Elem. Math. 73 (2018) 151 – 160
0013-6018/18/040151-10
DOI 10.4171/EM/368

Elemente der Mathematik

The Lucas property for linear recurrences of second order

Carsten Elsner and Jürgen Spilker

Jürgen Spilker, Jahrgang 1935, studierte und promovierte an der Universität Göttingen und arbeitete an der Universität in Freiburg (Breisgau) bis zu seinem Ruhestand 2001. Seine Forschungsgebiete sind die automorphen Formen, die zahlentheoretischen Funktionen sowie Probleme der elementaren Zahlentheorie. Sein Hobby ist die Geschichte der deutschen Post.

Carsten Elsner, Jahrgang 1961, studierte, promovierte und habilitierte sich an der ehemaligen Universität Hannover, heute Gottfried Wilhelm Leibniz Universität Hannover. Er forscht seit 1988 in der Zahlentheorie mit den Schwerpunkten diophantische Approximation und Transzendenztheorie. Nach einem kurzen Ausflug als versicherungsmathematischer Gutachter kehrte er 2003 an eine Hochschule zurück und arbeitet seitdem an der FHDW Hannover im Institut für Informatik und Wirtschaftsinformatik als Dozent für Mathematik.

Die Lucas-Eigenschaft modulo einer Primzahl p stellt eine Verbindung her zwischen allen Funktionswerten $f(n)$ einer Funktion $f : \mathbb{N} \to \mathbb{N}$ und dem Produkt $f(n_0)f(n_1) \cdots f(n_r)$, wobei die $n_0, \ldots, n_r$ die Ziffern der p-adischen Entwicklung von n sind, nämlich

$$f(n) \equiv f(n_0)f(n_1)\cdots f(n_r) \pmod{p} \quad (n \geq 1).$$

Diese Eigenschaft kommt jeder Exponentialfunktion $f(n) = c^n$ mit $c \in \mathbb{N}$ und jeder Primzahl p zu. Erstmalig wurde eine solche Beziehung 1878 von E. Lucas für Binomialkoeffizienten aufgestellt. In der vorliegenden Arbeit werden Funktionen g betrachtet, die einer linearen Rekursion zweiter Ordnung mit konstanten Koeffizienten genügen. Sollte eine solche Funktion g die Lucas-Eigenschaft modulo p noch nicht haben, so folgen die Autoren einer in der Zahlentheorie gängigen Vorgehensweise, indem sie die auf arithmetischen Progressionen beruhenden Teilfolgen $f(n) := g(an+b)$ betrachten und charakterisieren, wann f wieder die Lucas-Eigenschaft modulo p hat. Dies haben in einer kürzlich erschienenen Arbeit bereits H. Zhong und T. Cai für die Fibonacci-Funktion $F(n)$ getan. So hat etwa $f(n) = F(4n+7)$ die Lucas-Eigenschaft modulo 3. In dieser Arbeit wird gleichzeitig das Konzept der Lucas-Eigenschaft von den Primzahlen auf die Carmichael-Zahlen erweitert, die ja bekanntlich eine bedeutende Rolle in der Kryptographie spielen.

1 Introduction

Let p be a fixed prime number. It is well known that every positive integer n can be expressed by a p-adic representation, i.e.,

$$n = \sum_{0\le i\le r} n_i p^i \qquad (0 \le n_i < p)\,. \tag{1.1}$$

A real function $f : \mathbb{N}_0 \to \mathbb{Z}$ is said to fulfill the *Lucas property modulo p* if the following two conditions are satisfied, cf. [6].

