Journal of Integer Sequences, Vol. 21 (2018),
Article 18.6.7

Greatest Common Divisors of Shifted Fibonacci Sequences Revisited

Annalena Rahn and Martin Kreh
Institute of Mathematics and Applied Computer Science
University of Hildesheim
Samelsonplatz 1
31141 Hildesheim
Germany
rahnan@uni-hildesheim.de
kreh@imai.uni-hildesheim.de

Abstract

In 2011, Chen computed the greatest common divisors of consecutive shifted Fibonacci numbers $F_n + a$ and $F_{n+1} + a$ for $a \in \{\pm 1, \pm 2\}$. He also showed that $\gcd(F_n + a, F_{n+1} + a)$ is bounded if $a \neq \pm 1$. This was later generalized by Spilker, who also showed that $\gcd(F_n + a, F_{n+1} + a)$ is periodic if $a \neq \pm 1$. In this article, we compute the greatest common divisor for $a = \pm 3$ and we show how the results given in this article compare to bounds derived by Chen and periods derived by Spilker. We further give a necessary criterion for an integer d to occur as such a greatest common divisor.

1 Introduction and results

Let $(F_n)_{n\geq 1}$ be the Fibonacci sequence defined by the recursion

$$F_n = F_{n-1} + F_{n-2}, \quad F_1 = F_2 = 1. \tag{1}$$

Using this recursion, F_n can be extended to integer indices, where we have the relation $F_{-n} = (-1)^{n+1} F_n$. In this article, we want to investigate greatest common divisors of the form $\gcd(F_n + a, F_{n+1} + a)$.

It is well known, that $\gcd(F_n+a, F_{n+1}+a) = 1$ for all n if $a = 0$, i.e., consecutive Fibonacci numbers are coprime. In 1971, Dudley and Tucker [2] showed that $\gcd(F_n + a, F_{n+1} + a)$ is unbounded for $a = \pm 1$ by showing that

$$\gcd(F_{4n+1} + 1, F_{4n+2} + 1) = L_{2n}, \tag{2}$$
$$\gcd(F_{4n+1} - 1, F_{4n+2} - 1) = F_{2n}, \tag{3}$$
$$\gcd(F_{4n+3} - 1, F_{4n+4} - 1) = L_{2n+1}. \tag{4}$$

Here $(L_n)_{n\geq 1}$ denotes the Lucas sequence defined by $L_n = L_{n-1} + L_{n-2}, L_1 = 1, L_2 = 3$.

In 2011, Chen [1] determined $\gcd(F_n + a, F_{n+1} + a)$ for $a \in \{\pm 1, \pm 2\}$ and proved the following bound.

Theorem A ([1]). Let $n, a \in \mathbb{Z}$. Then

- $\gcd(F_{2n-1} + a, F_{2n} + a) \leq |a^2 - 1|$ if $a \neq \pm 1$.
- $\gcd(F_{2n} + a, F_{2n+1} + a) \leq a^2 + 1$.

Spilker [4] generalized some of Chen's results. Among other, he showed the following theorems (in even greater generality than mentioned here).

Theorem B ([4]). For all $a \in \mathbb{Z}$, $\gcd(F_n + a, F_{n+1} + a)$ divides $a^2 + (-1)^n$. If $a \neq \pm 1$, the function $n \mapsto \gcd(F_n + a, F_{n+1} + a)$ is simply periodic and a period $p \leq (a^4 - 1)^2$ can be chosen by

$$F_p \equiv 0 \pmod{a^4 - 1}, \quad F_{p+1} \equiv 1 \pmod{a^4 - 1}. \tag{5}$$

Theorem C ([4]). Let $a \in \mathbb{Z}$ with $|a| > 1, k \in \mathbb{N}$ and $i \in \{0, 1\}$.

