Journal of Algebra, Number Theory: Advances and Applications
Volume 10, Number 1-2, 2013, Pages 29-39

A NOTE ON CERTAIN RELATIONS BETWEEN THE FIBONACCI SEQUENCE AND THE EUCLIDEAN ALGORITHM

NAOTO ONDA

Kaijo School
Okubo 3-6-1
Shinjuku-ku.
Tokyo
Japan
e-mail: n.onda.go20@gmail.com

Abstract

Gabriel Lame gave an upper bound of the number of steps in the Euclidean algorithm. In this paper, we show that for the integer $F(m, n)$ belonging to "Lucas set" and a positive integer less than $F(m, n)$, the maximum number of steps in the Euclidean algorithm is equal to $m + n - 2$.

1. Introduction

Definition 1.1. We define the sequence $\{a_n\}$ as $a_{k+2} = a_{k+1} + a_k$, $a_1 = a_2 = 1$ and define the set $L = \{F(m, n) | F(m, n) = a_m a_{n+1} + a_{m+1} a_n$, $n, m \geq 2\}$. We call it Lucas set.

Remark 1.2. The set L contains Lucas numbers $F(m, 2)$, $F(2, n)$. We write down $F(m, n)$ for some values as follows:

2010 Mathematics Subject Classification: Primary 11A05; Secondary 11B39.

Keywords and phrases: Euclidean algorithm, Fibonacci sequence.

Received December 31, 2013; Revised January 8, 2014

	(1)	2	3	4	5	6	7	8	9	…
(1)	(2)	(3)	(5)	(8)	(13)	(21)	(34)	(55)	(89)	…
2	(3)	4	7	11	18	29	47	76	123	…
3	(5)	7	12	19	31	50	81	131	212	…
4	(8)	11	19	30	49	79	128	207	335	…
5	(13)	18	31	49	80	129	209	338	547	…
6	(21)	29	50	79	129	208	337	545	882	…
7	(34)	47	81	128	209	337	546	883	1429	…
8	(55)	76	131	207	338	545	883	1428	2311	…
9	(89)	123	212	335	547	882	1429	2311	3740	…
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	

Table 1.

Definition 1.3. We define $En(A, B)$ as the number of steps in the Euclidean algorithm to obtain $GCD(A, B)$, where $A > B$ and $A, B \in \boldsymbol{N}$.

Our main result is stated as follows:

Theorem 1.4. *If we fix* $A = F(m, n)$ *with* $m \geq 2$ *and* $n \geq 2$, *then the maximum number of* $En(A, B)$ *is equal to* $m + n - 2$. *Then the numbers* B *are equal to both* $F(m, n-1)$ *and* $F(m-1, n)$. *In particular, for the case* $n = m$, *we have* $B = F(m, n-1) = F(m-1, n)$.

Remark 1.5. $A = F(2, n) = a_2 a_{n+1} + a_3 a_n = a_{n+2} + a_n$ is a Lucas number with $m = 2$.

For reader's convenience, we give a brief example.

Example 1.6. For the case $m = 5$ and $n = 3$, we have

$$A = a_5 a_4 + a_6 a_3 = 5 \times 3 + 8 \times 2 = 31.$$

In this case, we have the following table. From these results, we see that the maximum number of $En(31, B)$ is equal to 6 and the numbers B are 18 and 19.

On the other hand, from Theorem 1.4, we see that the maximum number of $En(31, B)$ is equal to $m + n - 2 = 5 + 3 - 2 = 6$. Moreover, the numbers B are equal to $F(5, 3-1) = a_3a_5 + a_6a_2 = 2 \times 5 + 8 \times 1 = 18$ and $F(5-1, 3) = a_4a_4 + a_5a_3 = 3 \times 3 + 5 \times 2 = 19$.

$En(31, B)$	B
1	1
2	2, 3, 5, 6, 10, 15, 30
3	4, 7, 8, 9, 16, 21, 25, 26, 28, 29
4	11, 14, 22, 23, 24, 27
5	12, 13, 17, 20
6	18, 19

Table 2.

2. Preliminaries

Theorem 2.1 (Lame's theorem)**.** *The number of steps in an application of the Euclidean algorithm never exceeds* 5 *times the number of digits in the lesser.*

The following proposition is one of problems derived from Lame's theorem.

Proposition 2.2. *Assume that the numbers A and B are defined by* $100 > A > B$ *and* $A, B \in \boldsymbol{N}$. *Then the numbers A and B which make* $En(A, B)$ *maximum are* $(A, B) = (89, 55)$.

Proposition 2.3. *For any A and B with* $a_n \leq A < a_{n+1}$, $A < B$ *and* $A, B \in \boldsymbol{N}$, *we obtain the inequality* $En(A, B) \leq n - 2$.

