 \text{ or } x + y = z).$$

Julia ROBINSON's results

In a sense, folling the GÖDEL's works and the above relation due to TARSKI, the first important and really difficult result was the characterization of definability within a *Weak Arithmetic* structure and was obtained by J. ROBINSON:

Addition and multiplication are definable in the structure $\langle \mathbb{N}, S, | \rangle$.

In the same paper, J. ROBINSON showed that the set $\mathbb{N}$ of nonnegative integers is definable in terms of addition and multiplication within the field $\mathbb{Q}$ of rationals. This result is central to the investigation of decidable and undecidable theories.

In order to find other natural axiomatisations of arithmetic, J. ROBINSON asked whether $\mathrm{DEF}(\mathbb{N},+,\perp) = \mathrm{DEF}(\mathbb{N},+,\times)$.
There was first an unpublished positive solution by J. ROBINSON, then a second solution by A. WOODS proving that the $(+,\perp)$-definability of multiplication is a corollary of the SCHNIRELMANN Theorem (stating that every integer is the sum of a finite bounded number of primes). Finally we obtained a proof using coding devices.

It is worth observing that J. ROBINSON attempt to propose *a natural* axiomatization of first-order PEANO arithmetic in terms of S and $|$, was in part completely realized by P. CEGIELSKI in his thesis. Indeed CEGIELSKI has given *a first-order natural axiomatization of first-order* PEANO *Arithmetic in the language* $\{=, 0, 1, S, |\}$. To obtain this axiomatization, he used the so-called ZBV-method of coding which we describe below.

Alan WOODS' results.

Concerning the language $\{<,\perp\}$, the first result is due to A. WOODS who also proved that $\mathrm{DEF}(\mathbb{N},<,\perp) = \mathrm{DEF}(\mathbb{N},+,\times)$. In the sequel we call this question the ROBINSON *problem* (namely: *is there an equality between* $\mathrm{DEF}(\mathbb{N},=,S,\perp)$ *and* $\mathrm{DEF}(\mathbb{N},=,+,\times)$). A. WOODS has linked the ROBINSON problem to the WOODS-ERDÖS conjecture by proving that the answer to the ROBINSON problem is positive if and only if the WE conjecture is true. More precisely, Alan WOODS proved that the following assertions are all equivalent:

(i) *The answer to the* ROBINSON *problem is positive, namely one can define addition and multiplication in terms of equality, coprimeness predicate and successor function;* (and vice-versa)

(i') *One can define natural order, or addition, or multiplication in terms of equality, coprimeness predicate and successor function;*

(ii) *One can define equality, addition and multiplication in terms of coprimeness predicate and successor function;*

(ii') *One can define natural order, or addition, or multiplication in terms of coprimeness predicate and successor function;*

(iii) *One can define equality in terms of coprimeness predicate and successor function;*

(iv) *The answer to the* WOODS-ERDÖS *conjecture is positive, namely,* there is an integer k such that for every pair (x, y) of integers, the equality $x = y$ holds if and only if $x + i$ and $y + i$ have the same prime divisors for $0 \leq i \leq k$.

Remark. It is worth pointing out the *status of equality*: if we consider successor and coprimeness without equality, then to define equality is equivalent to a positive answer to WE; on the other hand, if we consider equality, successor and coprimeness together, then a success at definition equality order (resp. addition or multiplication) is still equivalent to a positive answer to WE.

At this step in the investigation of the ROBINSON problem, farther results are obtained via the so called ZBV-Method (for ZSIGMONDY-BIRKHOFF-VANDIVER) which we have introduced. This method allows are to prove all the results already mentioned this section as well as providing new results.

ZBV-method of coding.