1. If $F_{2k-i} \equiv \alpha_i \pmod{a^2 + 1}$ with $0 \leq \alpha_i < a^2 + 1$, then

$$\gcd(F_{4k} + a, F_{4k+1} + a) = \gcd(\alpha_0 + a\alpha_1, a\alpha_0 - \alpha_1, a^2 + 1), \tag{6}$$
$$\gcd(F_{4k-2} + a, F_{4k-1} + a) = \gcd(\alpha_0 + (a-1)\alpha_1, a\alpha_0 - (a+1)\alpha_1, a^2 + 1). \tag{7}$$

2. If $F_{2k-i} \equiv \beta_i \pmod{a^2 - 1}$ with $0 \leq \alpha_i < a^2 - 1$, then

$$\gcd(F_{4k-1} + a, F_{4k} + a) = \gcd((a+1)\beta_1, (a-1)\beta_0 - a\beta_1, a^2 - 1), \tag{8}$$
$$\gcd(F_{4k-3} + a, F_{4k-2} + a) = \gcd(\beta_0 - (a+2)\beta_1, (a-1)\beta_0 - (a-1)\beta_1, a^2 - 1). \tag{9}$$

Spilker also answered the question in which cases the upper bound of Chen is being attained. To state this, define the *entry point* of $m \in \mathbb{N}$ as $e(m) := \min\{i \in \mathbb{N} : m|F_i\}$ (the existence of $e(m)$ follows from [5, Theorem 1]).

Theorem D ([4]). Let $|a| > 1$. The function $n \mapsto \gcd(F_n + a, F_{n+1} + a)$ has the upper bound $m = a^2 + 1$ as a value if and only if $e(m)$ is odd and $a \equiv \pm F_{e(m)+1} \pmod{m}$. The function $n \mapsto \gcd(F_n + a, F_{n+1} + a)$ has the value $m = a^2 - 1$ on the odd integers if and only if $a = 2$ or $e(m)$ is even and $a \equiv -F_{e(m)+1} \pmod{m}$.

In this article, we will use Chen's method to determine $\gcd(F_n+a, F_{n+1}+a)$ for $a=\pm 3$. More precisely, we will show the following theorems.

Theorem 1. *We have*

1. $\gcd(F_{4n-1}+3, F_{4n}+3) = \begin{cases} 8, & \text{if } n \equiv 2 \pmod 3; \\ 1, & \text{otherwise.} \end{cases}$

2. $\gcd(F_{4n}+3, F_{4n+1}+3) = \begin{cases} 2, & \text{if } n \equiv 1 \pmod 3 \text{ and } n \not\equiv 4 \pmod 5; \\ 5, & \text{if } n \not\equiv 1 \pmod 3 \text{ and } n \equiv 4 \pmod 5; \\ 10, & \text{if } n \equiv 1 \pmod 3 \text{ and } n \equiv 4 \pmod 5; \\ 1, & \text{otherwise.} \end{cases}$

3. $\gcd(F_{4n+1}+3, F_{4n+2}+3) = \begin{cases} 4, & \text{if } n \equiv 0 \pmod 3; \\ 1, & \text{otherwise.} \end{cases}$

4. $\gcd(F_{4n+2}+3, F_{4n+3}+3) = \begin{cases} 2, & \text{if } n \equiv 2 \pmod 3; \\ 1, & \text{otherwise.} \end{cases}$

Theorem 2. *We have*

1. $\gcd(F_{4n-1}-3, F_{4n}-3) = \begin{cases} 2, & \text{if } n \equiv 2 \pmod 3; \\ 1, & \text{otherwise.} \end{cases}$

2. $\gcd(F_{4n}-3, F_{4n+1}-3) = \begin{cases} 2, & \text{if } n \equiv 1 \pmod 3; \\ 1, & \text{otherwise.} \end{cases}$

3. $\gcd(F_{4n+1}-3, F_{4n+2}-3) = \begin{cases} 2, & \text{if } n \equiv 0 \pmod 3; \\ 1, & \text{otherwise.} \end{cases}$

4. $\gcd(F_{4n+2}-3, F_{4n+3}-3) = \begin{cases} 2, & \text{if } n \equiv 2 \pmod 3 \text{ and } n \not\equiv 1 \pmod 5; \\ 5, & \text{if } n \not\equiv 2 \pmod 3 \text{ and } n \equiv 1 \pmod 5; \\ 10, & \text{if } n \equiv 2 \pmod 3 \text{ and } n \equiv 1 \pmod 5; \\ 1, & \text{otherwise.} \end{cases}$

We will further examine the sets

$$G_0(a) := \{\gcd(F_{2n}+a, F_{2n+1}+a) : n \in \mathbb{Z}\} \text{ and } G_1(a) := \{\gcd(F_{2n+1}+a, F_{2n+2}+a) : n \in \mathbb{Z}\}. \tag{10}$$

Let $D(n)$ denote the set of divisors of n. We already know from Theorem B that $G_0(a) \subset D(a^2+1)$ and $G_1(a) \subset D(a^2-1)$ Theorem D characterizes the cases in which $a^2+1 \in G_0(a)$ and $a^2-1 \in G_1(a)$. We will show the following extension.