Proof. The minimum number of A with $En(A, B) = n$, $A > B$ and $A, B \in \boldsymbol{N}$ is equal to a_{n+2}. Therefore, for any A and B with $A > B$ and

$A, B \in \boldsymbol{N}$, we see that $En(A, B) = n$ is a necessary condition of $A \geq a_{n+2}$. Hence, we see that $a_n \leq A < a_{n+1}$ is a necessary condition of $En(A, B) \leq n - 2$.

From Proposition 2.3, we see that if $En(A, B) = t$ and there exists A such that $a_{t+2} < A < a_{t+3}$, then the maximum value of $En(A, B)$ is equal to t. If $G(A, B) = 2$, the minimum value of A is equal to $2a_{t+2}$. Then we have $a_{t+3} < 2a_{t+2}$. Therefore, all we have to do is consider the case of $G(A, B) = 1$.

Definition 2.4. For any positive integers A and B, we have the Euclidean algorithm as follows:

$$A = Bq_1 + r_1, \text{ where } 0 < r_1 \leq B,$$

$$B = r_1q_2 + r_2, \text{ where } 0 < r_2 \leq r_1,$$

$$r_1 = r_2q_3 + r_3, \text{ where } 0 < r_3 \leq r_2,$$

$$\vdots$$

$$r_k = r_{k+1}q_{k+2} + r_{k+2}, \text{ where } 0 < r_{k+2} \leq r_{k+1},$$

$$\vdots$$

$$r_{n-2} = r \times q_n + r.$$

In this paper, we substitute $0 < r_{k+1} \leq r_k$ for $0 \leq r_{k+1} < r_k$ in any steps for Euclidean algorithm. We note that $r_{k+1} = r_k$, if and only if $k = n - 1$. Then we define the quantity

$$Q(A, B) = \sum_{k=1}^{n} (q_k - 1).$$

Definition 2.5. We define $(a, b) + (c, d) = (a + c, b + d)$ and also define $A \cdot B = (En(A, B), Q(A, B))$.

Proposition 2.6. *For two positive integers A and B, we have*

$$A \cdot B = \begin{cases} B \cdot (A - B) + (1, 0), & \textit{where } A < 2B, \\ (A - B) \cdot B + (0, 1), & \textit{where } A > 2B, \\ (1, 0), & \textit{otherwise.} \end{cases}$$

Proof. If $A < 2B$, we have

$$A = B \times 1 + (A - B), \text{ where } 0 < (A - B) \leq B,$$

$$B = (A - B) \times q + r, \text{ where } 0 < r \leq (A - B).$$

Therefore, we have

$$A \cdot B = B \cdot (A - B) + (1, 0). \tag{1}$$

For the case $A > 2B$, we have $A = B \times q + r$, where $0 < r \leq B$ and $q > 1$. On the other hand, we have $A - B = B \times (q - 1) + r$, where $0 < r \leq B$. Therefore, we see that

$$A \cdot B = (A - B) \cdot B + (0, 1). \tag{2}$$

Finally, for the case $A = 2B$, we have

$$A = B \times 1 + B, \text{ where } 0 < B \leq B. \tag{3}$$

From (1), (2), and (3), this assertion is proved.

Example 2.7. We can calculate $A \cdot B$ by using Proposition 2.6. For the case $A = 32$ and $B = 25$,

$$\begin{aligned} A \cdot B &= 32 \cdot 25 \\ &= 25 \cdot 7 + (1, 0) \\ &= 18 \cdot 7 + (1, 1) \\ &= 11 \cdot 7 + (1, 2) \end{aligned}$$

$$= 7 \cdot 4 + (2,\ 2)$$

$$= 4 \cdot 3 + (3,\ 2)$$

$$= 3 \cdot 1 + (4,\ 2)$$

$$= 2 \cdot 1 + (4,\ 3)$$

$$= (5,\ 3).$$

Lemma 2.8. *If* $A \cdot B = (t,\ 0)$, *then we have* $A = a_{t+2}$ *and* $B = a_{t+1}$.

Proof.

$$\begin{aligned} A \cdot B &= B \cdot r_1 + (1,\ 0) \\ &= r_1 \cdot r_2 + (2,\ 0) \\ &= \dots \\ &= r_{k-1} \cdot r_k + (k,\ 0) \\ &= \dots \\ &= r_{t-4} \cdot r_{t-3} + (t-3,\ 0) \\ &= r_{t-3} \cdot r_{t-2} + (t-2,\ 0) \\ &= 2 \cdot 1 + (t-1,\ 0) \\ &= (t,\ 0). \end{aligned}$$

From this equality, we have $r_k - r_{k+1} = r_{k+2}$, $r_{t-2} = 2 = a_3$, $r_{t-3} = 3 = a_4$. Therefore, we have $r_k = a_{t-k+1}$. So, we see that $B = r_1 + r_2 = a_t + a_{t-1} = a_{t+1}$ and $A = B + r_1 = a_{t+2}$.