1.) $$f(0) \equiv 1 \pmod{p}\,,$$

2.) $$f(n) \equiv \prod_{0\le i\le r} f(n_i) \pmod{p} \qquad (n \ge 1)\,.$$

For every integer k and every prime number p the exponential function $f(n) = k^n$ has the Lucas property modulo p. When p divides k it is trivial, and for all integers k which are coprime with p the Lucas property is a consequence of Fermat's little theorem, because $p^i = \big((p-1)+1\big)^i \equiv 1 \pmod{p-1}$ for $i \ge 0$ gives

$$\begin{aligned} f(n) &= k^{n_0+n_1 p+\cdots+n_r p^r} = k^{n_0} k^{n_1 p} \cdots k^{n_r p^r} \\ &\equiv k^{n_0} k^{n_1} \cdots k^{n_r} = f(n_0) f(n_1) \cdots f(n_r) \pmod{p}\,. \end{aligned}$$

Two rules follow immediately from the definition of the Lucas property modulo p, namely,

$$f(m) \equiv f\big(mp^\alpha\big) \pmod{p} \qquad (m \ge 0,\ \alpha \ge 0)\,, \tag{1.2}$$

and

$$f(m'+m'') \equiv f(m') f(m'') \pmod{p}\,, \tag{1.3}$$

if the p-adic representations of m' and m'' are

$$m' = \sum_{0\le i_1\le j} m_{i_1} p^{i_1} \quad \text{and} \quad m'' = \sum_{i_2 > j} m_{i_2} p^{i_2}\,.$$

Recently, Zhong and Cai [7] applied the concept of the Lucas property to the Fibonacci numbers $F(n)$. They proved that the function $f(n) := F(an+b)$, where a, b are positive integers, has the Lucas property for a prime p if and only if the congruences $F(a) \equiv 0 \pmod{p}$ and $F(b) \equiv 1 \pmod{p}$ hold. Some more examples of functions with the Lucas property are contained in [7].

Lucas himself [5] applied the concept to binomial coefficients. From his result we obtain the striking congruence

$$\binom{n}{m} \equiv \prod_{0\le i\le r} \binom{n_i}{m_i} \pmod{p}\,, \tag{1.4}$$

where the numbers n_i and m_i are the p-adic coefficients of n and m, respectively, given by (1.1). Here, the specific Lucas property occurs for the first time, generalized to two variables m and n. More precisely, Lucas proved the following theorem.

Theorem A (E. Lucas, [5]). *If p is a prime, n, r, n_0, and r_0 are nonnegative integers, and n_0 and r_0 are both less than p, then*

$$\binom{np+n_0}{rp+r_0} \equiv \binom{n}{r}\binom{n_0}{r_0} \pmod{p}\,.$$

If n and m are given by their p-adic representation, the iterated application of Theorem A gives the result of (1.4).

Example 1.

$$\binom{123}{12} = \binom{2\cdot 7^2+3\cdot 7+4}{0\cdot 7^2+1\cdot 7+5} \equiv \binom{2}{0}\binom{3}{1}\binom{4}{5} = 0 \pmod{7}\,,$$
$$\binom{123}{10} = \binom{2\cdot 7^2+3\cdot 7+4}{0\cdot 7^2+1\cdot 7+3} \equiv \binom{2}{0}\binom{3}{1}\binom{4}{3} \equiv 5 \pmod{7}\,.$$

Variations of Lucas' result in Theorem A are obtained by Bailey [2].

The subject of this note is to prove two sufficient and necessary criterions for the Lucas property of functions satisfying a second-order linear recurrence relation. At the same time we generalize the concept to Carmichael numbers. For the sake of simplicity we denote Carmichael numbers again by p. A Carmichael number p is an odd composite number satisfying the congruence

$$r^{p-1} \equiv 1 \pmod{p} \tag{1.5}$$

for all integers r which are coprime with p. Carmichael numbers are squarefree; the smallest Carmichael number is $561 = 3\cdot 11\cdot 17$. In 1994 it was proven by W. Alford, A. Granville, and C. Pomerance [1] that there exist infinitely many Carmichael numbers. For some elementary properties of these numbers we refer the reader to the book of O. Forster [3]. In (1.1) we may suppose that p is a Carmichael number, and we define the Lucas property modulo p in the same way as for a prime p. Moreover, the above formulas (1.2) and (1.3) remain valid if p is a Carmichael number.

