THE BULLETIN OF SYMBOLIC LOGIC
Volume 10, Number 3, Sept. 2004

IS THE EUCLIDEAN ALGORITHM OPTIMAL AMONG ITS PEERS?

LOU VAN DEN DRIES AND YIANNIS N. MOSCHOVAKIS

The Euclidean algorithm on the natural numbers $\mathbb{N} = \{0, 1, \dots\}$ can be specified succinctly by the *recursive program*

$$\varepsilon: \quad \gcd(a, b) = \begin{cases} b, & \text{if } \operatorname{rem}(a, b) = 0, \\ \gcd(b, \operatorname{rem}(a, b)), & \text{otherwise} \end{cases} \qquad (a \geq b \geq 1),$$

where $\operatorname{rem}(a, b)$ is the remainder in the division of a by b, the unique natural number r such that for some natural number q,

$$a = bq + r \qquad (0 \leq r < b). \tag{1}$$

It is an algorithm *from* (*relative to*) the remainder function rem, meaning that in computing its *time complexity function* $c_\varepsilon(a, b)$, we assume that the values $\operatorname{rem}(x, y)$ are provided on demand by some "oracle" in one "time unit". It is easy to prove that

$$c_\varepsilon(a, b) \leq 3 \log_2 a \quad (a > b > 1).$$

Much more is known about $c_\varepsilon(a, b)$, but this simple-to-prove upper bound suggests the proper formulation of the Euclidean's (worst case) optimality among its *peers*—algorithms from rem:

CONJECTURE. *If an algorithm α computes* $\gcd(x, y)$ *from* rem *with time complexity $c_\alpha(x, y)$, then there is a rational number $r > 0$ such that for infinitely many pairs $a > b > 1$, $c_\alpha(a, b) > r \log_2 a$.*

Our main aim here is to prove the following relevant result:

THEOREM A. *If a recursive program α decides the coprimeness relation $x \perp y$ from* $=, <, +, \dot{-}$, iq *and* rem, *then for infinitely many coprime pairs $a > b > 1$,*

$$c_\alpha(a, b) > \frac{1}{10} \log_2 \log_2 a. \tag{2}$$

Received December 22, 2003; revised April 22, 2004.
Van den Dries acknowledges support from NSF grant DMS 01-00979. Moschovakis acknowledges support from the Graduate Program in Algorithms and Computation (ΜΠΛΑ) and University of Athens Grant 70/4/5633.

1079-8986/04/1003-0004/$3.90