Lemma 2.9. *If* $A \cdot B = (t, 1)$, *then we have* $A = F(m, n)$, *and* $B = F(m-1, n)$, *where* $m + n = t + 2$.

Proof. We have the following equality:

$$\begin{aligned} A \cdot B &= B \cdot s_1 + (1, 0) \\ &= s_1 \cdot s_2 + (2, 0) \\ &= \dots \\ &= s_{m-3} \cdot s_{m-2} + (m-2, 0) \\ &= s_{m-2} \cdot s_{m-1} + (m-1, 0) \\ &= r_{m-2} \cdot s_{m-1} + (m-1, 1) \\ &= r_{m-1} \cdot r_m + (m, 1) \\ &= \dots \\ &= r_{t-4} \cdot r_{t-3} + (t-3, 1) \\ &= r_{t-3} \cdot r_{t-2} + (t-2, 1) \\ &= 2 \cdot 1 + (t-1, 1) \\ &= (t, 1). \end{aligned}$$

In the same way as Lemma 2.8, we have $r_{m-2} = a_{n+1}, r_{m-1} = a_n$. From Proposition 2.6, we have $s_{m-2} - s_{m-1} = r_{m-2} = a_{n+1}, s_{m-1} = r_{m-1} = a_n$. Moreover, by using the equality $s_k - s_{k+1} = s_{k+2}$, we have the following:

$$\begin{aligned} s_{m-3} &= s_{m-2} + s_{m-1} \\ &= a_{n+2} + a_n \\ &= a_2 a_{n+1} + a_3 a_n \\ &= F(2, n), \\ s_{m-4} &= F(3, n), \\ &\vdots \end{aligned}$$

$$s_2 = F(m-3, n),$$

$$s_1 = F(m-2, n),$$

$$B = s_2 + s_1$$

$$= F(m-1, n),$$

$$A = B + s_1$$

$$= F(m, n).$$

Lemma 2.10. *If* $A \cdot B = (t, 2)$, *we have the equality* $A = a_p F(m+1, n) + a_{p+1} F(m, n)$ *and* $B = a_{p-1} F(m+1, n) + a_p F(m, n)$, *where* $m + n + p = t + 2$.

Proof. By using Proposition 2.6, we have

$$\begin{aligned}
A \cdot B &= B \cdot u_1 + (1, 0) \\
&= u_1 \cdot u_2 + (2, 0) \\
&= u_2 \cdot u_3 + (3, 0) \\
&= \dots \\
&= u_{p-3} \cdot u_{p-2} + (p-2, 0) \\
&= u_{p-2} \cdot u_{p-1} + (p-1, 0) \\
&= s_{p-2} \cdot s_{p-1} + (p-1, 1) \\
&= s_{p-1} \cdot s_p + (p, 1) \\
&= \dots \\
&= s_{p+m-3} \cdot s_{p+m-2} + (p+m-2, 1) \\
&= s_{p+m-2} \cdot s_{p+m-1} + (p+m-1, 1) \\
&= r_{p+m-2} \cdot s_{p+m-1} + (p+m-1, 2)
\end{aligned}$$

$$
\begin{aligned}
&= r_{p+m-1} \cdot r_{p+m} + (p+m,\ 2) \\
&= \dots \\
&= r_{t-4} \cdot r_{t-3} + (t-3,\ 2) \\
&= r_{t-3} \cdot r_{t-2} + (t-2,\ 2) \\
&= 2 \cdot 1 + (t-1,\ 2) \\
&= (t,\ 2).
\end{aligned}
$$

In the same way as Lemma 2.9, we have $s_{p-2} = F(m+1,\ n)$, $s_{p-1} = F(m,\ n)$. From Proposition 2.6, we have $u_{p-1} = s_{p-1} = F(m,\ n)$, $u_{p-2} = s_{p-2} + s_{p-1} = F(m+2,\ n)$. Moreover, by using the equality $u_k - u_{k+1} = u_{k+2}$, we have the following:

$$
\begin{aligned}
u_{p-3} &= u_{p-1} + u_{p-2} \\
&= F(m,\ n) + (F(m+1,\ n) + F(m,\ n)) \\
&= a_2 F(m+1,\ n) + a_3 F(m,\ n) \\
u_{p-4} &= F(m,\ n) + 2F(m+2,\ n) \\
&= a_3 F(m+1,\ n) + a_4 F(m,\ n) \\
&\ \vdots \\
u_2 &= a_{p-3} F(m+1,\ n) + a_{p-2} F(m,\ n), \\
u_1 &= a_{p-2} F(m+1,\ n) + a_{p-1} F(m,\ n), \\
B &= u_1 + u_2 \\
&= a_{p-1} F(m+1,\ n) + a_p F(m,\ n), \\
A &= B + u_1 \\
&= a_p F(m+1,\ n) + a_{p+1} F(m,\ n).
\end{aligned}
$$

