ON THE GREATEST COMMON DIVISOR OF n AND THE nTH FIBONACCI NUMBER, II

ABHISHEK JHA AND CARLO SANNA†

Abstract. Let $\mathcal{A}$ be the set of all integers of the form $\gcd(n, F_n)$, where n is a positive integer and F_n denotes the nth Fibonacci number. Leonetti and Sanna proved that $\mathcal{A}$ has natural density equal to zero, and asked for a more precise upper bound. We prove that

$$\#\big(\mathcal{A} \cap [1, x]\big) \ll \frac{x \log\log\log x}{\log\log x}$$

for all sufficiently large x.

1. Introduction

Let (u_n) be a nondegenerate linear recurrence with integral values. Arithmetic relations between n and u_n have been studied by several authors. For example, the set of positive integers such that n divides u_n has been studied by Alba González, Luca, Pomerance, and Shparlinski [2], assuming that the characteristic polynomial of (u_n) is separable, and by André-Jeannin [3], Luca and Tron [11], Sanna [17], and Somer [21], when (u_n) is a Lucas sequence. Furthermore, Sanna [19] showed that the set of natural numbers n such that $\gcd(n, u_n) = 1$ has a natural density (see [13] for a generalization). Mastrostefano and Sanna [12, 18] studied the moments of $\log\big(\gcd(n, u_n)\big)$ and $\gcd(n, u_n)$ when (u_n) is a Lucas sequence, and Jha and Nath [7] performed a similar study over shifted primes. (See also the survey of Tron [23] on greatest common divisors of terms of linear recurrences.)

Let (F_n) be the linear recurrence of Fibonacci numbers, which is defined by $F_1 = F_2 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for every positive integer n. Sanna and Tron [20] proved that, for each positive integer k, the set of positive integers n such that $\gcd(n, F_n) = k$ has a natural density, which is given by an infinite series. Kim [9] and Jha [6] obtained formally analogous results in cases of elliptic divisibility sequences and orbits of polynomial maps, respectively. Let $\mathcal{A}$ be the set of numbers of the form $\gcd(n, F_n)$, for some positive integer n. Leonetti and Sanna [10] provided an effective method to enumerate the elements of $\mathcal{A}$ in increasing order. In particular, the first elements of $\mathcal{A}$ are

$$1, \quad 2, \quad 5, \quad 7, \quad 10, \quad 12, \quad 13, \quad 17, \quad 24, \quad 25, \quad 26, \quad 29, \quad 34, \quad 35, \quad 36, \quad \ldots$$

see [1, A285058] for more terms. Then they proved that

$$\#\mathcal{A}(x) \gg \frac{x}{\log x} \tag{1}$$

for all $x \geq 2$. Their approach relied on a result of Cubre and Rouse [4], which in turn follows from Galois theory and the Chebotarev density theorem. Later, Jha and Sanna [8, Proposition 1.4] obtained an elementary proof as an application of related arithmetic problem over shifted primes. Leonetti and Sanna [10] also gave the upper bound $\#\mathcal{A}(x) = o(x)$ as $x \to +\infty$; and asked for a more precise estimate. We prove the following upper bound on $\#\mathcal{A}(x)$.

Theorem 1.1. *We have*

$$\#\mathcal{A}(x) \ll \frac{x \log\log\log x}{\log\log x}$$

2010 *Mathematics Subject Classification.* Primary: 11B39, Secondary: 11A05, 11N25.

Key words and phrases. Fibonacci numbers; greatest common divisor; rank of appearance; upper bound.

† C. Sanna is a member of GNSAGA of INdAM and of CrypTO, the group of Cryptography and Number Theory of Politecnico di Torino.

for all sufficiently large x.

In light of the gap between the upper bound of Theorem 1.1 and the lower bound (1) it is natural to wonder which is the true order of $\#\mathcal{A}(x)$. By performing some numerical experiments (see Section 4 later), we found that $\#\mathcal{A}(x)$ appears to be asymptotic to $x/(\log x)^c$, as $x \to +\infty$, for some constant $c \approx 0.63$, see Figure 1. Of course, these kind of experiments has to be taken with a grain of salt, since they cannot reveal slow-growing factors like $\log\log x$.

