BEGINNERS' CORNER

Edited by DMITRI THORO
San Jose State College

THE EUCLIDEAN ALGORITHM II

1. INTRODUCTION

In Part I [1] we saw that the greatest common divisor of two numbers could be conveniently computed via the famous Euclidean algorithm. Suppose that exactly n steps (divisions) are required to compute the g. c. d. of s and t ($s \geq t$). We then have

$$
\begin{array}{lll}
(1) & s = t q_1 + r_1, & 0 < r_1 < t \\
(2) & t = r_1 q_2 + r_2, & 0 < r_2 < r_1 \\
(3) & r_1 = r_2 q_3 + r_3, & 0 < r_3 < r_2 \\
(4) & r_2 = r_3 q_4 + r_4, & 0 < r_4 < r_3 \\
(5) & r_3 = r_4 q_5 + r_5, & 0 < r_5 < r_4 \\
\vdots & & \\
(n-1) & r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}, & 0 < r_{n-1} < r_{n-2} \\
(n) & r_{n-2} = r_{n-1} q_n + 0 . &
\end{array}
$$

Since each quotient $q_i \geq 1$, the above equations imply

$$
\begin{array}{ll}
(2') & t \geq r_1 + r_2 \\
(3') & r_1 \geq r_2 + r_3 \\
(4') & r_2 \geq r_3 + r_4 \\
(5') & r_3 \geq r_4 + r_5
\end{array}
$$

etc.

From (2') and (3'), $t \geq 2r_2 + r_3$; but from (4'), $2r_2 + r_3 \geq (2r_3 + 2r_4) + r_3$. Similarly, from (5'), $3r_3 + 2r_4 \geq (3r_4 + 3r_5) + 2r_4$, etc. Continuing in this manner we note the generous abundance of Fibonacci numbers. Thus

$$t \geq r_1 + r_2 \geq 2r_2 + r_3 \geq 3r_3 + 2r_4 \geq 5r_4 + 3r_5$$

$$\ldots \geq F_{n-1} r_{n-2} + F_{n-2} r_{n-1} .$$

2. A BASIC RESULT

Since the remainders form a strictly decreasing sequence with r_{n-1} the last non-zero remainder,

$$r_{n-2} > r_{n-1} \geq 1 .$$

Consequently,

$$t \geq F_{n-1} r_{n-2} + F_{n-2} r_{n-1} \geq 2F_{n-1} + F_{n-2} = F_{n+1} .$$

To summarize, if n divisions are required to compute the g.c.d. of s and t, then t is at least as large as the $(n+1)^{st}$ Fibonacci number!

3. LAMÉ'S THEOREM

Although the Euclidean algorithm is over 2,000 years old, the following result was established by Gabriel Lamé in 1844.

Theorem

The number of divisions required to find the g.c.d. of two numbers is never greater than five times the number of digits in the smaller number.

Proof.

Let ϕ designate the golden ratio. In [2] it was shown that

$$\phi^n = F_n \phi + F_{n-1}, \qquad n = 1, 2, 3, \ldots$$

Now since $2 > \phi = (1 + \sqrt{5})/2$, we see that

$$2F_n + F_{n-1} > F_n \phi + F_{n-1} \quad \text{or}$$

$$F_{n+2} > \phi^n .$$

Replacing n by n-1 and using the "basic result" of the preceding section yields

$$t > \phi^{n-1} .$$

To complete the proof note that

(i) if t has d digits then $d > \log t$

(ii) $\log t > (n-1) \log \phi$

(iii) $\log \phi > 1/5$.

Thus $d > (n-1)/5$ or $n \leq 5d$.

REFERENCES

1. D. E. Thoro, "The Euclidean Algorithm I," Fibonacci Quarterly, Vol. 2, No. 1, February 1964.
(Note that in excercises E8 and E10, (F_{n+1}, F_n) and $\max_n (n, F-1)$ should be replaced by $N(F_{n+1}, F_n)$ and $\max_n N(n, F-1)$ respectively.)

2. D. E. Thoro, "The Golden Ratio: Computational Considerations," Fibonacci Quarterly, Vol. 1, No. 3, October 1963, pp. 53-59.

xxxxxxxxxxxxxxxxxxxx