The ZBV-method consists in considering *integers of the form* $x^m - y^m$ or $x^m + y^m$ (where x and y are coprime) to be coded by *their respective support or their respective set of primitive or characteristic divisors.* This method is most effective when x is a fixed prime p and y is 1, 2 or 3. By this method, one reduces arithmetical questions to an investigation of finite sets of primes and their boolean combinatorics.
Moreover, every finite set of primes (or every function of finite domain mapping primes to primes) is itself codable in infinitely many ways by a single prime integer using a combination

of the Chineese Remainder Theorem and the DIRICHLET Theorem. A prime which is a code plays the role of *a memory in which we store a finite set of primes.* One can *interpret the structure* $\langle\mathbb{N},\perp\rangle$ *as a set theory on the supports of nonnegative integers.* Any finite part A of the set of primes is coded by the set of integers x having A as its support.

New $(S,\perp)$-definable relations and undecidability of $\mathrm{Th}(\mathbb{N},S,\perp)$ via the ZBV-method.

It can be proved that an integer u *is a power of a prime* (we say also *primary*) if and only if the support of u is included in the support of any integer not coprime to u. As a consequence, the following relations are $(S,\perp)$-definable:
- the set $\mathbb{PP}$ of *powers of primes*;
- the set $\mathbb{PP}(a)$ of *powers of the same prime* a;
- every *finite relation* on $\mathbb{N}$;
- the *equality* $=_{\mathbb{PP}}$ *restricted* to $\mathbb{PP}$;
- the *successor function and the predecessor function restricted* to $\mathbb{PP}$;

every integer which is a *constant* (this is not obvious but is a corollary of the previous point).

A fundamental result derived from the ZBV-method is the possibility of defining the set $\mathbb{P}$ of primes within the structure $\langle\mathbb{N},S,\perp\rangle$. This result can be extended to the structure $\langle\mathbb{N},\mathrm{pred},\perp\rangle$ where *Pred* denotes the predecessor function on $\mathbb{N}$. They are in both structures $\langle\mathbb{N},S,\perp\rangle$ and $\langle\mathbb{N},\mathrm{pred},\perp\rangle$, we have *all set theoretical combinatorics exist on the supports.* For every pair (p,q) of distinct primes the notation $q^{ord(q,p)}$ is by definition the only power u of q such that p is a primitive divisor of $u-1$. The crucial fact is that the ternary relation

$$\{(p,q,u)\in\mathbb{P}\times\mathbb{P}\times\mathbb{PP}\ \textit{ such that }\ u=q^{ord(q,p)}\}$$

is definable in both structures $\langle\mathbb{N},S,\perp\rangle$ and $\langle\mathbb{N},\mathrm{pred},\perp\rangle$.

¿From this relation, one can provide a natural and intrinsic definability within $\mathbb{PP}$ by successor and coprimeness, and also shed some new light on why the elementary theory of $\langle\mathbb{N},S,\perp\rangle$ is undecidable. Let us begin by putting $\mathrm{NewAdd}(x,y,z)$ (resp. $\mathrm{NewMult}(x,y,z)$ if and only if $5^z=5^{x+y}$ (resp. $5^z=5^{xy}$) and denoting $=_{\mathbb{PP}}$ the restriction of equality to $\mathbb{PP}$. One can show that:

(i) *The function* $x\to 5^x$ *transforms the structure* $\langle\mathbb{N},=,+,\times\rangle$ *into a new structure* $\langle 5^{\mathbb{PN}},=_{\mathbb{PP}}$, *NewAdd, NewMult*$\rangle$ *which is definable in* $\langle\mathbb{N},S,\perp\rangle$;

(ii) *consequently, the theory* $\mathrm{Th}(\mathbb{N},S,\perp)$ *is undecidable;*

(iii) *moreover,* $\mathrm{DEF}(5^{\mathbb{PN}},=_{\mathbb{PP}},\mathit{NewAdd},\mathit{NewMult})=\mathrm{DEF}(\mathbb{N},=,+,\times)$.

What may be added to successor and coprimeness in order to define all arithmetical relations?