Theorem 3.

1. *We have* $1 \in G_0(a)$ *and* $\{1, a+1\} \subset G_1(a)$ *for all* a.
2. *We have* $2 \in G_0(a)$ *if and only if* $a \equiv 1 \pmod 2$ *and* $2 \in G_1(a)$ *if and only if* $a \equiv 1 \pmod 4$.
3. *Let* $d \neq 1, 2$ *be a divisor of* a^2+1. *If* $d \in G_0(a)$, *then* $e(d)$ *is odd and* $a \equiv \pm F_{e(d)+1} \pmod d$.
4. *Let* $d \neq 1, 2$ *be a divisor of* $a^2 - 1$ *such that* $a \not\equiv \pm 1 \pmod d$. *If* $d \in G_1(a)$, *then* $e(d)$ *is even and* $a \equiv -F_{e(d)+1} \pmod d$.

Before proving Theorems 1, 2, and 3, we will start with some lemmas in the next section. In Section 5, we will compare our results to those of Spilker and raise some new questions.

2 Preliminaries

We will need a few results about divisibility and greatest common divisors of Fibonacci numbers. We will state common facts without proof and prove some special identities. In the following we always assume that n is a (not necessarily positive) integer.

Lemma 4. *For all* $a, b, c \in \mathbb{Z}$ *we have* $\gcd(a, bc) = \gcd(a, \gcd(a, b)c)$.

Lemma 5 ([3])**.** *We have the following identities and rules about divisibility and greatest common divisors of Fibonacci numbers.*

- *For all* $m, n \in \mathbb{N}$ *we have* $F_{m+n} = F_{m+1}F_n + F_m F_{n-1}$.
- *For all* $n \in \mathbb{N}$ *we have* $F_{n+1}F_{n-1} = F_n^2 + (-1)^n$.
- $F_n \equiv 0 \pmod 2 \Leftrightarrow n \equiv 0 \pmod 3$.
- $F_n \equiv 0 \pmod 4 \Leftrightarrow n \equiv 0 \pmod 6$.
- $F_n \equiv 0 \pmod 5 \Leftrightarrow n \equiv 0 \pmod 5$.
- $F_n \equiv 0 \pmod 8 \Leftrightarrow n \equiv 0 \pmod 6$.
- *For all* $n \in \mathbb{N}$ *we have* $\gcd(F_n, F_{n+1}) = 1$.
- *For all* $m, n \in \mathbb{N}$ *we have* $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

Lemma 6. *For all* $n \in \mathbb{Z}$ *we have*

$$\gcd(F_{2n}, 4) = \begin{cases} 4, & \text{if } n \equiv 0 \pmod 3; \\ 1, & \text{otherwise.} \end{cases} \tag{11}$$

Proof. Let $n = 3m + k$ with $k \in \{-1, 0, 1\}$. Then we get with Lemma 5

$$\gcd(F_{2n}, 4) = \gcd(F_{6m+2k}, 4) = \begin{cases} 4, & \text{if } k = 0; \\ 1, & \text{otherwise.} \end{cases} \tag{12}$$

□

Lemma 7. *For all $n \in \mathbb{Z}$ we have*

$$\gcd(10, F_{2n-1} - 2F_{2n}) = \begin{cases} 2, & \text{if } n \equiv 2 \pmod 3; \\ 1, & \text{otherwise.} \end{cases} \tag{13}$$

Proof. Analogously to above, $F_{2n-1} - 2F_{2n}$ is divisible by 2 if and only if $2n - 1 \equiv 0 \pmod 3$, i.e., if $n \equiv 2 \pmod 3$. Further we have

$$F_{2n-1} - 2F_{2n} = -(3F_{2n-2} + F_{2n-3}) = -(4F_{2n-3} + 3F_{2n-4}) \tag{14}$$

and for any residue class of n modulo 5 we can pick one of the three terms above such that one summand is divisible by 5 while the other is not (for example, if $n \equiv 4 \pmod 5$ then F_{2n-3} is divisible by 5 and $3F_{2n-2}$ is not divisible by 5 due to Lemma 5). Thus $F_{2n-1} - 2F_{2n}$ is not divisible by 5. □

