ON THE LUCAS PROPERTY OF LINEAR RECURRENT SEQUENCES

HAO ZHONG AND TIANXIN CAI

ABSTRACT. Let $S$ be an arithmetic function. $S$ has Lucas property if for any prime $p$ and $n = \sum_{i=0}^{r} n_i p^i$, where $0 \leq n_i \leq p - 1$,
$$S(n) \equiv S(n_0)S(n_1) \ldots S(n_r) \pmod{p}.$$ (0.1)

In this note, we discuss the Lucas property of Fibonacci sequences and Lucas numbers. Meanwhile, we find some other interesting results.

1. INTRODUCTION

The famous Lucas’ theorem states that
$$\binom{n}{m} \equiv \binom{n_0}{m_0} \binom{n_1}{m_1} \ldots \binom{n_r}{m_r} \pmod{p},$$ (1.1)
where $n, m \in \mathbb{N}$, the base $p$ expansions of $n$ and $m$ are $n = \sum_{i=0}^{r} n_i p^i$, $m = \sum_{i=0}^{r} m_i p^i$ ($0 \leq n_i, m_i \leq p - 1$).

In 1992, Richard J. McIntosh [5] gave a definition of the Lucas property and the double Lucas property, i.e.,

Definition 1.1. Let $S$ be an arithmetic function. $S$ has Lucas property if for any prime $p$ and $n = \sum_{i=0}^{r} n_i p^i$, where $0 \leq n_i \leq p - 1$,
$$S(n) \equiv S(n_0)S(n_1) \ldots S(n_r) \pmod{p}.$$ (1.2)

And let $D$ be a bivariate arithmetic function. $D$ has double Lucas property if for any prime $p$, $n = \sum_{i=0}^{r} n_i p^i$, and $m = \sum_{i=0}^{r} m_i p^i$, where $0 \leq n_i, m_i \leq p - 1$,
$$D(n, m) \equiv D(n_0, m_0)D(n_1, m_1) \ldots D(n_r, m_r) \pmod{p}.$$ (1.3)

Another way of stating this is to say that $S$ is an LP function and $D$ is a DLP function.

There are numerous examples: $a^n$ is an LP function for any rational number $a$; the Apéry numbers $A(n) = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2$ is an LP function (Cf. Gessel [4]); the function $\omega(n)$ defined by
$$\frac{1}{J_0(2z^{1/2})} = \sum_{n=0}^{\infty} \frac{\omega(n) z^n}{(n!)^2}$$
is an LP function (Cf. Carlitz [2]); and according to Lucas’ theorem, the binomial coefficient $D(n, m) = \binom{n}{m}$ is a DLP function.

Moreover, we add another definition.

2010 Mathematics Subject Classification. 11B50, 11B39.
Key words and phrases. Lucas property, Fibonacci sequences, Lucas numbers, linear recurrent sequences.
Definition 1.2. Let $S$ be an arithmetic function. $S$ has Lucas property with the prime $p$ if for any $n = \sum_{i=0}^{r} n_ip^i$, where $0 \leq n_i \leq p - 1$,

$$S(n) \equiv S(n_0)S(n_1)\ldots S(n_r) \pmod{p}.$$  

(1.4)

It can be said that $S$ is an LP function with the prime $p$.

In this paper, we discuss the Lucas property of Fibonacci and Lucas numbers.

Let $F_n$ be the Fibonacci sequence, i.e., $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$ ($n \geq 2$), and $L_n$ be the Lucas numbers $L_n = 2, L_1 = 1, L_n = L_{n-1} + L_{n-2}$ ($n \geq 2$).

We obtain the following theorems.

**Theorem 1.1.** Let $a, b$ be two positive integers. Then $S(n) = F_{an+b}$ is an LP function with the prime $p$ if and only if

$$\begin{cases} F_a \equiv 0 \pmod{p}, \\ F_b \equiv 1 \pmod{p}. \end{cases}$$

(1.5)

For Lucas numbers, we have

**Theorem 1.2.** Let $a, b$ be two positive integers. Then $S(n) = L_{an+b}$ is an LP function with the prime $p$ if and only if

$$\begin{cases} 5F_a \equiv 0 \pmod{p}, \\ F_b \equiv 1 \pmod{p}. \end{cases}$$

(1.6)

From these two theorems, we can obtain some corollaries.

**Corollary 1.1.** Let $a$ and $b$ be positive integers. Then $S(n) = F_{an+b}$ is not an LP function and $L_{an+b}$ is not an LP function.

