THE G.C.D-FUNCTION OF TWO RECURSIVE FUNCTIONS

Jan-Christoph Schlage-Puchta and Jürgen Spilker

Abstract. Let g, h be solutions of a linear recurrence relation of length 2. We show that under some mild assumptions the greatest common divisor of $g(n)$ and $h(n)$ is periodic as a function of n and compute its mean value.

1. Problems and Results

Let a, b be coprime integers, $b \neq 0$, and consider the recurrence relation

$$f(n+2) = af(n+1) + bf(n), \qquad n \in \mathbb{N}_0. \tag{1}$$

Let $g, h : \mathbb{N}_0 \to \mathbb{Z}$ be solutions of (1) with

$$|g(n)| + |h(n)| > 0 \tag{2}$$

for all $n \in \mathbb{N}_0$. We consider the g.c.d.-function $t(n) = (g(n), h(n))$.

Problem 1. Under which conditions on g and h is the function $t(n)$ periodic?

Problem 2. If $t(n)$ is periodic, what is the mean value of $t(n)$?

We first need a

Definition. We call a function $f : \mathbb{N}_0 \to \mathbb{Z}$ periodic and $q \in \mathbb{N}$ a period of f, iff there exists some $n_0 \in \mathbb{N}_0$ such that $f(n) = f(n+q)$ for all $n \geq n_0$. If one can choose $n_0 = 0$, f is called simply periodic.

In this note we prove the following two theorems.

Theorem 1. *Let $g, h : \mathbb{N}_0 \to \mathbb{Z}$ be solutions of (1) satisfying (2), and assume that $c := g(1)h(0) - g(0)h(1) \neq 0$. Then*

(a) *the function $t(n)$ is periodic, moreover, if $(b, c) = 1$, it is simply periodic;*
(b) *every common period of $g(n)$ mod $|c|$ and $h(n)$ mod $|c|$ is a period of $t(n)$;*
(c) *for all $n \in \mathbb{N}_0$ we have $t(n)|c$.*

Theorem 2. *Let $g, h : \mathbb{N}_0 \to \mathbb{Z}$ be solutions of (1) satisfying (2), and assume that $g(0) = 0$, $g(1) = 1$, $c := h(0) \neq 0$ and $(b, c) = 1$. Then the mean value of $t(n)$ equals $\sum_{d|c} \frac{\varphi(d)}{k(d)}$, where $k(d) := \min\{n \in \mathbb{N} : d|g(n)\}$.*

Examples. 1. In the case $g(0) = 0$, $g(1) = 1$, $h(0) = 2$, $h(1) = a$, McDaniel [1] has shown, that $t(n)$ is 1 or 2 for $n \in \mathbb{N}$. This follows also from our Theorem 1 (c). If further $a = b = 1$, we obtain the Fibonacci- resp. Lucas-function. Since $g(n)$ mod 2 and $h(n)$ mod 2 are simply periodic with period 3, we get

$$t(n) = \begin{cases} 2, & n \equiv 0 \pmod 3; \\ 1, & n \not\equiv 0 \pmod 3), \end{cases}$$

with mean value $\frac{4}{3}$. This is a well-known result (see e.g. [2], [3]).

2. Defining g and h by $a = 1, b = 2$, $g(0) = h(0) = 1$, $g(1) = 2$, $h(1) = 0$, we obtain the g.c.d-function

$$t(n) = \begin{cases} 1, & n = 0 \\ 2, & n \geq 1 \end{cases},$$

which is periodic, but not simply periodic.

Remarks. 1. The assumption $(a, b) = 1$ in Theorem 1 is necessary, since for every common divisor d of a and b we have

$$d^n | t(2n), \qquad n \in \mathbb{N}.$$

If $d > 1$, $t(n)$ is unbounded, hence not periodic.

2. The g.c.d.-functions of recurrences of higher order need not be periodic. The companion polynomial $(x-1)(x-2)(x-3)$ corresponds to

$$f(n+3) = 6f(n+2) - 11f(n+1) + 6f(n), \qquad n \in \mathbb{N}_0.$$

It has solutions $g(n) = 2^{n+1} - 1$ and $h(n) = 3^{n+1} - 1$ with $c = -2$. If $p \geq 5$ is a prime, and $n \equiv -1 \pmod{p-1}$, then

$$t(n) = (2^{n+1} - 1, 3^{n+1} - 1) \equiv 0 \pmod p$$

and $t(n) \geq p$; hence, $t(n)$ is not bounded and a forteriori not periodic.

