THE LEAST REMAINDER ALGORITHM

J. L. BROWN, JR., and R. L. DUNCAN
The Pennsylvania State University, University Park, Pennsylvania

Lamé's theorem [1] asserts that the number of divisions n required to find the greatest common divisor (a, b) of a and b ($a \geq b$) using the Euclidean algorithm does not exceed five times the number of digits p in b. More precisely,

$$n < \frac{p}{\log \xi} + 1, \qquad \text{where} \qquad \xi = \frac{1 + \sqrt{5}}{2} .$$

It is also known [2], [3] that the number of divisions required to find (μ_{n+1}, μ_n) is n and that

$$\left[\frac{p_n - 1}{\log \xi}\right] \leq n - 1 \leq \left[\frac{p_n}{\log \xi}\right] , \tag{1}$$

where p_n is the number of digits in μ_n and $\mu_1 = 1$, $\mu_2 = 2$ and $\mu_n = \mu_{n-1} + \mu_{n-2}$ $(n > 2)$ are the Fibonacci numbers. Thus the upper bound given by Lamé's theorem is about the best possible and it has been shown [3], [4] that the upper and lower bounds in (1) are attained for infinitely many n.

We recall that the remainders in the ordinary Euclidean algorithm are always positive but that shorter algorithms may be obtained by allowing negative remainders. A well known result of Kronecker [1] asserts that the least-remainder algorithm (L. R. A.) is never longer than any other Euclidean algorithm. The purpose of this note is to derive results analogous to (1) for the L. R. A. To do this, we define $v_1 = 1$, $v_2 = 2$ and $v_m = 2v_{m-1} + v_{m-2}$ $(m > 2)$. This sequence has been applied to a similar problem by Shea [5].

Let

$$\begin{aligned}
a &= bq_1 + e_1 b_1 \\
b &= b_1 q_2 + e_2 b_2 \\
&\vdots \qquad\qquad \vdots \\
b_{m-2} &= b_{m-1} q_m + e_m b_m \\
b_{m-1} &= b_m q_{m+1}
\end{aligned}$$

be the L. R. A. for (a,b), where $a_k = \pm 1$ (k = 1, $\cdots$, m) and $a > b \geq 2b_1 \geq 4b_2 \geq \cdots \geq 2^m b_m > 0$. Then the required number of divisions is m + 1 and [1]

$$b_m \geq 1 = v_1, \quad b_{m-1} \geq 2b_m \geq 2 = v_2,$$
$$b_{m-2} \geq 2b_{m-1} + b_m \geq 2v_2 + v_1 = v_3, \cdots .$$

Hence

$$b_{m-k} \geq v_k + 1 \quad \text{and} \quad b \geq v_{m+1}.$$

Now let $N = 1 + \sqrt{2}$. Then

$$N < \frac{1}{2} \cdot 5 = \frac{1}{2} v_3 ,$$

$$N^2 = 2N + 1 < \frac{1}{2}(2v_3 + v_2) = \frac{1}{2} v_4, \cdots .$$

Hence,

$$N^{m-1} < \frac{1}{2} v_{m+1} \leq \frac{1}{2} b .$$

If p is the number of digits in b, then $b < 10^p$ and

$$m - 1 < \frac{\log b - \log 2}{\log N} < \frac{p - \log 2}{\log N} \quad \text{or} \quad m + 1 \leq 2 + \left[\frac{p - \log 2}{\log N}\right] .$$

Also,

$$N > 2 = v_2, \quad N^2 = 2N + 1 > 2v_2 + v_1 = v_3, \cdots .$$

Hence $N^{n-1} > v_n$. If q_n is the number of digits in v_n, then

$$v_n \geq 10^{q_n - 1}$$

and

$$n - 1 > \frac{q_n - 1}{\log N} \quad .$$

The L. R. A. for (v_{n+1}, v_n) is

$$\begin{aligned} v_{n+1} &= 2v_n + v_{n-1} \\ v_n &= 2v_{n-1} + v_{n-2} \\ &\vdots \\ v_3 &= 2v_2 + v_1 \\ v_2 &= 2v_1 \end{aligned}$$

and the required number of divisions is n. Thus

$$\left[\frac{q_n - 1}{\log N}\right] \leq n - 2 \leq \left[\frac{q_n - \log 2}{\log N}\right] \tag{2}$$

and the upper bound for the required number of divisions in the L. R. A. is about the best possible.

We now show that both the upper and lower bounds in (2) are attained for infinitely many n. Using standard difference equation techniques, it is easily shown that

$$v_n = \frac{1}{2\sqrt{2}} \left[(1 + \sqrt{2})^n - (1 - \sqrt{2})^n\right]$$

and it follows that

$$v_n \backsim \frac{N^n}{2\sqrt{2}} \quad .$$

Let ϕ_n be the fractional part (mantissa) of $\log v_n$. Then, since

$$q_n = 1 + [\log v_n],$$

we have

$$q_n = 1 + \log v_n - \phi_n .$$

Hence

$$q_n = 1 + n \log N - \log 2\sqrt{2} - \phi_n + o(1) . \tag{3}$$

But (3) implies that

$$n > \frac{q_n - \log 2}{\log N} + \frac{\phi_n - \frac{1}{4}}{\log N}$$

for all sufficiently large n. Thus

$$n - 2 \geq \left[\frac{q_n - \log 2}{\log N}\right]$$

If $\phi_n \geq 1/4 + \log N$ and n is sufficiently large. Also, (3) implies that

$$n < \frac{q_n - 1}{\log N} + \frac{\phi_n + \frac{1}{2}}{\log N}$$

for all sufficiently large n. Thus

$$n - 2 \leq \left[\frac{q_n - 1}{\log N}\right]$$

if $\phi_n \leq 2 \log N - 1/2$ and n is sufficiently large.

The desired results will follow when it is shown that the sequence $\{\log v_n\}$ is uniformly distributed modulo one [6]. The proof is almost identical to that of a similar result [3] and is therefore omitted. Also, further discussion of such results occurs elsewhere [7].

[Continued on page 401.]