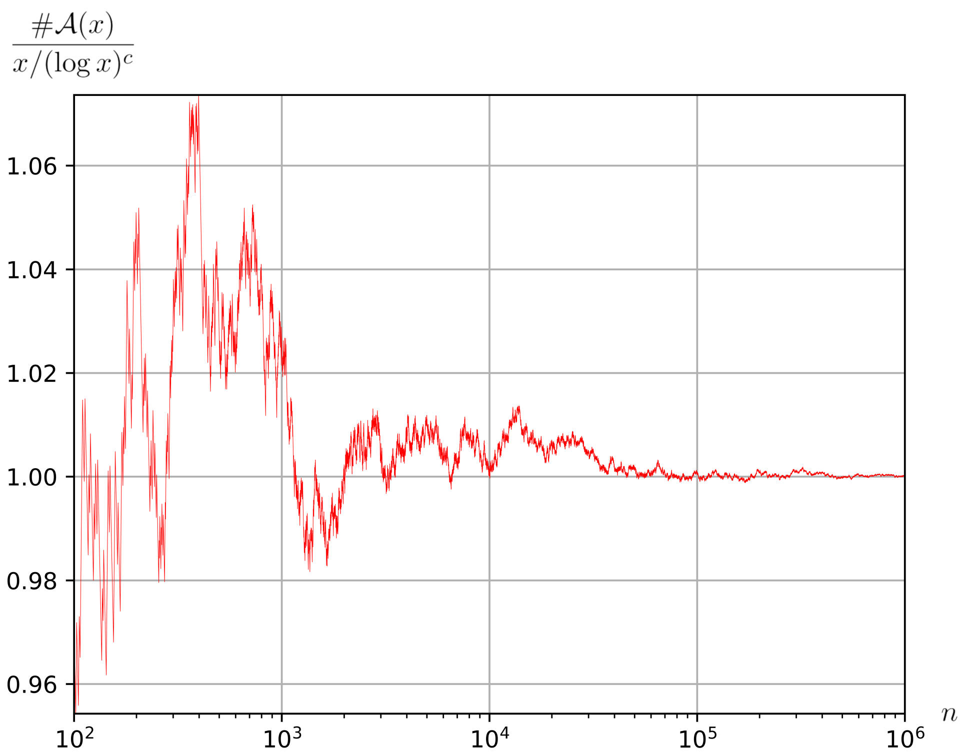

FIGURE 1. A plot of $\#\mathcal{A}(x)/(x/(\log x)^c)$ for x up to 10^6.

Notation. For every set of positive integers $\mathcal{S}$ and for every $x > 0$, we define $\mathcal{S}(x) := \mathcal{S} \cap [1, x]$. We employ the Landau–Bachmann "Big Oh" and "little oh" notation O and o, as well as the associated Vinogradov symbols $\ll$ and $\gg$. In particular, all of the implied constants are intended to be absolute. We let $\operatorname{Li}(x) := \int_2^x (\log t)^{-1}\,dt$ denote the integral logarithm.

2. Preliminaries

For each positive integer n, let $z(n)$ be the *rank of appearance* of n, that is, $z(n)$ is the smallest positive integer k such that n divides F_k. It is well known that $z(n)$ exists. Moreover, put $\ell(n) := \operatorname{lcm}\big(n, z(n)\big)$ and $g(n) := \gcd\big(n, F_n\big)$. The next lemma collects some elementary properties of z, ℓ, and g.

Lemma 2.1. *For all positive integer m, n and all prime numbers p, we have:*

(i) *$z(m) \mid z(n)$ whenever $m \mid n$.*

(ii) *$n \mid g(m)$ if and only if $\ell(n) \mid m$.*

(iii) *$n \in \mathcal{A}$ if and only if $n = g\big(\ell(n)\big)$.*

(iv) *$m \mid n$ whenever $\ell(m) \mid \ell(n)$ and $n \in \mathcal{A}$.*

(v) *$z(p) \mid p - (p/5)$ where $(p/5)$ is a Legendre symbol.*

(vi) $z(p^n) = p^{\max(n - e(p)\,,0)}\, z(p)$, *where* $e(p) := \nu_p(F_{z(p)}) \geq 1$ *and* ν_p *is the usual* p*-adic valuation.*

(vii) $\ell(p^n) = p^n z(p)$ *if* $p \neq 5$, *and* $\ell(5^n) = 5^n$.