Lemma 8. *For all $n \in \mathbb{Z}$ we have*

$$\gcd(10, F_{2n-1} - 3F_{2n}) = \begin{cases} 2, & \text{if } n \equiv 1 \pmod 3 \text{ and } n \not\equiv 4 \pmod 5; \\ 5, & \text{if } n \not\equiv 1 \pmod 3 \text{ and } n \equiv 4 \pmod 5; \\ 10, & \text{if } n \equiv 1 \pmod 3 \text{ and } n \equiv 4 \pmod 5; \\ 1, & \text{otherwise.} \end{cases} \tag{15}$$

Proof. It suffices to show that $2 | F_{2n-1} - 3F_{2n}$ if and only if $n \equiv 1 \pmod 3$ and $5 | F_{2n-1} - 3F_{2n}$ if and only if $n \equiv 4 \pmod 5$. With Lemma 5, $F_{2n-1} - 3F_{2n} = -F_{2n-2} - 2F_{2n}$ is divisible by 2 if and only if $2n - 2 \equiv 0 \pmod 3$, i.e., if $n \equiv 1 \pmod 3$ and $F_{2n-1} - 3F_{2n} = -5F_{2n} + F_{2n+2}$ is divisible by 5 if and only if $2n + 2 \equiv 0 \pmod 5$, i.e., if $n \equiv 4 \pmod 5$. □

Lemma 9. *For all $n \in \mathbb{Z}$ we have*

$$\gcd(8, 4F_{2n} - F_{2n-1}) = \begin{cases} 2, & \text{if } n \equiv 2 \pmod 3; \\ 1, & \text{otherwise.} \end{cases} \tag{16}$$

Proof. Let $n = 3m + k$ with $k \in \{-1, 0, 1\}$. Then we get with Lemma 5

$$F_{2n-1} = F_{6m+2k-1} \equiv \begin{cases} 2 \pmod 4, & \text{if } k = -1; \\ 1 \pmod 2, & \text{otherwise,} \end{cases} \tag{17}$$

and this shows the lemma. □

Lemma 10. *For all $n \in \mathbb{Z}$ we have*

$$\gcd(10, F_{2n-1} + 3F_{2n}) = \begin{cases} 2, & \text{if } n \equiv 1 \pmod 3; \\ 1, & \text{otherwise.} \end{cases} \tag{18}$$

Proof. Since $F_{2n-1} + 3F_{2n} = F_{-2n+1} - 3F_{-2n} = F_{-2n-1} - 2F_{-2n}$, this follows from Lemma 7. ☐

Lemma 11. *For all $n \in \mathbb{Z}$ we have*

$$\gcd(10, F_{2n+1} + 3F_{2n}) = \begin{cases} 2, & \text{if } n \equiv 2 \pmod 3 \text{ and } n \not\equiv 1 \pmod 5; \\ 5, & \text{if } n \not\equiv 2 \pmod 3 \text{ and } n \equiv 1 \pmod 5; \\ 10, & \text{if } n \equiv 2 \pmod 3 \text{ and } n \equiv 1 \pmod 5; \\ 1, & \text{otherwise.} \end{cases} \tag{19}$$

Proof. Since $F_{2n+1} + 3F_{2n} = F_{-2n-1} - 3F_{-2n}$, this follows from Lemma 8. ☐

The following lemma due to Chen is the main part for computing the greatest common divisors.

Lemma 12 ([1])**.** *For all $m, k, a \in \mathbb{Z}$ we have*

$$\gcd(F_m + a, F_{m+1} + a) = \gcd(F_{m-2k} + aF_{2k-1}, F_{m-(2k+1)} - aF_{2k}). \tag{20}$$

3 Proof of Theorem 1 and Theorem 2

In this section we will give the proof for Theorems 1 and 2.

Proof of Theorem 1.

1. We use Lemma 12 with $m = 4n-1, k = n, a = 3$ to get

$$\gcd(F_{4n-1} + 3, F_{4n} + 3) = \gcd(4F_{2n-1}, F_{2n-2} - 3F_{2n}) = \gcd(4F_{2n-1}, F_{2n+2}) \tag{21}$$
$$= \gcd(4F_{2n-1} + 4F_{2n+2}, F_{2n+2}) = \gcd(8F_{2n+1}, F_{2n+2}). \tag{22}$$

   Since $\gcd(F_{2n+1}, F_{2n+2}) = 1$, we get with Lemma 5

$$\gcd(F_{4n-1} + 3, F_{4n} + 3) = \gcd(8, F_{2n+2}) = \gcd(F_6, F_{2n+2}) = F_{\gcd(6,2n+2)}, \tag{23}$$

   and since

$$\gcd(6, 2n+2) = \begin{cases} 6, & \text{if } n \equiv 2 \pmod 3; \\ 2, & \text{otherwise,} \end{cases} \tag{24}$$

   this proves the first case.