2 The main theorem

Throughout this paper p either denotes a fixed prime number or a fixed Carmichael number, and u, v are fixed integers. Let $g : \mathbb{N}_0 \to \mathbb{Z}$ be a solution of the linear recurrence formula

$$g(n+2) = ug(n+1) + vg(n) \qquad (n \geq 0)\,. \tag{2.1}$$

Moreover, set

$$d := g(2)g(0) - g^2(1) = ug(0)g(1) + vg^2(0) - g^2(1)\,.$$

Theorem 1. *Let $(v, p) = 1$ and $(d, p) = 1$. Moreover, let $f(n) := g(an+b)$ for nonnegative integers a, b. In the case when p is a Carmichael number, we additionally presume that $\big(f(1), p\big) = 1$. Then the following three statements about the function $f(n)$ are equivalent.*

(i) $f(n)$ *has the Lucas property modulo* p.

(ii) $g(b) \equiv 1 \pmod{p}$ *and* $g(0)g(a+1) \equiv g(1)g(a) \pmod{p}$.

(iii) $f(n) \equiv f^n(1) \pmod{p}$ *holds for all integers* $n \geq 0$.

From this theorem the above-mentioned result of Zhong and Cai for the Fibonacci sequence $F(n) = g(n)$ with $F(0) = 0$, $F(1) = 1$, and $u = v = 1$, can be rediscovered in the case of primes p. This follows from the equivalence between (i) and (ii).

We organize our paper as follows. In Section 3 we present more applications of Theorem 1. In order to prove the main result in Section 6, we need a lemma, which will be treated in Sections 4 and 5.

3 Applications of the main theorem

1.) We apply Theorem 1 to the difference of two exponential functions. Let k and l be two different integers, and set $g(n) := k^n - l^n$. It can easily be seen that (2.1) is fullfilled by

$$g(n+2) = (k+l)g(n+1) - klg(n) \qquad (n \geq 0)\,.$$

Next, let p be either a prime number or a Carmichael number such that p and $kl(k-l)$ are coprime. Then the conditions of the coprimality of p and $v = -kl$ as well as the coprimality of p and $d = -(k-l)^2$ in Theorem 1 are satisfied. Thus the theorem guarantees the Lucas property modulo p for every function $f(n) = g(an+b)$ with positive integers a, b if and only if the two congruences

$$k^b - l^b \equiv 1 \pmod{p} \quad \text{and} \quad k^a - l^a \equiv 0 \pmod{p} \tag{3.1}$$

hold; note that $g(0) = 0$ and $g(1) = k - l \not\equiv 0 \pmod{p}$.

2.) The congruences from (3.1) allow to construct more concrete examples. Let $k = 7$, $l = -3$, $p = 41$, $a = 10$, and $b = 3$. One easily checks that the congruences in (3.1) are fulfilled as well as the condition $kl(k-l) \not\equiv 0 \pmod{p}$. Hence, the function

$$f(n) := 7^{10n+3} - (-3)^{10n+3} = 7^{10n+3} + 3^{10n+3} \qquad (n \geq 0)$$

has the Lucas property modulo 41. Moreover, it turns out that the function $f(n) \pmod{41}$ is periodic, namely, for $m \geq 0$ we obtain

$$\begin{aligned} f(4m) &\equiv 1 \pmod{41}\,,\\ f(4m+1) &\equiv 9 \pmod{41}\,,\\ f(4m+2) &\equiv 40 \pmod{41}\,,\\ f(4m+3) &\equiv 32 \pmod{41}\,. \end{aligned}$$

Even the function $f(n)$ satisfies a linear recurrence formula of order two, namely

$$f(n+2) = 282534298f(n+1) - 16679880978201f(n) \qquad (n \geq 0)\,.$$

In the general case, if $g(n)$ satisfies the recurrence formula (2.1), the function $f(n) = g(an+b)$ satisfies a linear second-order recurrence formula, too, namely

$$f(n+2) \;=\; P_a(u,v)\,f(n+1) + (-1)^{a-1}v^a\,f(n) \qquad (n \geq 0)\,,$$

where $P_a(u,v)$ is an integer polynomial of total degree a. In the case just considered we have $u = 4$, $v = 21$, and the polynomial

$$P_{10}(u,v) \;:=\; (u^2+2v)(u^8+8u^6v+19u^4v^2+12u^2v^3+v^4)\,.$$

For $a = 1, 2, 3, 4$ the polynomials $P_a(u,v)$ are given by

$$\begin{aligned} P_1(u,v) &= u\,,\\ P_2(u,v) &= u^2+2v\,,\\ P_3(u,v) &= u^3+3uv\,,\\ P_4(u,v) &= u^4+4u^2v+2v^2\,. \end{aligned}$$