**Proof.** The proof is by contradiction. Let $a$ and $b$ be positive integers such that $S(n) = F_{an+b}$ is an LP function. Then by Theorem 1.1, $p$ divides $F_a$ for any prime $p$, a contradiction. A similar proof follows for $S(n) = L_{an+b}$. □

**Corollary 1.2.** Let $p = 5$. Then for any positive integer $a$,

(1) $S(n) = F_{5an+b}$ is an LP function with the prime 5, where $b \equiv 1, 2, 8$ or 19 (mod 20).

(2) $S(n) = L_{an+b}$ is an LP function with the prime 5, where $b \equiv 1$ (mod 4).

**Corollary 1.3.** Let $p$ be a Fibonacci prime, namely, there exists a positive integer $a$ such that $F_a = p$. Then $F_{an+1}$ is an LP function with the prime $p$ and $L_{an+1}$ is an LP function with the prime $p$.

More generally, let $\alpha(p) := \min\{n | p \text{ divides } F_n\}$ for a prime $p$. Then we have

**Corollary 1.4.** The condition $F_a \equiv 0 \pmod{p}$ in Theorem 1.1 can be replaced by $a = \alpha(p)k$, where $k$ is an arbitrary positive integer. And if $p \neq 5$, the condition $5F_a \equiv 0 \pmod{p}$ in Theorem 1.2 can also be replaced by $a = \alpha(p)k$, where $k$ is an arbitrary positive integer.
Proof. For any integers $m, n$, $gcd(F_m, F_n) = F_{gcd(m,n)}$. Hence, $gcd(F_a, F_{\alpha(p)}) = F_{gcd(a,\alpha(p))}$. And if $F_a \equiv 0 \pmod{p}$, then $p|F_{gcd(a,\alpha(p))}$. From the definition of $\alpha(p)$, we obtain that $gcd(a, \alpha(p)) = \alpha(p)$. So, $a = \alpha(p)k$ for some integer $k$.

Similarly, for any positive integer $k$, $gcd(F_{\alpha(p)k}, F_{\alpha(p)}) = F_{gcd(\alpha(p)k, \alpha(p))}$. Hence, $F_{\alpha(p)k} \equiv 0 \pmod{p}$.

A natural extension of these two theorems is to look at the Lucas property of general linear recurrent sequences. We obtain an analogous result to the two theorems above.

**Theorem 1.3.** Let $A_n$ be a linear recurrent sequence, i.e., $\{A(n)\}$ satisfies the linear recurrent relation:

$$A_n = uA_{n-1} + vA_{n-2} \quad (n \geq 2),$$

where $A_0, A_1, u$ and $v$ are all integers. Then for any integers $a$ and $b$, $S(n) = A_{an+b}$ is an LP function with the prime $p$ if and only if

$$\begin{align*}
\text{vs}(a-1, u, v)(vA_0^2 + uA_0A_1 - A_1^2) & \equiv 0 \pmod{p}, \\
A_b & \equiv 1 \pmod{p}.
\end{align*}$$

(1.7)

where

$$s(k, u, v) = \sum_{i=0}^{[k/2]} \binom{k-i}{i} u^{k-2i} v^i.$$

When it comes to the generalizations of Fibonacci numbers, we obtain two more corollaries.

**Corollary 1.5.** Let $\{A_n\}$ be an Lucas sequence or $(P, -Q)$-Fibonacci sequence, that is, $A_0 = 0$, $A_1 = 1$ $u = P$, and $v = -Q$. Then for any integers $a$ and $b$, $S(n) = A_{an+b}$ is an LP function with the prime $p$ if and only if

$$\begin{align*}
Qs(a-1, P, -Q)A_1^2 & \equiv 0 \pmod{p}, \\
A_b & \equiv 1 \pmod{p}.
\end{align*}$$

(1.8)

In particular, when $\{A_n\}$ are Pell numbers, $S(n) = A_{an+b}$ is an LP function with the prime $p$ if and only if

$$\begin{align*}
s(a-1, 2, 1) & \equiv 0 \pmod{p}, \\
A_b & \equiv 1 \pmod{p}.
\end{align*}$$

(1.9)

Another famous generalization of Fibonacci numbers is Fibonacci word, which is in the case of $u = v = 1$. Similarly, we have

**Corollary 1.6.** Let $\{A_n\}$ be Fibonacci words. Then for any integers $a$ and $b$, $S(n) = A_{an+b}$ is an LP function with the prime $p$ if and only if

$$\begin{align*}
F_a(A_0^2 + A_0A_1 - A_1^2) & \equiv 0 \pmod{p}, \\
A_b & \equiv 1 \pmod{p}.
\end{align*}$$

(1.10)

where $F_a$ is the $a$th Fibonacci number.
2. Preliminaries

For a fixed prime $p$, the following two corollaries from McIntosh [5] will be needed.

