ON THE LENGTH OF THE EUCLIDEAN ALGORITHM

E. P. MERKES and DAVID MEYERS
University of Cincinnati, Cincinnati, Ohio

Throughout this article let a and b be integers, $a > b > 0$. The Euclidean algorithm generates finite sequences of nonnegative integers,

$$\{q_j\}_{j=1}^{n} \quad \text{and} \quad \{r_j\}_{j=1}^{n}$$

such that

$$
\begin{aligned}
a &= q_1 b + r_1, & 0 &< r_1 < b, \\
b &= q_2 r_1 + r_2, & 0 &< r_2 < r_1, \\
r_1 &= q_3 r_2 + r_3, & 0 &< r_3 < r_2, \\
&\cdots \\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, & 0 &< r_{n-1} < r_{n-2} \\
r_{n-2} &= q_n r_{n-1} + r_n, & r_n &= 0 .
\end{aligned} \tag{1}
$$

The integers r_{n-1} is the greatest common divisor of a and b and $q_n \geq 2$.

Define $\ell(a,b)$ to be the number of divisions n in the algorithm (1). Some basic properties of $\ell(a,b)$ are

(i) $$\ell(a,a) = 1;$$

(ii) $$\ell(ac,bc) = \ell(a,b), \quad c > 0;$$

(iii) $$\ell(a+b,b) = \ell(a,b);$$

(iv) $$\ell(a+b,a) = 1 + \ell(a,b).$$

Each of these properties is proved directly from the definition (1). Property (ii) permits us to assume a and b are relatively prime.

This paper is concerned with maximizing $\ell(a,b)$ when the integers a and b are drawn from certain subclasses of positive integers. There are some classical results in this direction such as the theorem of Lamé [3, p. 43] which states that $\ell(a,b)$ is never greater than five times the number of digits in b. We begin with a known result, the proof of which is instrumental for the justification of the main theorem of the paper.

Theorem 1. Let $\{F_j\}$ be the Fibonacci sequence generated by

(2) $$F_{j+2} = F_{j+1} + F_j, \quad F_{-1} = 0, \quad F_0 = 1 \quad (j = -1, 0, 1, 2, \cdots).$$

Editorial note: This is not our standard Fibonacci sequence.

If $a < F_{m+1}$ or $b < F_m$ for some integer $m > 0$, then $\ell(a,b) < \ell(F_{m+1}, F_m) = m$.

Proof. From (1) the rational number a/b has a continued fraction expansion

$$\text{(3)} \qquad \frac{a}{b} = q_1 + \frac{1}{q_2} + \frac{1}{q_3} + \cdots + \frac{1}{q_n}, \qquad 0 < q_j \quad (1 \le j < n), \qquad q_n \ge 2 .$$

The k^{th} numerator A_k and the k^{th} denominator B_k of this continued fraction are determined from the equations

$$\text{(4)} \qquad A_k = q_k A_{k-1} + A_{k-2}, \qquad B_k = q_k B_{k-1} + B_{k-2} \qquad (k = 1, 2, \cdots, n),$$

where

$$A_0 = 1, \ B_0 = 0, \ A_1 = q_1, \quad B_1 = 1 \quad [2, \text{p. } 3].$$

Since $q_k > 0$ for each index $k \le n$, it follows from (4) that

$$A_k > A_{k-1}, \quad B_k > B_{k-1} \quad (k = 2, 3, \cdots, n).$$

Moreover, by (1) and (4) we have $a \ge A_n$, $b \ge B_n$.

Suppose a and b are integers for which $n = \ell(a,b) \ge m$. Since $q_k \ge 1$ $(1 \le k \le n)$, we have $A_0 = F_0$, $A_1 \ge F_1$, $A_2 \ge F_1 + F_0 = F_2$, and, in general,

$$A_k \ge A_{k-1} + A_{k-2} \ge F_{k-1} + F_{k-2} = F_k \qquad (1 < k < n).$$

Finally, since $q_n \ge 2$, we have by (2)

$$A_n \ge 2A_{n-1} + A_n \ge 2F_{n-1} + F_{n-2} = F_{n-1} + F_n = F_{n+1}.$$

Similarly, $B_k \ge F_{k-1}$ $(1 \le k < n)$ and $B_n \ge F_n$. Furthermore, $A_n = F_{n+1}$ if and only if $q_k = 1$ $(1 \le k < n)$, $q_n = 2$ and $B_n = F_n$ if and only if $q_k = 1$ $(1 < k < n)$, $q_n = 2$. Since $a \ge A_n \ge F_{n+1} \ge F_{m+1}$ and $b \ge B_n \ge F_n \ge F_m$, we have the contrapositive of the first part of the implication in the statement of the theorem proved. The fact that $\ell(F_{m+1}, F_m) = m$ is a consequence of the statements concerning equality of A_m and B_m with F_{m+1} and F_m, respectively [1].