3.) Let $k = 41$, $l = -20$, $a = 40$, and $b = 29$. Then, (3.1) is fulfilled for the smallest Carmichael number $p = 561$, such that the function

$$f(n) \;:=\; 41^{40n+29} + 20^{40n+29} \qquad (n \geq 0)$$

has the Lucas property modulo 561. Note that $\big(f(1), 561\big) = 1$ because $41^{69}+20^{69}$ is not divisible by 3, 11, and 17. Here the periodicity of $f(n)$ mod 561 is given by

$$\begin{aligned} f(2m) &\equiv \;\; 1 \pmod{561}\,,\\ f(2m+1) &\equiv 67 \pmod{561} \end{aligned}$$

for all integers $m \geq 0$.

4 An auxiliary result

Let $g : \mathbb{N}_0 \to \mathbb{Z}$ be a function satisfying (2.1) with $d \neq 0$. Moreover, we introduce the matrices

$$\mathbf{C} \;:=\; \begin{pmatrix} u & v \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \mathbf{G}(n) \;:=\; \begin{pmatrix} g(n+1) & g(n) \\ g(n) & g(n-1) \end{pmatrix} \quad (n \geq 1)\,.$$

Hence, the recurrence formula (2.1) can be expressed by $\mathbf{G}(n+1) = \mathbf{C}\mathbf{G}(n)$ for all integers $n \geq 1$. Consequently the iterated process yields

$$\mathbf{G}(n+1) \;=\; \mathbf{C}^2\mathbf{G}(n-1) \;=\; \cdots \;=\; \mathbf{C}^n\mathbf{G}(1) \qquad (n \geq 0)\,. \tag{4.1}$$

Since

$$\det \mathbf{G}(1) \;=\; g(2)g(0) - g^2(1) \;=\; d \;\neq\; 0\,,$$

there exists the inverse matrix

$$\mathbf{G}^{-1}(1) \;=\; \frac{1}{d}\begin{pmatrix} g(0) & -g(1) \\ -g(1) & g(2) \end{pmatrix}.$$

Applying (4.1) three times, we obtain for positive integers n, m

$$\begin{aligned}\mathbf{G}(n+m) &= \mathbf{C}^{n+m-1}\mathbf{G}(1) \;=\; \mathbf{C}^{n-1}\mathbf{G}(1)\mathbf{G}^{-1}(1)\mathbf{C}^{m}\mathbf{G}(1)\\ &= \mathbf{G}(n)\mathbf{G}^{-1}(1)\mathbf{G}(m+1)\\ &= \mathbf{G}(n)\mathbf{H}(m)\,,\end{aligned} \tag{4.2}$$

where

$$\mathbf{H}(m) \;:=\; \mathbf{G}^{-1}(1)\mathbf{G}(m+1) \;=:\; \begin{pmatrix} \star & x \\ \star & y \end{pmatrix} \tag{4.3}$$

with

$$\left.\begin{aligned} x &= \frac{1}{d}\big(g(0)g(m+1) - g(1)g(m)\big)\,,\\ y &= \frac{1}{d}\big(g(2)g(m) - g(1)g(m+1)\big)\,. \end{aligned}\right\} \tag{4.4}$$

The element $g(n+m)$ in the first row and second column of the matrix $\mathbf{G}(n+m)$ can be expressed using (4.2) and (4.3),

$$g(n+m) \;=\; xg(n+1) + yg(n)\,. \tag{4.5}$$

The above preliminaries will be useful in the subsequent Section 5 in order to prove the following lemma.

Lemma 1. *Let $g : \mathbb{N}_0 \to \mathbb{Z}$ be a function satisfying* (2.1) *with $d \neq 0$. Then we have for all integers n, m with $n \geq m \geq 0$ the identity*

$$g(n+m)g(n-m) - g^2(n) \;=\; \frac{1}{d}(-v)^{n-m}\big(g(0)g(m+1) - g(1)g(m)\big)^2\,.$$

Remark 1. In the case of Fibonacci numbers $g(n) = F(n)$ the equation in Lemma 1 reduces to Catalan's identity, namely

$$F^2(n) - F(n+m)F(n-m) \;=\; (-1)^{n-m}F^2(m)\,,$$

cf. [4, p. 59].