3. The function $\ell(d)$ does not depend on the period q of $t(n)$ mod d. If $f(n)$ is the solution of (1) with initial values $f(0) = 0, f(1) = 1$ (the generalized Fibonacci-function), one can take any period q of $f(n)$ mod d: We have

$$g(n) = (g(1) - ag(0))f(n) + g(0)f(n+1), \qquad n \in \mathbb{N}_0,$$

hence, q is a period of $g(n)$ mod d, and similarly for $h(n)$ mod d, thus q is a period of $t(n)$ mod d, too.

4. The mean value M of $t(n)$ depends only on the determinant c of the initial values of g and h. It is unbounded as a function of $m = |c|$, even if $g(0) = 0, g(1) = 1$, since $k(d) \leq d4^{\omega(d)}$ (see [3]) implies

$$M \geq \sum_{d|m} \frac{\varphi(d)}{d4^{\omega(d)}} = \prod_{p^j \| m} \left(1 + \frac{p-1}{4p} j\right) \geq \left(\frac{9}{8}\right)^{\omega(m)}$$

5. The assumption $(b, c) = 1$ in Theorem 2 is necessary, however, there is always some n_0 such that the function $\tilde{t}(n) = t(n + n_0)$ has the same mean value as $t(n)$ and the mean value formula holds true for $\tilde{t}$.

2. Proofs

We first need two lemmas, which are well-known for the classical Fibonacci-function (see [2]).

Lemma 1. *Let $f : \mathbb{N}_0 \to \mathbb{Z}$ be a solution of (1), and $d \in \mathbb{N}$. Then the function $n \mapsto f(n) \bmod d$ is periodic, and simply periodic if $(b, d) = 1$.*

Proof. There are positive integers $n_1 < n_2$, such that both $f(n_1) \equiv f(n_2) \pmod d$ and $f(n_1+1) \equiv f(n_2+1) \pmod d$. Then $q = n_2 - n_1$ is a period of $f(n) \bmod d$, since by (1), $f(n+q) \equiv f(n) \pmod d$ for all $n \geq n_1$. Assume that $f(n_0+q) \not\equiv f(n_0) \pmod d$, and choose n_0 maximal with this property. Then by (1), we have mod d the congruences

$$\begin{aligned} bf(n_0) &= f(n_0+2) - af(n_0+1) \\ &\equiv f(n_0+q+2) - af(n_0+q+1) \\ &= bf(n_0+q). \end{aligned}$$

If $(b, d) = 1$, this gives the contradiction $f(n_0) \equiv f(n_0+q) \pmod d$. □

Lemma 2. *Let $f : \mathbb{N}_0 \to \mathbb{Z}$ be the generalized Fibonacci-solution of (1), i.e., $f(0) = 0, f(1) = 1$. Then*

(a) $(f(n), f(n+1)) = 1, n \in \mathbb{N}_0$;
(b) $f(m+n) = f(m+1)f(n) + bf(m)f(n-1), m \in \mathbb{N}_0, n \in \mathbb{N}$;
(c) *if* $d, n \in \mathbb{N}$, *and* $k(d) = \min\{n \in \mathbb{N} : d|f(n)\}$, *then* $\big(d|f(n) \Leftrightarrow k(d)|n\big)$.

Proof. (a). Let p be a prime, and n be the least integer with $p|f(n), p|f(n+1)$; in particular, $n > 1$. The equation $f(n+1) = af(n) + bf(n-1)$ implies $p|bf(n-1)$, hence, $p|b$. Similarly, $f(n) = af(n-1) + bf(n-2)$ implies $p|af(n-1)$, thus $p|a$. This contradicts the assumption $(a, b) = 1$.

(b). This follows by induction on n.