The ordered pairs of integers (a,b) can be partially ordered by defining $(a,b)\alpha(a',b')$ if $a \le a'$ and $b \le b'$. Relative to this partial order, the theorem states, in particular, that (F_{m+1}, F_m) is the "first" pair for which $\ell(a,b) = m$, i.e., if $(a', b')\alpha(F_{m+1}, F_m)$, then $\ell(a',b') < \ell(F_{m+1}, F_m)$ unless $a' = F_{m+1}$ and $b' = F_m$.

The proofs of our next results are dependent on the following known lemma.

Lemma 1. $\qquad F_{p+q} = F_p F_q + F_{p-1}F_{q-1} \quad (p, q = 1, 2, \cdots).$

Proof. Set $S_{p,q} = F_p F_q + F_{p-1}F_{q-1}$. Then by (2)

$$S_{p,q} = (F_{p-1} + F_{p-2})F_q + F_{p-1}F_{q-1} = F_{p-1}F_{q+1} + F_{p-2}F_q = S_{p-1,q+1}.$$

Repeated application of this identity yields

$$S_{p,q} = S_{1,q+p-1} = F_1F_{p+q-1} + F_0F_{p+q-2} = F_{p+q} .$$

Corollary (Lamé). If m is the number of digits in the integer b, then $\ell(a,b) \le 5m$.

Proof. We first show $F_{5n+1} > 10^n$ by induction. For $n = 1$, $F_6 = 13 > 10$. If the inequality is valid for an integer n, then by Lemma 1

$$F_{5n+6} = F_{5n+1}F_5 + F_{5n}F_4 > 8\cdot 10^n + \frac{5}{2}10^n = \frac{21}{2}10^n > 10^{n+1}$$

since

$$F_{5n} > \frac{1}{2}F_{5n+1} .$$

Thus, the inequality is valid for all integers.

Now if b has m digits, then $b < 10^m$ and, hence, $b < F_{5m+1}$. By Theorem 1 it follows that $\ell(a,b) < 5m + 1$ and Lamé theorem is proved.

It is interesting to observe that equality is possible in Lamé theorem if $b < 10^3$. If b has four digits, then $b < F_{20} = 10946$ and, by Theorem 1, $\ell(a,b) < \ell(F_{21}, F_{20}) = 20$. More generally, equality cannot hold in the Corollary for $m > 3$. Indeed, by Lemma 1 and the argument used in the proof of the corollary, we have $F_p > 10^k$ implies $F_{p+5} > 10^{k+1}$. Since $F_{20} > 10^4$, it follows that $F_{5m} > 10^m$ for $m \ge 4$. If $b < 10^m$ $(m \ge 4)$, then

$$\ell(a,b) < \ell(F_{5m+1}, F_{5m}) = 5m .$$

The next problem considered in this article pertains to the number of distinct pairs (a,b) such that

$$(F_{m+1}, F_m)\alpha(a,b)\alpha(F_{m+2}, F_{m+1})$$

and $\ell(a,b) = m$. We prove there are $m + 1$ such pairs and obtain formulas for the integers a and b that comprise the pairs. It is convenient to establish these results from a sequence of lemmas.

Lemma 2. Let the Euclidean algorithm for a and b, a and b are relatively prime, be (1) where for some integer m $(1 < m < n)$ - $q_m = 2$ and $q_k = 1$ $(k \ne m,\ 1 \le k < n)$, $q_n = 2$. Then

$$a = F_{n+1} + F_{n-m+1}F_{m-1}$$

and

$$b = F_n + F_{n-m+1}F_{m-2} .$$

Moreover, $(a,b)\alpha(F_{n+2}, F_{n+1})$.

Proof. From the proof of Theorem 1, we have that the k^{th} numerator and denominator of the continued fraction expansion for a/b when $\ell(a,b) = n$ satisfy, for $k < m$, the conditions $A_k = F_k$, $B_k = F_{k-1}$. From this fact and (4), we have

$$A_m = 2F_{m-1} + F_{m-2} = F_m + F_{m-1} = F_m + F_0F_{m-1} ,$$
$$B_m = 2F_{m-2} + F_{m-3} = F_{m-1} + F_{m-2} = F_{m-1} + F_0F_{m-2} ,$$
$$A_{m+1} = (F_m + F_{m-1}) + F_{m-1} = F_{m+1} + F_1F_{m-1} ,$$
$$B_{m+1} = (F_{m-1} + F_{m-2}) + F_{m-2} = F_m + F_1F_{m-2} .$$

Thus, by induction, we obtain

$$A_{n-1} = F_{n-1} + F_{m-1}F_{n-m-1} ,$$
$$B_{n-1} = F_{n-2} + F_{m-2}F_{n-m-1} .$$

Finally, by (4) and these formulas,

$$A_n = 2F_{n-1} + F_{n-2} + (2F_{n-m+1} + F_{n-m-2})F_{m-1} = F_{n+1} + F_{n-m+1}F_{m-1}$$

and, similarly, $B_n = F_n + F_{n-m+1}F_{m-2}$. Therefore, $a = A_n$ and $b = B_n$ and the first part of the lemma is proved.