**Lemma 2.1.** Let $S(n)$ be an LP function with the prime $p$, which is not identically zero. Then $S(0) \equiv 1 \pmod{p}$.

**Lemma 2.2.** $S(n)$ is an LP function with the prime $p$, and $S(n)$ is periodic modulo $p$ if and only if $S(n) \equiv S(1)^n \pmod{p}$.

Meanwhile, we can get the following lemma by induction on $n$.

**Lemma 2.3.** Let $n$ be a positive integer. Then

(1) $F_n \equiv n 3^{n-1} \pmod{5}$. \hfill (2.1)

(2) $L_n \equiv 3^{n-1} \pmod{5}$. \hfill (2.2)

**Remarks.** By using Lemma 2.2 and Lemma 2.3, we can find some LP functions with the prime 5,

(1) $S(n) = F_{5n+b}$ is an LP function with the prime 5, where $b \equiv 1, 2, 8 \text{ or } 19 \pmod{20}$.

(2) $S(n) = L_{n+1}$ is an LP function with the prime 5.

In order to get the theorems, we need one more lemma.

**Lemma 2.4.** Let $n, r$ be two integers. Then

(1) (Catalan’s identity)
\[
F_n^2 - F_{n+r}F_{n-r} = (-1)^{n-r} \cdot F_r^2.
\] \hfill (2.3)

(2)
\[
L_{n+r}L_{n-r} - L_n^2 = (-1)^{n-r} \cdot 5F_r^2.
\] \hfill (2.4)

(3)
\[
A_{n+r}A_{n-r} - A_n^2 = (-v)^{n-r} s^2(r-1, u, v)(vA_0^2 + uA_0A_1 - A_1^2).
\] \hfill (2.5)

**Proof of (2.4).** We prove it by using the determinant of the matrix and the fact that
\[
\begin{align*}
L_{n+r} &= F_{r+1}L_n + F_rL_{n-1}, \\
L_n &= F_{r+1}L_{n-r} + F_rL_{n-r-1}.
\end{align*}
\]

Hence,
\[
L_{n+r}L_{n-r} - L_n^2 = \begin{vmatrix} L_{n+r} & L_n \\ L_n & L_{n-r} \end{vmatrix} = \begin{vmatrix} F_{r+1}L_n + F_rL_{n-1} & L_n \\ F_{r+1}L_{n-r} + F_rL_{n-r-1} & L_{n-r} \end{vmatrix} = F_r \begin{vmatrix} L_{n-1} & L_n \\ L_{n-r-1} & L_{n-r} \end{vmatrix} = F_r \begin{vmatrix} L_{n-1} & L_{n-2} \\ L_{n-r-1} & L_{n-r-2} \end{vmatrix} = \ldots
\]
So, (2.4) is true. □

**Proof of (2.5).** To prove (2.5), we first prove that

$$A_{n+r} = s(k, u, v)A_{n+r-k} + t(k, u, v)A_{n+r-k-1},$$

(2.6)

where

$$s(k, u, v) = \sum_{i=0}^{\lfloor \frac{k-1}{2} \rfloor} {k-i \choose i} u^{k-2i} v^i$$

and

$$t(k, u, v) = \sum_{j=0}^{\lfloor \frac{k-1}{2} \rfloor} (k-1-j) u^{k-1-2j} v^{j+1}.$$  

For $k = 1$, (2.6) holds. By inducting on $k$, we can obtain the result. Assume for $k = 1, 2, \ldots, m$, (2.6) holds. For $k = m + 1$, 

$$A_{n+r} = s(m, u, v)A_{n+r-m} + t(m, u, v)A_{n+r-m-1}$$

$$= \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m-i}{i} u^{m-2i} v^i A_{n+r-m} + \sum_{j=0}^{\lfloor \frac{m-1}{2} \rfloor} \binom{m-1-j}{j} u^{m-1-2j} v^{j+1} A_{n+r-m-1}$$

$$= \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m-i}{i} u^{m+1-2i} v^i (u A_{n+r-m-1} + v A_{n+r-m-2}) + \sum_{j=0}^{\lfloor \frac{m-1}{2} \rfloor} \binom{m-1-j}{j} u^{m-1-2j} v^{j+1} A_{n+r-m-1}$$

$$= \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m-i}{i} u^{m+1-2i} v^i A_{n+r-m-1} + \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m-i}{i} u^{m-2i} v^{i+1} A_{n+r-m-2}$$

$$= \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m-i}{i} u^{m+1-2i} v^i + \sum_{j=0}^{\lfloor \frac{m-1}{2} \rfloor} \binom{m-1-j}{j} u^{m-1-2j} v^{j+1} A_{n+r-m-1} + t(m + 1, u, v) A_{n+r-m-2}$$