Lemma 2.11. *For any* $m \geq 2$ *and* $n \geq 2$, *we have* $a_{m+n} \leq F(m, n) < a_{m+n+1}$.

Proof. We have

$$\begin{aligned} a_{m+n} &= a_{m+n-1} + a_{m+n-2} \\ &= (a_{m+n-2} + a_{m+n-3}) + a_{m+n-2} \\ &= 2a_{m+n-2} + a_{m+n-3} \\ &= a_3 a_{m+n-2} + a_2 a_{m+n-3} \\ &= a_4 a_{m+n-3} + a_3 a_{m+n-4} \\ &= \dots \\ &= a_m a_{n+1} + a_{m-1} a_n. \end{aligned}$$

If we substitute $m + 1$ for m, then we have

$$a_{m+n+1} = a_{m+1} a_{n+1} + a_m a_n. \tag{4}$$

On the other hand, we have $a_m a_{n+1} + a_{m-1} a_n \leq a_m a_{n+1} + a_{m+1} a_n < a_{m+1} a_{n+1} + a_m a_n$. By using (4), we obtain $a_{m+n} \leq F(m, n) < a_{m+n+1}$.

Lemma 2.12. *For any* $m \geq 2, n \geq 2,$ *and* $p \geq 2,$ *we have* $a_p F(m + 1, n) + a_{p+1} F(m, n) > a_{t+1}$, *where* $m + n + p = t + 2$.

Proof. By using a character of Fibonacci sequence, we have the following:

$$\begin{aligned} &a_{p+1} F(m, n) + a_p F(m + 1, n) - a_{t+1} \\ &= a_{p+1}(a_m a_{n+1} + a_{m+1} a_n) + a_p F(m + 1, n) - a_{t+1} \\ &= a_m(a_{p+1} a_{n+1}) + a_{m+1}(a_{p+1} a_n) + a_p(a_{m+1} a_{n+1} + a_{m+2} a_n) - a_{t+1} \\ &= a_m(a_{p+1} a_{n+1}) + a_{m+1}(a_{p+1} a_n) + a_p(a_{m+1} a_{n+2} + a_m a_n) - a_{t+1} \end{aligned}$$

$$= a_m(a_{p+1}a_{n+1} + a_p a_n) + a_{m+1}(a_{p+1}a_n + a_p a_{n+2}) - a_{m+n+p-1}$$

$$= a_m a_{p+n+1} + a_{m+1}(a_{p+1}a_n + a_p a_{n+2}) - (a_m a_{p+n} + a_{m-1}a_{p+n-1})$$

$$= a_m(a_{p+n+1} - a_{p+n}) + a_{m+1}(a_{p+n} + 2a_p a_n) - a_{m-1}a_{p+n-1}$$

$$= a_m a_{p+n-1} + a_{m+1}a_{p+n} + 2a_{m+1}a_p a_n - a_{m-1}a_{p+n-1}$$

$$= a_{m+n+p} + (a_m + a_{m-1} + a_{m+1})a_p a_n - a_{m-1}(a_p a_n + a_{p-1}a_{n-1})$$

$$= a_{m+n+p} + a_m a_n a_p + a_{m+1}a_n a_p - (a_{m-1}a_{p-1}a_{n-1})$$

$$= a_{m+n+p} + 2a_m a_n a_p + a_{m-1}(a_n a_p - a_{n-1}a_{p-1})$$

$$> 0.$$

3. A Proof of Main Theorem

By using Lemmas 2.8, 2.9, 2.10, 2.11, and 2.12, we see that if A and B satisfy $En(A, B) = t$ and $a_{t+2} \leq A < a_{t+3}$, then $Q(A, B) = 0$ or 1. From this result and Proposition 2.3, Theorem 1.4 which is our main theorem has proved.

References

[1] R. L. Duncan, Note on the Euclidean algorithm, The Fibonacci Quarterly 4 (1966), 367-68.

[2] R. Honsberger, Mathematical Gems II, Mathematical Assn. of Amer. (1976)

■