A note on formalization of Euclide's algorithm in arithmetics

We consider Euclide's algorithm in its simple form.

E: { **while** *not* equal(x,y) **do if** less(x,y) **then** y:=subtract(y,x) **else** x:= subtract(x,y) **fi od** }

A run of the algorithm is a sequence of pairs of natural numbers, e.g.,

$$(4, 10),\ (4, 6),\ (4, 2),\ (2, 2)$$

We encode a sequence of pairs $(a_1, b_1), \ldots, (a_k, b_k)$ by a product of the consecutive prime numbers

$$2^{\alpha_1} \cdot 3^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k},$$

where $\alpha_i = 2^{a_i}3^{b_i}$, for $i = 1, \ldots, k$. For example, the run above is encoded by

$$2^{2^4 3^{10}} \cdot 3^{2^4 3^6} \cdot 5^{2^4 3^2} \cdot 7^{2^2 3^2}$$

We can express this encoding in the language of first-order arithmetics with the set of basic operations $\{0, 1, +, \cdot, x^y\}$. More specifically, we can write a formula $Euclide(a, b, m, d)$, which forces the following properties of a, b, m, d.

- $a, b \geq 1$,
- 2 divides m with the exponent $2^a 3^b$,
- if some prime p divides m with the exponent $2^x 3^y$ with $x \neq y$ then
  if $x < y$ then the **next** prime divides m with the exponent $2^x 3^{y-x}$
  else the next prime divides m with the exponent $2^{x-y} 3^y$,
- if some prime p divides m with the exponent $2^z 3^z$ then no greater prime divides m, and $d = z$.

Now consider a formula

$$\varphi \equiv (\forall a, b)\,(a \geq 1 \wedge b \geq 1) \Rightarrow \exists! m\, \exists! d\, Euclide(a, b, m, d) \wedge d = gcd(a, b)$$

(where *gcd* stands for *greates common divisor*).

Claim. The sentence φ is satisfied in the standard model of arithmetics (with exponentiation).

Conjecture. There is a set of first-order axioms $\mathbf{PA}_{exp}$, such that the sentence φ is satisfied in *any* model of $\mathbf{PA}_{exp}$, and consequently (by Gödel's completeness theorem) it is provable from $\mathbf{PA}_{exp}$.

dn