5 Proof of Lemma 1

Let $n \geq m \geq 0$ be integers. From (4.5) we have

$$g(n) \;=\; g\big((n-m)+m\big) \;=\; xg(n-m+1) + yg(n-m)\,. \tag{5.1}$$

Next, we express the left-hand side of the identity in Lemma 1 by a determinant and then substitute the right-hand sides of (4.5) and (5.1) for the elements of the first column.

$$\begin{aligned} g(n+m)g(n-m) - g^2(n) &= \begin{vmatrix} g(n+m) & g(n) \\ g(n) & g(n-m) \end{vmatrix}\\ &= \begin{vmatrix} xg(n+1) + yg(n) & g(n) \\ xg(n-m+1) + yg(n-m) & g(n-m) \end{vmatrix}\\ &= x\begin{vmatrix} g(n+1) & g(n) \\ g(n-m+1) & g(n-m) \end{vmatrix}\,. \end{aligned} \tag{5.2}$$

The last determinant in (5.2) can be computed as follows. Firstly, we apply the recurrence formula (2.1) to the elements of the first column and then take determinant rules into account, among them we interchange the columns. This gives

$$\begin{vmatrix} g(n+1) & g(n) \\ g(n-m+1) & g(n-m) \end{vmatrix} = \begin{vmatrix} vg(n-1) & g(n) \\ vg(n-m-1) & g(n-m) \end{vmatrix} = (-v) \begin{vmatrix} g(n) & g(n-1) \\ g(n-m) & g(n-m-1) \end{vmatrix}.$$

We iterate this process $(n-m-1)$ more times. Then it ends with

$$\begin{vmatrix} g(n+1) & g(n) \\ g(n-m+1) & g(n-m) \end{vmatrix} = (-v)^{n-m} \begin{vmatrix} g(m+1) & g(m) \\ g(1) & g(0) \end{vmatrix} = (-v)^{n-m} \big(g(0)g(m+1) - g(1)g(m) \big). \tag{5.3}$$

Substituting the right-hand sides of the first equation from (4.4) and from (5.3) for the corresponding terms in (5.2), we obtain the identity in Lemma 1. □

6 Proof of Theorem 1

The proof of the theorem is divided into four parts.

(i) $\Longrightarrow$ (iii). The map

$$n \mapsto \begin{cases} \mathbb{N}_0 \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, \\ \big(g(n) \bmod p,\ g(n+1) \bmod p \big) \end{cases}$$

takes at most p^2 many values. By the pigeonhole principle there are two integers $0 \le n_1 < n_2$ such that

$$\begin{aligned} g(n_1) &\equiv g(n_2) \pmod p, \\ g(n_1+1) &\equiv g(n_2+1) \pmod p. \end{aligned}$$

This together with (2.1) leads by the induction principle to the congruence

$$g(n_1+n) \equiv g(n_2+n) \pmod p \qquad (n \ge 0).$$

Here, we replace n by $n - n_1 \ge 0$ and introduce $q := n_2 - n_1$. Then,

$$g(n+q) = g(n_2+n-n_1) \equiv g(n_1+n-n_1) = g(n) \pmod p. \tag{6.1}$$

This holds initially for $n \ge n_1$, but the hypothesis $v \not\equiv 0 \pmod p$ allows to derive the congruence

$$g(n+q-1) \equiv v^{-1}\big(g(n+q+1) - ug(n+q)\big) \pmod p$$

from the recurrence relation (2.1). Again by the induction principle it follows that (6.1) additionally holds for $0 \le n < n_1$. Thus, by (6.1), the function $g(n) \bmod p$ has the period q, and the same is true for the function $f(n) = g(an+b) \bmod p$.