2. We use Lemma 12 with $m = 4n, k = n, a = 3$ to get

$$\begin{aligned}\gcd(F_{4n}+3, F_{4n+1}+3) &= \gcd(F_{2n}+3F_{2n-1}, F_{2n-1}-3F_{2n}) && (25)\\ &= \gcd(F_{2n}+3F_{2n-1}-3(F_{2n-1}-3F_{2n}), F_{2n-1}-3F_{2n}) && (26)\\ &= \gcd(10F_{2n}, F_{2n-1}-3F_{2n}). && (27)\end{aligned}$$

With Lemma 4 we get

$$\begin{aligned}\gcd(F_{4n}+3, F_{4n+1}+3) &= \gcd(10\cdot\gcd(F_{2n}, F_{2n-1}-3F_{2n}), F_{2n-1}-3F_{2n}) && (28)\\ &= \gcd(10, F_{2n-1}-3F_{2n}), && (29)\end{aligned}$$

thus the claim follows with Lemma 8.

3. We use Lemma 12 with $m = 4n+1, k = n, a = 3$ and Lemma 4 to get

$$\begin{aligned}\gcd(F_{4n+1}+3, F_{4n+2}+3) &= \gcd(F_{2n+1}+3F_{2n-1}, 2F_{2n}) && (30)\\ &= \gcd(F_{2n}+4F_{2n-1}, 2\cdot\gcd(F_{2n}+4F_{2n-1}, F_{2n})) && (31)\\ &= \gcd(F_{2n}+4F_{2n-1}, 2\cdot\gcd(4, F_{2n})). && (32)\end{aligned}$$

With Lemma 6 and Lemma 5 we get

$$\begin{aligned}&\gcd(F_{2n}+4F_{2n-1}, 2\cdot\gcd(4, F_{2n})) && (33)\\ &= \begin{cases}\gcd(F_{2n}+4F_{2n-1}, 8) = \gcd(4F_{2n-1}, 8) = 4, & \text{if } n \equiv 0 \pmod 3;\\ \gcd(F_{2n}+4F_{2n-1}, 2) = \gcd(F_{2n}, 2) = 1, & \text{otherwise.}\end{cases} && (34)\end{aligned}$$

4. We use Lemma 12 with $m = 4n+2, k = n, a = 3$ to get

$$\begin{aligned}\gcd(F_{4n+2}+3, F_{4n+3}+3) &= \gcd(F_{2n+2}+3F_{2n-1}, F_{2n+1}-3F_{2n}) && (35)\\ &= \gcd(2F_{2n}+4F_{2n-1}, F_{2n-1}-2F_{2n}) && (36)\\ &= \gcd(10F_{2n}, F_{2n-1}-2F_{2n}). && (37)\end{aligned}$$

With Lemma 4 we get

$$\begin{aligned}\gcd(F_{4n+2}+3, F_{4n+3}+3) &= \gcd(10\cdot\gcd(F_{2n}, F_{2n-1}-2F_{2n}), F_{2n-1}-2F_{2n}) && (38)\\ &= \gcd(10, F_{2n-1}-2F_{2n}), && (39)\end{aligned}$$

hence the statement follows with Lemma 7.

$\square$

Proof of Theorem 2.

1. We use Lemma 12 with $m = 4n-1, k = n, a = -3$ to get

$$\gcd(F_{4n-1}-3, F_{4n}-3) = \gcd(2F_{2n-1}, F_{2n-2}+3F_{2n}) \tag{40}$$
$$= \gcd(2F_{2n-1}, 4F_{2n}-F_{2n-1}) \tag{41}$$
$$= \gcd(8F_{2n}, 4F_{2n}-F_{2n-1}). \tag{42}$$

   Using Lemma 4 we get

$$\gcd(F_{4n-1}-3, F_{4n}-3) = \gcd(8\cdot\gcd(F_{2n}, 4F_{2n}-F_{2n-1}), 4F_{2n}-F_{2n-1}) \tag{43}$$
$$= \gcd(8, 4F_{2n}-F_{2n-1}), \tag{44}$$

   thus the claim folows with Lemma 9.

