

1016-03-242

Lou van den Dries* (vddries@math.uiuc.edu), Department of Mathematics, University of Illinois, 1409 West Green Street, Urbana, IL 61801-2917. *On the Number of Arithmetic Steps Needed To Generate the Greatest Common Divisor of Two Integers.*

Given integers a, b , define an increasing sequence

$$G_0(a, b) \subseteq G_1(a, b) \subseteq \dots \subseteq G_n(a, b) \subseteq \dots$$

of finite subsets of \mathbf{Z} as follows: $G_0(a, b) = \{0, 1, a, b\}$, and

$$G_{n+1}(a, b) = G_n(a, b) \cup \{\text{sums, differences, integer quotients, remainders, and products of two numbers in } G_n(a, b)\}.$$

Let $g(a, b)$ be the least n such that $\gcd(a, b) \in G_n(a, b)$. There is a very easy double logarithmic *upper bound* (logarithms to base 2):

$$g(a, b) \leq 4 \log \log a \quad (a > b > 1).$$

This talk will focus on a more difficult *lower bound*:

There are infinitely many (a, b) with $a > b > 1$ such that

$$g(a, b) \geq \frac{1}{4} \sqrt{\log \log a}.$$

The proof uses arithmetic properties of integer solutions to the Pell equation $x^2 - 2y^2 = 1$. There are also connections, via model theory, to irrationality and transcendence. Motivation for finding such bounds comes from joint work with Yiannis Moschovakis on *arithmetic complexity*. I will mention some open problems in this area. (Received February 13, 2006)