Next, we consider the map $i \mapsto p^i \bmod q$, which takes at most finitely many values. Therefore, there are integers $1 \le i_1 < i_2$ satisfying $p^{i_1} \equiv p^{i_2} \pmod q$. Since f has the Lucas property modulo p, we may apply (1.2) and (1.3). This together with the q-periodicity of f and with $i_2 - i_1 > 0$ yields

$$\begin{aligned} f(n) &\equiv f\big(np^{i_2}\big) \equiv f\big(np^{i_2} - (p^{i_2} - p^{i_1})\big) \\ &= f\big(p^{i_1}\big(1 + (n-1)p^{i_2-i_1}\big)\big) \\ &\equiv f\big(1 + (n-1)p^{i_2-i_1}\big) \\ &\equiv f(1) f\big((n-1)p^{i_2-i_1}\big) \\ &\equiv f(1) f(n-1) \pmod p . \end{aligned}$$

The iterated application of this congruence gives

$$f(n) \equiv f^2(1) f(n-2) \equiv \cdots \equiv f^n(1) f(0) \equiv f^n(1) \pmod p \qquad (n \ge 0),$$

which is (iii).

(iii) $\Longrightarrow$ (i). Let $n \in \mathbb{N}$ be given by its p-adic representation,

$$n = \sum_{0 \le i \le r} n_i p^i = n_0 + mp \qquad \text{with} \qquad m = \sum_{1 \le i \le r} n_i p^{i-1},$$

say.

Case 1. p is a prime number. If p and $f(1)$ are coprime, Fermat's little theorem yields

$$\big(f^m(1)\big)^p \equiv f^m(1) \pmod p ,$$

otherwise p divides $f(1)$ and the congruence becomes trivial.

Case 2. p is a Carmichael number. Then the above congruence holds by (1.5) with $r = f^m(1)$, since $f(1)$ and p are coprime by the hypothesis of the theorem.

Taking (iii) into account, we obtain for all integers $n \ge 1$,

$$f(n) \equiv f^n(1) = f^{n_0}(1) f^{mp}(1) \equiv f^{n_0}(1) f^m(1) \equiv f(n_0) f(m) \pmod p .$$

Repeating this process r times and observing $f(0) \equiv f^0(1) = 1 \pmod p$ by (iii), it turns out that

$$f(n) \equiv f(n_0) f(n_1) \cdots f(n_r) f(0) \equiv f(n_0) f(n_1) \cdots f(n_r) \pmod p ,$$

which is (i), the Lucas property modulo p of f.

(iii) $\Longrightarrow$ (ii). We have $f(n) = g(an + b)$ for $n \ge 0$. Setting $n = 0$ in (iii) gives

$$g(b) = f(0) \equiv f^0(1) = 1 \pmod p . \tag{6.2}$$

In order to prove the second congruence in (ii) we first apply (iii) with $n = 2$.

$$g(2a + b) = f(2) \equiv f^2(1) = g^2(a + b) \pmod p . \tag{6.3}$$

Then, we use the identity from Lemma 1 with $n = a + b$ and $m = a$.

$$d\big(g(2a+b)g(b) - g^2(a+b)\big) \;=\; (-v)^b\big(g(0)g(a+1) - g(1)g(a)\big)^2 .$$

Here, the left-hand side is divisible by p, which follows from (6.2) and (6.3). On the right-hand side we know by the hypothesis of Theorem 1 that v and p are coprime. p is squarefree in any case, and then $g(0)g(a+1) - g(1)g(a)$ is divisible by p, which proves the second congruence in (ii).

(ii) $\Longrightarrow$ (iii). We prove the congruence

$$f(n) \;\equiv\; f^n(1) \pmod{p} \qquad (n \geq 0) \tag{6.4}$$

by induction with respect to n. For $n = 0$ we have by (ii),

$$f(0) \;=\; g(b) \;\equiv\; 1 \;=\; f^0(1) \pmod{p},$$

while (6.4) is trivial for $n = 1$. Next, let $n \geq 2$, and assume that (6.4) is already proven for $1, 2, \ldots, n$. In Lemma 1 we replace n by $an + b$ and m by a. Then,

$$\begin{aligned} &d\big[g\big(a(n+1)+b\big)g\big(a(n-1)+b\big) - g^2(an+b)\big] \\ &\;=\; (-v)^{a(n-1)+b}\big(g(0)g(a+1) - g(1)g(a)\big)^2 . \end{aligned} \tag{6.5}$$

