A Note on the Number of Division Steps in the Euclidean Algorithm

S.A. Abramov

Computer Centre of the Russian Academy of Science,
Vavilova 40, Moscow 117967, Russia
abramov@ccas.ru

Let w be a natural number and let $\mu(w)$ be the maximal number of divisions that the Euclidean algorithm,

$$\begin{aligned} a_0 &= q_1 a_1 + a_2 \ , \\ a_1 &= q_2 a_2 + a_3 \ , \\ &\cdots \\ a_{k-2} &= q_{k-1} a_{k-1} + a_k \ , \\ a_{k-1} &= q_k a_k \ , \end{aligned} \tag{1}$$

needs for a given input (a_0, a_1), where $a_0 > a_1 = w$. Lamé's theorem [2, 1] (this theorem was proved earlier by Finck in 1841 [1]) implies the asymptotic estimate

$$\mu(w) = O(\log w), \tag{2}$$

and $\log w$ cannot be replaced by any function $h(w)$ such that $h(w) = o(\log w)$, since, if $F_0, F_1, \ldots$ is the Fibonacci sequence, for $a_0 = F_{k+2}$, $w = a_1 = F_{k+1}$ the number of divisions is equal to k. The difference between the latter number and $\log_\phi w$, where $\phi = \left(1 + \sqrt{5}\right)/2$, is a bounded value. One of the results related to the average case behavior of the Euclidean algorithm is by Heilbronn [4, 1]:

$$\frac{1}{\varphi(v)} \sum_{\substack{1 \le w \le v \\ \gcd(v,w)=1}} E(v,w) \sim \frac{12 \ln 2}{\pi^2} \ln v \ ,$$

where $E(v,w)$ is the number of division steps performed by the Euclidean algorithm on the input (v,w). From this asymptotic equality it follows that for some constant C the inequality

$$\mu(w) > \frac{12 \ln 2}{\pi^2} \ln w + C \tag{3}$$

holds. Using the standard notation $f(n) = \Theta(g(n))$, which is defined for functions $f(n)$, $g(n)$ with positive values by $f(n) = \Theta(g(n))$ if and only if

$$\exists c_1, c_2, n_0 > 0 \ , \ \forall n > n_0 \ , \ \ c_1 g(n) \le f(n) \le c_2 g(n) \ ,$$

we therefore have

Theorem 1 $\mu(w) = \Theta(\log w)$.

This article was formally reviewed following the procedures described in THIS BULLETIN, **32**(2), issue 124, 1998, pp 5–6.

We now prove the following main theorem.

Theorem 2 *For a constant c,*

$$\mu(w) > \frac{1}{2} \log_\phi w + c \ , \tag{4}$$

where $\phi = \left(1 + \sqrt{5}\right)/2$.

Notice that $(12 \ln 2)/\pi^2 < 1/(2 \ln \phi)$, and (4) is stronger than (3) for all large enough w. Additionally, the proof of Theorem 2, which will be given, is elementary and thereby we get an elementary proof of Theorem 1.

We start with a lemma on Fibonacci numbers.

Lemma 1 *For any $0 < d < \sqrt{5}$ the inequality*

$$\left| \frac{F_{n+1}}{F_n} - \phi \right| < \frac{1}{d F_n^2} \tag{5}$$

holds for all large enough n.

Proof. An easy induction shows that

$$\frac{F_{n+1}}{F_n} - \phi = \frac{(-1)^{n+1}}{F_n \phi^n}$$

for $n = 1, 2, \ldots$ Set $\tilde{\phi} = (1 - \sqrt{5})/2$; $|\tilde{\phi}| < 1$. Since

$$F_n = (\phi^n - \tilde{\phi}^n)/\sqrt{5} \ ,$$

we have

$$\phi^n = \sqrt{5} F_n + \tilde{\phi}^n$$

and

$$\frac{F_{n+1}}{F_n} - \phi = \frac{(-1)^{n+1}}{\left(\sqrt{5} + \frac{\tilde{\phi}^n}{F_n}\right) F_n^2}.$$

The claim follows. ∎

Define $v = \lfloor \phi w \rfloor$. This yields

$$\left| \frac{v}{w} - \phi \right| \le \frac{1}{w} \ . \tag{6}$$

Fix d such that $2 < d < \sqrt{5}$ and choose positive g such that $\frac{1}{g} + \frac{1}{d} < \frac{1}{2}$. Set

$$n = \max\{m : w \ge g F_m^2\} \ . \tag{7}$$

(Note that the value of n depends on w.) Since

$$\frac{1}{w^2} \le \frac{1}{g F_n^2} \ ,$$

we have from (5), (6) for all large enough w

$$\left| \frac{F_{n+1}}{F_n} - \frac{v}{w} \right| < \frac{1}{2F_n^2} .$$

By a well-known theorem (cf., for example, [3], Theorem 184), F_{n+1}/F_n is a convergent to v/w in the sense of Hardy & Wright [3], Section 10.2, i.e., if $a_0 = v$, $a_1 = w$ in (1), then for some integer l, such that $1 \leq l \leq k$, the equality

$$F_{n+1}/F_n = q_1 + 1/(q_2 + 1/(q_3 + \ldots + 1/(q_{l-1} + 1/q_l) \ldots))$$

holds. But this equality implies $l = n$ (and, additionally, $q_1 = \cdots = q_n = 1$). Hence the continued fraction for v/w is at least of length n, and so $\mu(w) \geq n - 1$. However, by (7), $n > \frac{1}{2} \log_\phi w + c$ for some constant c. Theorem 2 is proved.

Conjecture: $\mu(w) \sim \log_\phi w$.

This Conjecture is based on numerical experiments.

In conclusion we make a remark on the input size of the Euclidean algorithm. Using the value a_1 as the size of the input (a_0, a_1) is preferable to a_0 because a_0 can be much bigger than a_1, but the number of division steps for (a_0, a_1) is the same as that for (a_0', a_1), where $a_0' = a_1 + a_2$.

The value a_0/a_1 contains full information on the number of divisions, but if we use a_0/a_1 as the input size, then for inputs with bounded sizes we can get an unbounded number of divisions. As a consequence, no upper bound of the form $f(a_0/a_1)$ for the number of division can be obtained, if f is a continuous function. Asymptotic estimates of the form $O(f(a_0/a_1))$, $\Theta(f(a_0/a_1))$ with continuous f do not exist either. For example, an upper bound of the form $f(a_0/a_1)$ does not exist since $\lim_{n\to\infty} \frac{u_{n+1}}{u_n} = \phi$, and therefore f cannot be bounded in any neighborhood of ϕ.

Acknowledgement

Partially supported by Natural Sciences and Engineering Research Council of Canada Grant No. CRD215442-98.
The author thanks the anonymous referee for his helpful comments and E.V. Zima for useful discussions and numerical experiments related to the topic of the paper.

References

[1] E. Bach, J. Shallit. *Algorithmic Number Theory, Vol. 1.* The MIT Press, 1997.

[2] D.E. Knuth. *The Art of Computer Programming, Vol. 2.* Third edition. Addison-Wesley, 1997.

[3] G.H. Hardy, E.M. Wright. *An Introduction to the Theory of Numbers, 4th edition.* Oxford, 1960.

[4] H. Heilbronn. On the average length of a class of finite continued fractions. In P. Turán, ed., *Number Theory and Analysis*, New York: Plenum, 1969, pp. 87–96.