If $m \equiv 0 \pmod{2}$,

$$\sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m-i}{i} u^{m+1-2i} v^i + \sum_{j=0}^{\lfloor \frac{m-1}{2} \rfloor} \binom{m-1-j}{j} u^{m-1-2j} v^{j+1}$$

$$= \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m-i}{i} u^{m+1-2i} v^i + \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m-i}{i} u^{m+1-2i} v^i$$

$$= u^{m+1} + \sum_{i=1}^{m} \left( \binom{m-i}{i} + \binom{m-i}{i-1} \right) u^{m+1-2i} v^i$$
\[ u^{m+1} + \sum_{i=1}^{\lfloor m/2 \rfloor} \binom{m + 1 - i}{i} u^{m+1-2i} v^i \\
= s(m + 1, u, v). \]

If \( m \equiv 1 \pmod{2} \),
\[
\sum_{i=0}^{\lfloor (m - 1)/2 \rfloor} \binom{m - i}{i} u^{m+1-2i} v^i + \sum_{j=0}^{\lfloor (m - 1)/2 \rfloor} \binom{m - 1 - j}{j} u^{m+1-2j} v^{j+1} \\
= v^{\frac{m+1}{2}} + \sum_{i=0}^{\lfloor (m - 1)/2 \rfloor} \binom{m - i}{i} u^{m+1-2i} v^i \\
= v^{\frac{m+1}{2}} + \sum_{i=0}^{\lfloor (m - 1)/2 \rfloor} \binom{m + 1 - i}{i} u^{m+1-2i} v^i \\
= s(m + 1, u, v). \]

Hence, \( A_{n+r} A_{n-r} - A_n^2 = (-1)^{n-r} v^{n-r-1} t(r, u, v)(A_{r+1} A_0 - A_r A_1) \).

By using (2.6) and the fact \( t(r, u, v) = vs(r - 1, u, v) \), we have
\[
A_{n+r} A_{n-r} - A_n^2 = (-1)^{n-r} v^{n-r-1} t(r, u, v)(A_{r+1} A_0 - A_r A_1) \\
= (-1)^{n-r} v^{n-r-1} t(r, u, v)(t(r, u, v)A_0^2 - s(r - 1, u, v)A_0^2 + s(r, u, v)A_1 A_0 - t(r - 1, u, v)A_0 A_1) \\
= (-v)^{n-r} s(r - 1, u, v)(vs(r - 1, u, v)A_0^2 - s(r - 1, u, v)A_1^2 + s(r, u, v)A_1 A_0 - vs(r - 2, u, v)A_0 A_1) \\
= (-v)^{n-r} s^2(r - 1, u, v)(vA_0^2 + uA_0 A_1 - A_1^2). \\
\]
So, (2.5) is true. \( \square \)

3. PROOFS OF THE THEOREMS

**Proof of Theorem 1.1.** The Fibonacci numbers are periodic modulo \( p \) for any prime \( p \).
So is \( S(n) = F_{an+b} \), where \( a, b \) are positive integers.

We first prove the necessity. Assume that \( S(n) = F_{an+b} \) is an LP function with the prime \( p \). From Lemma 2.1, \( S(0) \equiv 1 \pmod{p} \), so \( F_b \equiv 1 \pmod{p} \). And from Lemma 2.2, for any positive integer \( n \), \( F_{an+b} \equiv F_{an+b}^p \pmod{p} \). Set \( n = 2, F_{2a+b} \equiv F_{2a+b}^2 \pmod{p} \). By using Catalan’s identity (2.3), we have
\[
F_{a+b+a} F_{a+b-a} = F_{a+b}^2 - (-1)^{a+b-a} F_a^2 \\
F_{2a+b} F_b = F_{a+b}^2 - (-1)^b F_a^2 \]
Hence, \( a \) and \( b \) satisfy
\[
\begin{cases}
F_a \equiv 0 \pmod{p} \\
F_b \equiv 1 \pmod{p}
\end{cases}
\]

Next we prove the sufficiency. From Lemma 2.2, we have to prove that
\[
S(n) \equiv S(1)^n \pmod{p}.
\] (3.1)

And we’ll prove it by induction on \( n \). For \( n = 1 \), it’s obviously true. Assume that for \( n \leq k \), (3.1) holds. For \( n = k + 1 \), by using Catalan’s identity (2.3), we have
\[
\begin{align*}
F_{a+b} &\equiv F_{a+b} - (-1)^b F_a ^2 \pmod{p} \\
F_a ^2 &\equiv 0 \pmod{p} \\
F_a &\equiv 0 \pmod{p}.
\end{align*}
\]

Hence, (3.1) holds for any positive integer \( n \). And \( F_{an+b} \) is an LP function with the prime \( p \).