Next, by Lemma 1, it follows that

$$F_{n+1} < A_n = F_{n+1} + F_{n-m+1}F_{m-1} = F_{n+1} + F_n - F_{n-m}F_{m-2} < F_{n+2}$$

and, similarly, $F_n < B_n < F_{n+1}$.

This lemma gives us $n - 2$ pairs $(m = 2, 3, \cdots, n - 1)$ of integers (a,b) such that

$$F_{n+1} < a < F_{n+2}, \qquad F_n < b < F_{n+1} ,$$

and $\ell(a,b) = n$. Since $\ell(F_{n+1}, F_n)$ and

$$\ell(F_{n+2}, F_n) = \ell(F_{n+1} + F_n, F_n) = \ell(F_{n+1}, F_n) = n,$$

there are so far n pairs in the range

$$(F_{n+1}, F_n)\alpha(a,b)\alpha(F_{n+2}, F_{n+1})$$

for which $\ell(a,b) = n$. The fact that there exists only one additional such pair is proved by the next two lemmas.

Lemma 3. Let $q_k = 1$ $(k = 1, 2, \cdots, n-1)$, $q_n = 3$ in the Euclidean algorithm (1) for the relatively prime integers a and b. Then

$$a = F_{n+1} + F_{n-1}, \qquad b = F_n + F_{n-2},$$

and

$$(F_{n+1}, F_n)\alpha(a,b)\alpha(F_{n+2}, F_{n+1}) .$$

If $q_k \geq 1$ $(k = 1, 2, \cdots, n-1)$, $q_n > 3$, then the corresponding integers a and b obey the inequalities $a > F_{n+2}$ and $b > F_{n+1}$.

Proof. From the proof of Theorem 1, we have $A_{n-1} = F_{n-1}$ and $B_{n-1} = F_{n-2}$ when $q_k = 1$ $(1 \leq k < n)$. If $q_n = 3$, then by (4),

$$A_n = 3F_{n-1} + F_{n-2} = F_n + 2F_{n-1} = F_{n+1} + F_{n-1}$$

and, similarly, $B_n = F_n + F_{n-2}$. Since $F_{n-2} < F_{n-1} < F_n$, we have

$$a = A_n < F_{n+1} + F_n = F_{n+2}$$

and

$$b = B_n < F_n + F_{n-1} = F_{n+1} .$$

Next, if $q_k \geq 1$ $(1 \leq k < n)$ and $q_n \geq 4$, we have $A_{n-1} \geq F_{n-1}$ and $B_{n-1} \geq F_{n-2}$. By (4)

$$\begin{aligned} a = A_n &\geq 4A_{n-1} + A_{n-2} \geq 4F_{n-1} + F_{n-2} \\ &= F_{n+1} + 2F_{n-1} > F_{n+1} + F_n = F_{n+2} . \end{aligned}$$

Similarly, $b = B_n > F_{n+1}$.

Lemma 4. Let the Euclidean algorithm for the integers a and b be (1), where $q_k \geq 2$ for at least three indices k or where $q_p \geq 2$, $q_m \geq 3$ for $1 \leq p, m \leq n$, $p \neq m$. Then $a > F_{n+2}$.

Proof. Let $q_k \geq 2$ for $k = m, p$ $(1 \leq m < p < n)$. Then, paralleling the proof of Lemma 2, we obtain

$$a \geq A_n \geq F_{n+1} + F_{n-m+1}F_{m-1} + F_{n-p+1}F_{p-1} . \tag{5}$$

Now the last expression is greater than F_{n+2} provided

$$F_{n-m+1}F_{m-1} + F_{n-p+1}F_{p-1} > F_n . \tag{6}$$

Since

$$F_{n-s+1}F_{s-1} > \frac{1}{2}F_n$$

for $1 \le s \le n$ by Lemma 1, the inequality (6) is valid. We conclude from (5) that

$$a \ge A_n > F_{n+1} + F_n = F_{n+2}.$$

If for some index m, $1 \le m < n$, we have $q_m \ge 3$, then $A_k \ge F_k$ for $k = 1, 2, \cdots, m - 1$ and by (4)

$$A_m \ge 3F_{m-1} + F_{m-2} = F_{m+1} + F_{m-1} > F_{m+1},$$
$$A_{m+1} \ge (F_{m+1} + F_{m-1}) + F_{m-1} > F_{m+1} + F_m = F_{m+2}.$$

By induction, $A_k > F_{k+1}$ for $m \le k < n$. Now

$$A_n \ge 2A_{n-1} + A_{n-2} > 2F_n + F_{n-1} = F_{n+2}$$

so $a > F_{n+2}$.