(c). Let $L := \{n \in \mathbb{N}_0 : d|f(n)\}$. If $m, n \in L$, we get $m + n \in L$ by (b)., and if $m > n$, we have $f(m) = f(m-n)f(n+1) + bf(m-n-1)f(n)$, hence, $d|f(m-n)f(n+1)$, so $m - n \in L$ by (a). Take $n \in L$ and write $n = mk(d) + t$ with $0 \leq t < k(d)$. Since $t = n - mk(d) \in L$, we have $t = 0$ and $L = k(d) \cdot \mathbb{N}_0$. This proves the last claim. □

Proof of Theorem 1. Let $f : \mathbb{N}_0 \to \mathbb{Z}$ be the solution of (1) with initial values $f(0) = 0, f(1) = 1$. We have

$$cf(n) = h(0)g(n) - g(0)h(n), \qquad n \in \mathbb{N}_0, \tag{3}$$

since both sides solve (1), and the initial values are 0 and c. Similarly,

$$cf(n+1) = (ah(0) - h(1))g(n) - (ag(0) - g(1))h(n), \qquad n \in \mathbb{N}_0. \tag{4}$$

Fix $n \in \mathbb{N}_0$ and let t be a common divisor of $g(n)$ and $h(n)$. Then $t|c(f(n), f(n+1))$ by (3) and (4), hence $t|c$ by Lemma 2 (a) From this we deduce

$$t(n)|c, \qquad \text{for all } n \in \mathbb{N}_0. \tag{5}$$

By Lemma 1, a common period q of $g(n)$ mod $|c|$ and $h(n)$ mod $|c|$ exists, so, by (5),

$$t(n) = (g(n), h(n), c) = (g(n+q), h(n+q), c) = t(n+q), \quad \text{if } n \geq n_0.$$

This proves Theorem 1. $\square$

Proof of Theorem 2. Set $m := |c|$, and let q be a period of $t(n)$ mod m, which exists by Lemma 1. Then, since t is simply periodic, the mean value of $t(n)$ is

$$M = \frac{1}{q} \sum_{1 \leq n \leq q} t(n),$$

and by Theorem 1 (c), this quantity is equal to $\frac{1}{q} \sum_{d|m} d\ell(d)$, where $\ell(d) = \#\{n \leq q : (t(n), m) = d\}$. Further, we have

$$M = \frac{1}{q} \sum_{1 \leq n \leq q} (t(n), m) = \frac{1}{q} \sum_{s|m} s \left(\sum_{\substack{1 \leq n \leq q \\ (t(n),m)=s}} 1 \right).$$

Since

$$\sum_{k|n} \mu(k) = \begin{cases} 1, & n = 1 \\ 0, & n > 1 \end{cases}, \tag{6}$$

the inner sum can be written as

$$\sum_{\substack{1 \leq n \leq q \\ s|t(n)}} \sum_{k|(t(n)/s, m/s)} \mu(k) = \sum_{k|\frac{m}{s}} \left(\mu(k) \sum_{\substack{1 \leq n \leq q \\ sk|t(n)}} 1 \right).$$

Set $d := sk$; then

$$M = \sum_{d|m} \left(\ell(d) \sum_{k|d} \mu(k) \frac{d}{k} \right).$$

We use $\sum_{d|n} \varphi(d) = n$ together with (6) and see $\sum_{k|d} \mu(k) \frac{d}{k} = \varphi(d)$. Hence,

$$M = \frac{1}{q} \sum_{d|m} \varphi(d) \#\{n \leq q : d|t(n)\}$$

Since $g(0) = 0, g(1) = 1$, we have

$$h(n) = (h(1) - ah(0))g(n) + h(0)g(n+1),$$

and by Lemma 2 (a), we obtain

$$t(n) = (g(n), h(0)g(n+1)) = (g(n), h(0)) = (g(n), m).$$

We finally get by Lemma 2 (c) for every $d|m$

$$\#\{n \leq q : d|t(n)\} = \sum_{\substack{1 \leq n \leq q \\ d|g(n)}} 1 = \sum_{\substack{1 \leq n \leq q \\ k(d)|n}} 1 = \frac{q}{k(d)},$$

and Theorem 2 is proven. $\square$

References

[1] W. L. McDaniel, The g.c.d in Lucas sequences and Lehmer number sequences. *Fibonacci Quart.* **29** (1991), 24–29.
[2] V. E. Hoggatt, *Fibonacci and Lucas numbers*, Boston etc.: Houghton Mifflin Company IV, 1969.
[3] D. D. Wall, Fibonacci series modulo m, *Amer. Math. Monthly* **67** (1960), 525–532.

MSC-Index: 11B37, 11B39, 11A05

J.-C. Schlage-Puchta
J. Spilker
Mathematisches Institut
Eckerstr. 1
79111 Freiburg
Germany
jcp@math.uni-freiburg.de
Juergen.Spilker@math.uni-freiburg.de