Since the right-hand side of (6.5) vanishes by (ii), the same is true for the left-hand side. By the hypothesis of the theorem d and p are coprime, such that the term inside the square brackets in (6.5) is divisible by p. This fact can be rewritten by the congruence

$$f(n+1)f(n-1) \;\equiv\; f^2(n) \pmod{p}.$$

Here we may apply the induction hypothesis for $n - 1$ and n, i.e.,

$$f(n+1)f^{n-1}(1) \;\equiv\; f^{2n}(1) \pmod{p}. \tag{6.6}$$

If $\big(f(1), p\big) = 1$, we get

$$f(n+1) \;\equiv\; f^{n+1}(1) \pmod{p},$$

since $f^{-1}(1) \bmod p$ exists. Then the induction is finished, so that (6.4) is proved. In the case when p is a Carmichael number, we already have the coprimality of $f(1)$ and p by the hypothesis of the theorem.

Thus, if p is a prime, we finally must show that

$$f(1) \;\equiv\; 0 \pmod{p} \tag{6.7}$$

is impossible. In (4.4) and (4.5) we set $m = a$ and $n = b$. This yields

$$g(b+a) \;=\; xg(b+1) + yg(b) \tag{6.8}$$

with

$$dx \;=\; g(0)g(a+1) - g(1)g(a)\,.$$

From (ii) it follows that $dx \equiv 0 \pmod{p}$, and since d is not divisible by p we conclude that $x \equiv 0 \pmod{p}$. Together with $g(b) \equiv 1 \pmod{p}$ from (ii) the identity (6.8) simplifies to

$$y \;\equiv\; g(b+a) \;=\; f(1) \;\equiv\; 0 \pmod{p}\,, \tag{6.9}$$

where the last congruence holds by (6.7). We apply (4.5) for a second time with $n = b-1$ and $m = a$. Then,

$$g(b+a-1) \;=\; xg(b) + yg(b-1) \;\equiv\; 0 \pmod{p} \tag{6.10}$$

by $x \equiv y \equiv 0 \pmod{p}$. From (2.1) with $n = b+a-2 \geq 0$ we have

$$vg(b+a-2) \;=\; g(b+a) - ug(b+a-1)\,.$$

The right-hand side is divisible by p, which follows from (6.9) and (6.10). By $v \not\equiv 0 \pmod{p}$ it turns out that

$$g(b+a-2) \;\equiv\; 0 \pmod{p}\,. \tag{6.11}$$

This process via (6.9), (6.10), and (6.11), can be iterated, finally leading to the congruence $g(b) \equiv 0 \pmod{p}$. This contradicts to $g(b) \equiv 1 \pmod{p}$ in (ii). Hence (6.7) does not hold. This completes the proof of (6.4), and herewith the proof of Theorem 1. □

References

[1] W. Alford, A. Granville, and C. Pomerance, *There are Infinitely Many Carmichael Numbers*, Ann. Math. **139** (1994), 703–722.

[2] D.F. Bailey, *More binomial coefficient congruences*, Trinity University, San Antonio, TX 78212, 1992, 121–125.

[3] O. Forster, *Algorithmische Zahlentheorie*, Vieweg (1996), ISBN: 3-528-06580-X

[4] V.E. Hogatt, *Fibonacci and Lucas Numbers*, Houghton Mifflin (1969).

[5] E. Lucas, *Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier*, Bull. Soc. Math. France **6** (1878), 49–54.

[6] R. McIntosh, *A generalization of a congruential property of Lucas*, Amer. Math. Monthly **99**, no. 3 (1992), 231–238.

[7] H. Zhong and T. Cai, *On the Lucas property of linear recurrent sequences*, J. Number Theory **13**, no. 6 (2017), 1617–1625.

Carsten Elsner
Fachhochschule für die Wirtschaft
University of Applied Sciences
Freundallee 15
D-30173 Hannover, Germany
e-mail: carsten.elsner@fhdw.de

Jürgen Spilker
Am Schloßpark 10
D-79252 Stegen, Germany
e-mail:
juergen.spilker@t-online.de