2. We use Lemma 12 with $m = 4n, k = n, a = -3$ to get

$$\gcd(F_{4n}-3, F_{4n+1}-3) = \gcd(F_{2n}-3F_{2n-1}, F_{2n-1}+3F_{2n}) = \gcd(10F_{2n}, F_{2n-1}+3F_{2n}). \tag{45}$$

   Using Lemma 4 gives

$$\gcd(F_{4n}-3, F_{4n+1}-3) = \gcd(10\cdot\gcd(F_{2n}, F_{2n-1}+3F_{2n}), F_{2n-1}+3F_{2n}) \tag{46}$$
$$= \gcd(10, F_{2n-1}+3F_{2n}), \tag{47}$$

   and Lemma 10 gives the result.

3. We use Lemma 12 with $m = 4n+1, k = n, a = -3$ to get

$$\gcd(F_{4n+1}-3, F_{4n+2}-3) = \gcd(F_{2n+1}-3F_{2n-1}, 4F_{2n}) \tag{48}$$
$$= \gcd(F_{2n-3}, 8F_{2n-1}-4F_{2n-3}) = \gcd(F_{2n-3}, 8F_{2n-1}) \tag{49}$$
$$= \gcd(F_{2n-3}, 8) = \gcd(F_{2n-3}, F_6). \tag{50}$$

   Using Lemma 5 gives $\gcd(F_{4n+1}-3, F_{4n+2}-3) = F_{\gcd(6,2n-3)}$, and since

$$\gcd(6, 2n-3) = \begin{cases} 3, & \text{if } n \equiv 0 \pmod 3; \\ 1, & \text{otherwise,} \end{cases} \tag{51}$$

   we get

$$\gcd(F_{4n+1}-3, F_{4n+2}-3) = F_{\gcd(2n-3,6)} = \begin{cases} F_3 = 2, & \text{if } n \equiv 0 \pmod 3; \\ F_1 = 1, & \text{otherwise.} \end{cases} \tag{52}$$

4. We use Lemma 12 with $m = 4n+2, k = n, a = -3$ to get

$$\gcd(F_{4n+2}-3, F_{4n+3}-3) = \gcd(F_{2n+2}-3F_{2n-1}, F_{2n+1}+3F_{2n}) \tag{53}$$
$$= \gcd(4F_{2n}-2F_{2n+1}, F_{2n+1}+3F_{2n}) \tag{54}$$
$$= \gcd(10F_{2n}, F_{2n+1}+3F_{2n}). \tag{55}$$

   Using Lemma 4, we get $\gcd(F_{4n+2}-3, F_{4n+3}-3) = \gcd(10, F_{2n+1}+3F_{2n})$, hence the statement follows with Lemma 11.

□

4 Proof of Theorem 3

To prove Theorem 3, we first note that

$$\gcd(F_0+a,F_1+a)=\gcd(a,a+1)=1, \tag{56}$$
$$\gcd(F_1+a,F_2+a)=\gcd(a+1,a+1)=a+1, \tag{57}$$
$$\gcd(F_3+a,F_4+a)=\gcd(a+2,a+3)=1. \tag{58}$$

This proves the first statement. For the second statement, note that a has to be odd, since otherwise $2\nmid a^2\pm 1$. So suppose that a is odd. Then we have

$$\gcd(F_4+a,F_5+a)=\gcd(a+3,a+5)=2, \tag{59}$$

hence $2\in G_0(a)$. We turn our attention to $G_1(a)$. First let $a\equiv 1 \pmod 4$. We have $\gcd(F_7+a,F_8+a)=\gcd(F_7+a,F_6)|8$ and $F_7+a\equiv 2 \pmod 4, F_8+a\equiv 2 \pmod 4$, hence

$$2=\gcd(F_7+a,F_8+a)\in G_1(a). \tag{60}$$

Assume now that $a\equiv 3 \pmod 4$. We will use the formula of the greatest common divisor given in Theorem C. Let

$$A_1:=(a+1)\beta_1,\quad B_1:=(a-1)\beta_0-a\beta_1,\quad A_2:=\beta_0-(a+2)\beta_1,\quad B_2:=(a-1)\beta_0-(a-1)\beta_1, \tag{61}$$

where β_0,β_1 are defined as in Theorem C. Since $a^2-1\equiv 0 \pmod 4$, we can only have $2\in G_1(a)$ if there is an $i\in\{1,2\}$ such that both A_i and B_i are even and further $A_i\equiv 2 \pmod 4$ or $B_i\equiv 2 \pmod 4$.