The final case to consider is when $q_m = 2$ for some index m, $1 \le m < n$ and $q_n \ge 3$. As in the proof of Lemma 2, it is easily shown that

$$A_k \ge F_k + F_{m-1} F_{k-m} \qquad (k = m, m + 1, \cdots, n - 1).$$

Thus,

$$A_n \ge 3A_{n-1} + A_{n-2} \ge 3F_{n-1} + F_{n-2} + (3F_{n-m-1} + F_{n-m-2})F_{m-1}$$
$$\ge F_{n+1} + F_{n-1} + (F_{n-m+1} + F_{n-m-1})F_{m-1} > F_{n+2},$$

provided

$$F_{n-m+1} F_{m-1} + F_{n-m-1} F_{m-1} > F_{n-2}.$$

This is the case since, by Lemma 1,

$$F_{n-s+1} F_{s-1} > \frac{1}{2} F_n$$

for $1 \le s \le n$ and, hence,

$$F_{n-m+1} F_{m-1} + F_{n-m-1} F_{m-1} > \frac{1}{2} (F_n + F_{n-2}) > F_{n-2}.$$

Therefore, $a > F_{n+2}$ in all cases considered in this Lemma.

Collecting the results in the last three lemmas, we have proved the following:

Theorem 2. Let $\mathfrak{A}$ be the set of ordered pairs (a,b) such that $(a,b)\alpha(F_{n+2}, F_{n+1})$. There are exactly $n + 1$ pairs in $\mathfrak{A}$ such that $\ell(a,b) = n$. These pairs are obtained from the formulas

$$a = F_{n+1} + F_{n-m+1} F_{m-1}, \qquad b = F_n + F_{n-m+1} F_{m-2}$$

$(m = 0, 1, 2, \cdots, n)$, where $F_{-2} = F_{-1} = 0$ and F_j for each $j \geq 0$ is the j^{th} Fibonacci number (2).

The results in Theorem 2 were suggested to the authors by considering a number of special cases on an IBM 360/65 computer.

REFERENCES

1. R. L. Duncan, "Note on the Euclidean Algorithm," The Fibonacci Quarterly, Vol. 4 (1966), pp. 367-368.
2. O. Perron, Die Lehre von den Kettenbruchen, Vol. 1, Teubner, Stuttgart, 1954.
3. J. V. Uspensky and M. A. Heaslet, Elementary Number Theory, McGraw-Hill, 1939.

LETTERS TO THE EDITOR

Dear Editor:

In the paper (*) by W. A. Al-Salam and A. Verma, "Fibonacci Numbers and Eulerian Polynomials," Fibonacci Quarterly, February 1971, pp. 18-22, an error occurs in (9), which is readily corrected. I will generalize their (4) by defining a general polynomial operator M by

$$\text{(I)} \qquad Mf(x) = Af(x + c_1) + Bf(x + c_2), \qquad c_1 \neq c_2 ,$$

where $f(x)$ is a polynomial and A, B, c_1, and c_2 are given numbers. With $D = d/dx$, we note that $M = Ae^{c_1 D} + Be^{c_2 D}$ so that

$$Mf(x) = A\sum_{n=0}^{\infty} \frac{c_1^n}{n!} D^n f(x) + B\sum_{n=0}^{\infty} \frac{c_2^n}{n!} D^n f(x) ,$$

or

$$\text{(II)} \qquad Af(x + c_1) + Bf(x + c_2) = \sum_{n=0}^{\infty} \frac{W_n}{n!} D^n f(x) ,$$

where $W_n = Ac_1^n + Bc_2^n$ is the solution of $W_{n+2} = PW_{n+1} - QW_n$ and $c_1 \neq c_2$ are the roots of $x^2 = Px - Q$. In (*), Eq. (4) is a special case of (I) with $A = \mu$ and $B = 1 - \mu$. There are two cases of (II) to consider:

Case 1. $A + B \neq 0$. If $A = B$, we obtain from (II)

$$\text{(III)} \qquad f(x + c_1) + f(x + c_2) = \sum_{n=0}^{\infty} \frac{V_n}{n!} D^n f(x) ,$$

where $V_0 = 2$, $V_1 = P$, and $V_{n+2} = PV_{n+1} - QV_n$. If c_1 and c_2 are roots of $x^2 = x + 1$,
[Continued on page 71.]