Report on the paper (version from August 4, 2017)

"A new proof of Euclids algorithm"

submitted to Fundamenta Informaticae by Andrzej SALWICKI

The paper presents a proof of the correctness of Euclid's algorithm in the theory of algorithmic logic containing the usual first-order Peano arithmetic.

Algorithmic logic is a very interesting theory with nice properties (in particular, the completeness theorem) which is a natural framework (though not the only one) to get correctness proofs. As such, the proof for Euclid's algorithm, which is clearly and nicely presented in the paper, is an interesting contribution which deserves publication.

However, the paper contains outrageous claims that are absolutely unacceptable. In the Abstract and the Introduction, the author explains that all proofs of Euclid's algorithm are semantical and cannot be formalized in any first-order theory, say usual first-order Peano arithmetic, since they require all integers to be standard:

- *"For these reasons the proofs go beyond the elementary Peano's theory"* (line 6 of the Abstract),
- *"Till today, every one of known proofs of correctness of Euclid's algorithm is conducted in an intuitive number theory. Among others, it is assumed that the arguments are standard natural numbers."* (line 6 of §1).

These claims are false. Correctness of Euclid's algorithm is indeed a theorem in usual first-order Peano arithmetic. The reason is that one can code finite sequences of integers by integers in a definable way (this is the trick of Gödel's beta function) and thus express computations and prove the correctness of Euclid's algorithm via a simple formal induction which mimics the one given in informal proofs. Such a proof in usual first-order Peano arithmetic can even be seen as much stronger than the one the author gives in algorithmic logic since it does not require standard time computations (a basic inherent feature of algorithmic logic).

It is a fact that most proofs in mathematical papers and books are presented in an informal way which seems to deal with standard objects: standard integers, standard reals, standard well-founded relations, ... But this does not mean that they cannot be formalized in a formal mathematical theory. This simply means that mathematicians do not care about formal versions, leaving them to logicians (and now also to computer scientists). And long ago, logicians have seen that such a formalization is possible, let it be in first-order Peano arithmetic, in "second-order" Peano arithmetic (which is really a first-order theory with two kinds of variables and a membership relation) or in Zermelo set theory or Zermelo-Fraenkel set theory. Indeed, one of the numerous topics in logic is to look at how much induction (Δ_0-induction, Σ_1-induction,...) or comprehension (Δ_0-comprehension, Σ_1-comprehension,...) is needed to prove a given theorem. And the Polish and Čech mathematical communities have some brilliant specialists of these questions, e.g., Zofia Adamowicz, Pavel Pudlak, Jan Krajìček.

The author will find some clarification in the book by Stephen Simpson "Subsystems of Second Order Arithmetic" which deals with these questions, mostly for questions in analysis. The considered subsystems are first-order theories with set variables but the notion of model is NOT reduced to the standard one: there may be non standard integers and in case all integers are standard some sets of integers may be missing. In a few pages, Simpson describes different subsystems of Second Order Arithmetic and the different kinds of models: the β-models in which the integers are the standard ones and well-foundedness is the standard one, the ω-models in which the integers are the standard ones but well-foundedness may not be the standard one (due to missing subsets), and all other models in which the integers may not be the standard ones. Another book, more centered on arithmetic, is the one by Petr Hajék and Pavel Pudlák, "Metamathematics of First-Order Arithmetic". There is also a book by C. Smorynski.

A remark about Fact 4.1: it is not clear how to extend with a multiplication operation the nonstandard model $\mathbb{N}+(\mathbb{Z}\times\mathbb{Q})$ of Presburger arithmetic described in Appendix A so as to get a model of Peano's arithmetic.

I suggest that the author looks at the above references, discusses the topic with colleagues aware of "weak arithmetic", "reverse mathematics", and modifies the paper adequately, removing completely the material of section 1. The main part of the paper, the proof of correctness of Euclid's algorithm in the theory of algorithmic logic, is interesting and will deserve publication.