- Then we have $A_1\equiv 0 \pmod 4$ in any case.
- We have $B_1\equiv 2 \pmod 4$ if and only if $2\beta_0+\beta_1\equiv 2 \pmod 4$. Since $\beta_i\equiv F_{2k-i} \pmod{a^2-1}$, this holds if and only if $2F_{2k}+F_{2k-1}\equiv 2 \pmod 4$, i.e., if and only if $F_{2k+2}\equiv 2 \pmod 4$. From Lemma 5, this holds if and only if $2k+2\equiv 0 \pmod 3$ and $2k+2\not\equiv 0 \pmod 6$, which is impossible.
- We have $A_2\equiv 2 \pmod 4$ if and only if $\beta_0-\beta_1\equiv 2 \pmod 4$. This is the case precisely when $F_{2k}-F_{2k-1}=F_{2k-2}\equiv 2 \pmod 4$. From Lemma 5, this holds if and only if $2k-2\equiv 0 \pmod 3$ and $2k-2\not\equiv 0 \pmod 6$, which is impossible.
- Finally, we have $B_2\equiv 2 \pmod 4$ if and only if $\beta_0-\beta_1\equiv 1 \pmod 2$, in which case we also have $A_2\equiv 1 \pmod 2$.

Hence $2\notin G_1(a)$ if $a\equiv 3 \pmod 4$.

For the proof of the fourth statement, we mimic Spilker's proof of Theorem D. We use the identity $F_{m+n} = F_{m+1}F_n + F_mF_{n-1}$ from Lemma 5 to find, that the integers $F_1, F_2, \ldots$ are modulo d equivalent to

$$\begin{array}{llllll} F_1, & F_2, & \ldots, & F_{e(d)-1}, & 0, & \\ F_{e(d)+1}F_1, & F_{e(d)+1}F_2, & \ldots, & F_{e(d)+1}F_{e(d)-1}, & 0, & \\ F^2_{e(d)+1}F_1, & F^2_{e(d)+1}F_2, & \ldots, & F^2_{e(d)+1}F_{e(d)-1}, & 0, & \ldots \end{array} \tag{62–64}$$

where $F_n^k := (F_n)^k$. Hence

$$F_{ke(d)} \equiv 0 \pmod{d} \text{ and } F_{ke(d)+1} \equiv F^k_{e(d)+1} \pmod{d} \text{ for all } k \in \mathbb{N}. \tag{65}$$

From Lemma 5, we get

$$F_{e(d)+1} = F_{e(d)} + F_{e(d)-1} \equiv F_{e(d)-1} \pmod{d}, \tag{66}$$

$$F_{e(d)+1}F_{e(d)-1} = F^2_{e(d)} + (-1)^{e(d)} \equiv (-1)^{e(d)} \pmod{d}, \tag{67}$$

hence we further have

$$F^2_{e(d)+1} \equiv (-1)^{e(d)} \pmod{d}. \tag{68}$$

We begin with the set $G_0(a)$. Suppose that $d \in G_0(a)$, i.e.,

$$d = \gcd(F_{n_0} + a, F_{n_0+1} + a) = \gcd(F_{n_0} + a, F_{n_0-1}) \tag{69}$$

for some even integer n_0. Then $F_{n_0} + a \equiv 0 \pmod{d}$ and $F_{n_0-1} \equiv 0 \pmod{d}$. From [5, Theorem 3], $n_0 - 1$ is a multiple of $e(d)$, i.e., $n_0 = ke(d) + 1$ for some $k \in \mathbb{Z}$. Since n_0 is even, k and $e(d)$ are odd, thus (65) and (68) give

$$F_{n_0} = F_{ke(d)+1} \equiv F^k_{e(d)+1} \equiv (-1)^{\frac{k-1}{2}} F_{e(d)+1} \pmod{d}, \tag{70}$$

hence $a \equiv \pm F_{e(d)+1} \pmod{d}$, and this proves the statement for $G_0(a)$.

The statement for the set $G_1(a)$ can be proved almost analogously. Since here n_0 is odd, $ke(d)$ is even. If k was even, we would get

$$F_{n_0} \equiv F^k_{e(d)+1} \equiv \pm 1 \pmod{d}, \tag{71}$$

hence $a \equiv \pm 1 \pmod{d}$. This contradiction yields that k is odd, thus $e(d)$ is even and we get

$$a \equiv -F_{n_0} \equiv -F^k_{e(d)+1} \equiv -\left((-1)^{e(d)}\right)^{\frac{k-1}{2}} F_{e(d)+1} \equiv -F_{e(d)+1} \pmod{d}. \tag{72}$$

5 Remarks and future work

In this section we will briefly compare our results to the general results of Spilker [4].