Proof of Theorem 1.2. The proof is similar to Theorem 1.1. Lucas number is periodic modulo \( p \) for any prime \( p \). So is \( S(n) = L_{an+b} \), where \( a \) and \( b \) are positive integers. We first prove the necessity. Assume that \( S(n) = L_{an+b} \) is an LP function with the prime \( p \). From Lemma 2.1, \( S(0) \equiv 1 \pmod{p} \), so \( L_b \equiv 1 \pmod{p} \). And from Lemma 2.2, for any positive integer \( n \), \( L_{an+b} \equiv L_{a+b} ^n \pmod{p} \). Set \( n = 2 \), \( L_{2a+b} \equiv L_{a+b} ^2 \pmod{p} \). By using (2.4), we have
\[
\begin{align*}
L_{a+b} ^{2a+b} L_{a+b} ^{a-b-a} &= L_{a+b} ^2 + (-1)^{a+b-a} \cdot 5F_a ^2 \\
L_{2a+b} L_b &= L_{a+b} ^2 + (-1)^b \cdot 5F_a ^2 \\
L_{2a+b} ^2 &\equiv L_{a+b} ^2 + (-1)^b \cdot 5F_a ^2 \pmod{p} \\
5F_a ^2 &\equiv 0 \pmod{p} \\
5F_a &\equiv 0 \pmod{p}.
\end{align*}
\]

Hence, \( a \) and \( b \) satisfy
\[
\begin{cases}
5F_a \equiv 0 \pmod{p} \\
L_b \equiv 1 \pmod{p}
\end{cases}
\]

Next we prove the sufficiency. From Lemma 2.2, we also have to prove that (3.1) is true. And we’ll prove it by induction on \( n \). For \( n = 1 \), it’s obviously true. Assume that for \( n \leq k \), (3.1) holds. For \( n = k + 1 \), by using (2.4), we have
\[
\begin{align*}
L_{a+b} ^{2a+b} L_{a+b} ^{a+b-a} &= L_{a+b} ^2 + (-1)^{a+b-a} \cdot 5F_a ^2 \\
L_{a(k+1)+b} L_{a(k-1)+b} &= L_{a+b} ^2 + (-1)^{a(k-1)+b} \cdot 5F_a ^2 \\
L_{a(k+1)+b} ^{k-1} L_{a+b} ^{a+b} &\equiv L_{a+b} ^2 + (-1)^{a(k-1)+b} \cdot 5F_a ^2 \pmod{p} \\
L_{a(k+1)+b} ^{k+1} &\equiv L_{a+b} ^{k+1} \pmod{p}.
\end{align*}
\]
Hence, (3.1) holds for any positive integer $n$. And $L_{an+b}$ is an LP function with the prime $p$. □

Proof of Theorem 1.3. From [3] and [6], we know that for any integer $m$, a linear recurrent sequence of integers modulo $m$ is periodic. The same is true for a prime $p$. Hence $S(n) = A_{an+b}$ is periodic modulo $p$. To obtain the proof it is enough to apply the reasoning just like in the proofs of Theorem 1.1 and Theorem 1.2. □

Acknowledgments. This work is supported by the National Natural Science Foundation of China (Grant No. 11501052 and Grant No. 11571303).

References

1. T. Cai, The Book of Numbers, World Scientific Publishing Co., 2016.
2. L. Carlitz, The coefficients of the reciprocal of $J_0(x)$, Arch. Mat. 6 (1955), no. 6, 121–127.
3. R. D. Carmichael, On sequences of integers defined by recurrence relations, Quart. Jour. Math. 48 (1920), 343–372.
4. I. Gessel, Some congruences for Apéry numbers, J. Number Theory 14 (1982), no. 3, 362–368.
5. R. McIntosh, A generalization of a congruential property of Lucas, Amer. Math. Monthly 99 (1992), no. 3, 231–238.
6. D. W. Robinson, A Note on Linear Recurrent Sequences Modulo m, Amer. Math. Monthly 73 (1966), no. 6, 619–621.

(H. Zhong) School of Mathematical Sciences, Zhejiang University, Hangzhou, 310027, China
E-mail address: 11435011@zju.edu.cn

(T. Cai) School of Mathematical Sciences, Zhejiang University, Hangzhou, 310027, China
E-mail address: txcai@zju.edu.cn