At this step the logical approach consists in finding out what are the relations we can add to successor and coprimeness to obtain the definability of all arithmetical relations. With this in mind, we consider the *binary* relations of *exponentiation* and power of the form

$$\mathrm{EXP}=\{(\mathrm{x},\mathrm{y})\in\mathbb{N}\times\mathbb{N}\ \textit{ such that there exists }\ \mathrm{a}\ \textit{ which satisfies }\ \mathrm{y}=\mathrm{a}^{\mathrm{x}}\},$$

and

$$\mathrm{POW}(\mathrm{x},\mathrm{y})=\{(\mathrm{x},\mathrm{y})\in\mathbb{N}\times\mathbb{N}:\exists\mathrm{n}[(\mathrm{n}\neq 0)\wedge(\mathrm{y}=\mathrm{x}^{\mathrm{n}})]\}.$$

From the previous result, it can be shown (see [RD,1985-4] and [GSRD,1989]) that

(i) *Every relation or function which is first-order definable in* $\langle\mathbb{N},+,\times,=\rangle$ *is actually first-order definable in* $\langle\mathbb{N},S,\perp,\mathrm{EXP}\rangle$.

(ii) *Every relation or function definable by a first-order formula of* $\{+,\times,=\}$ *is also definable in the structure* $\langle\mathbb{N},\mathrm{S},\perp,\mathrm{POW}\rangle$ *by a first-order formula of the associated language* $\{\mathrm{S},\perp,\mathrm{POW}\}$.

It now follows that *the structure* $\langle\mathbb{N},\perp,<_{\mathbb{PP}}\rangle$ *where* $<_{\mathbb{PP}}$ *denotes the natural order on* $\mathbb{N}$ *restricted to primaries, allows the first-order definition all arithmetical relations on* $\mathbb{PP}$, *and verifies* that $\mathrm{DEF}(\mathbb{N},=+,\times)\underset{\neq}{\supset}\mathrm{DEF}(\mathbb{N},\perp,<_{\mathbb{PP}})$.

The last result we would like to mention, is due to Francis NEZONDET who showed the importance of *equality* and, the *difference between relational and functional languages*, to the investigation of arithmetical definability in terms of successor and exprimeness. Actually, there is a structure $\langle M, +_f, \times_f, 0, 1, \perp\rangle$ which is *elementarily equivalent to the standard model* $\langle \mathbb{N}, +_f, \times_f, \perp, 0, 1\rangle$ and in which the identity relation is not definable. More precisely:
Let $+_f$, $\times_f$ be respectively the functional symbols of addition and multiplication. There exists an arithmetical model

$$\mathcal{M} = \langle M, =, +, \times, \perp, 0, 1\rangle \quad \textit{of} \quad Th(\mathbb{N}, +_f, \times_f, \perp, 0, 1)$$

and of the relational theory with equality of the finite arithmetic and within which there is no $(+_f, \times_f, \perp, 0, 1)$-formula defining equality, thus refuting WE.

Here $+_f$, $\times_f$ are respectively the *functional* symbols of addition and multiplication, will be interpreted in the usual way on $\mathbb{N}$. The coprimeness predicate $\perp$ on $\mathbb{N}$ and on the domain M is the interpreted as a first-order formula $F(x, y)$ meaning (x *and* y *are coprime*) on $\mathbb{N}$. By finite arithmetic, we denote the $(=, +, \times)$-axioms which characterize an ordered semi-ring. Of course, our finite arithmetic (namely the RR system of Raphael ROBINSON) is a purely relational theory which contains a symbol of equality and *does not contain any schema of induction.* The proof of this result, consists in first building a model of the finite arithmetic RR and of $Th\langle \mathbb{N}, +_f, \times_f, \perp, 0, 1\rangle$ and then demonstration, that equality is not $(+_f, \times_f, \perp)$-definable. We emphasise that here addition and multiplication are functions *and not relations.* Finally, the theory of the standard model with the functions of addition and multiplication, the coprimeness relation and the constants 0 and 1, does not decide the WOODS-ERDÖS conjecture.

Conclusion: Due to the new tools, the computers, and the new objects of our investigation, the abstracts machines modelizing fragments of the human reasoning, weak arithmetics have appeared. Perhaps weak arithmetics precede weak real analysis which we can observe showing up against the mist of the complexity theory of reals.