For $a = \pm 2$, Theorems B, C, and D state, that $\gcd(F_n \pm 2, F_{n+1} \pm 2)$ is a divisor of 5 respectively 3, a period of $\gcd(F_n \pm 2, F_{n+1} \pm 2)$ is given by 40, and since

$$e(3) = 4, \quad F_5 = 5 \equiv 2 \pmod 3 \qquad \text{and} \qquad e(5) = 5, \quad F_6 = 8 \equiv -2 \pmod 5, \tag{73}$$

the values 3 and 5 are attained. The exact values of $\gcd(F_n \pm 2, F_{n+1} \pm 2)$ can be found in [1] and [4], it turns out, that 40 is indeed the smallest period.

For $a = \pm 3$, Theorems B, C, and D state, that $\gcd(F_n \pm 3, F_{n+1} \pm 3)$ is a divisor of 10 respectively 8, a period of $\gcd(F_n \pm 3, F_{n+1} \pm 3)$ is given by 120, and since

$$e(8) = 6, \quad F_7 = 13 \equiv -3 \pmod 8 \qquad \text{and} \qquad e(10) = 15, \quad F_{16} = 987 \equiv -3 \pmod{10}, \tag{74}$$

the values 8 and 10 are attained. Theorem 3 additionally states, that the value 2 is attained by $\gcd(F_{n_0} \pm 3, F_{n_0+1} \pm 3)$ for some even n_0, while it is attained for some odd n_0 only in the case $a = -3$. This, together with Theorems 1 and 2, shows that the cases $a = \pm 3$ are the first ones, in which not every divisor of $a^2 + 1$ respectively $a^2 - 1$ occurs as a greatest common divisor. From the exact values computed in Theorems 1 and 2, we also see that the smallest period of $\gcd(F_n \pm 3, F_{n+1} \pm 3)$ is not 120, but 60.

These observations give rise to some new questions:

Problem 13. Given $a \in \mathbb{Z}$ with $|a| \geq 2$, what is the smallest period of $\gcd(F_n + a, F_{n+1} + a)$?

Problem 14. Theorem 3 only gives a necessary but not a sufficient condition for a divisor d of $a^2 \pm 1$ to occur as a greatest common divisor. Theorem D gives also a sufficient condition for $d = a^2 \pm 1$ to occur as a greatest common divisor. Are there any sufficient conditions for $d \neq a^2 \pm 1$?

Problem 15. Let $a \in \mathbb{Z}$ with $|a| \geq 2$. Since $G_0(a) \subset D(a^2 + 1)$ and $G_1(a) \subset D(a^2 - 1)$, we have $|G_0(a)| \leq \tau(a^2 + 1)$ and $|G_1(a)| \leq \tau(a^2 - 1)$ (where $\tau(n) = \sum_{d|n} 1$ denotes the divisor function). What are the (exact or asymptotic) sizes of $G_0(a)$ and $G_1(a)$?

References

[1] K.-W. Chen, Greatest common divisors in shifted Fibonacci sequences, *J. Integer Sequences* **14** (2011), Article 11.4.7.

[2] U. Dudley and B. Tucker, Greatest common divisors in altered Fibonacci sequences, *Fibonacci Quart.* **9** (1971), 89–91.

[3] T. Koshy, *Fibonacci and Lucas Numbers With Applications*, Wiley-Interscience, 2001.

[4] J. Spilker, The gcd of the shifted Fibonacci sequence, in Jürgen Sander, Jörn Steuding, and Rasa Steuding, eds., *From Arithmetic to Zeta-Functions*, Springer, 2016, pp. 473–483.

[5] D. D. Wall, Fibonacci series modulo m, *Amer. Math. Monthly* **67** (1960), 525–532.

2010 *Mathematics Subject Classification*: Primary 11B39; Secondary 11A05.
Keywords: shifted Fibonacci sequence, greatest common divisor.

(Concerned with sequence A000045.)

Received January 31 2018; revised version received June 20 2018. Published in *Journal of Integer Sequences*, August 22 2018.

Return to Journal of Integer Sequences home page.