Proof. For (i), (ii). and (iii), see [10, Lemma 2.1 and 2.2]. Fact (iv) follows easily from (ii) and (iii). Facts (vi) and (v) are well known (cf. [11, Lemma 1]). Fact (vii) follows quickly from (vi) and (v). □

For each positive integer d, let $\mathcal{P}_d$ be the set of prime numbers p such that d divides $z(p)$. Cubre and Rouse [4] proved that $\#\mathcal{P}_d(x) \sim \delta(d)\,\mathrm{Li}(x)$, as $x \to +\infty$, where

$$\delta(d) := \frac{1}{d}\prod_{p\,|\,d}\left(1 - \frac{1}{p^2}\right)^{-1}\begin{cases}1 & \text{if } 10 \nmid d;\\ 5/4 & \text{if } d \equiv 10 \pmod{20};\\ 1/2 & \text{if } 20 \mid d.\end{cases}$$

Sanna [16] extended this result to Lucas sequences (under some mild restrictions) and provided also an error term. In particular, as a consequence of [16, Theorem 1.1], we have the following asymptotic formula.

Lemma 2.2. *There exists an absolute constant* $B > 0$ *such that*

$$\#\mathcal{P}_d(x) = \delta(d)\,\mathrm{Li}(x) + O\!\left(\frac{x}{(\log x)^{12/11}}\right), \tag{2}$$

for all odd positive integers d *and for all* $x \geq \exp(Bd^{40})$.

Proof. From [16, Theorem 1.1] we have that there exists an absolute constant $B > 0$ such that

$$\#\mathcal{P}_d(x) = \delta(d)\,\mathrm{Li}(x) + O\!\left(\frac{d}{\varphi(d)} \cdot \frac{x\,(\log\log x)^{\omega(d)}}{(\log x)^{9/8}}\right),$$

for all odd positive integers d and for all $x \geq \exp(Bd^{40})$, where $\varphi(d)$ and $\omega(d)$ are the Euler totient function and the number of prime factors of d, respectively. Note that we can assume that B (and consequently x) is sufficiently large. In particular, we have that $d \leq (\log x)^{1/40}$. Put $\varepsilon := 1/330$. By the classic lower bound for $\varphi(d)$ (see, e.g., [22, Ch. I.5, Theorem 5.6]) we have that

$$\frac{d}{\varphi(d)} \ll \log\log d \ll \log\log\log x \leq (\log x)^{\varepsilon}.$$

Recall that $\omega(d) \leq \big(1 + o(1)\big)\log d/\log\log d$ as $d \to +\infty$ (see, e.g., [22, Ch. I.5, Theorem 5.5]). Therefore, there exists an absolute constant $C > 0$ such that if $d > C$ then

$$\omega(d) \leq (1+\varepsilon)\frac{\log d}{\log\log d} \leq \left(\frac{1}{40} + 2\varepsilon\right)\frac{\log\log x}{\log\log\log x},$$

and consequently $(\log\log x)^{\omega(d)} \leq (\log x)^{\frac{1}{40}+2\varepsilon}$. Also, if $d \leq C$ then $(\log\log x)^{\omega(d)} \leq (\log x)^{\varepsilon}$. The claim follows. □

Remark 2.1. In Lemma 2.2 the exponent $12/11$ can be replaced by $11/10 + \varepsilon$, for every $\varepsilon > 0$, assuming that x is sufficiently large depending on ε.

We also need an upper bound for $\#\mathcal{P}_d(x)$.

Lemma 2.3. *We have*

$$\#\mathcal{P}_d(x) \ll \frac{x}{\varphi(d)\log(x/d)}$$

for all positive integers d *and for all* $x > d$.

Proof. By Lemma 2.1(v), we have that

$$\#\mathcal{P}_d(x) \leq 1 + \#\big\{p \leq x : p \equiv \pm 1 \pmod{d}\big\} \ll \frac{x}{\varphi(d)\log(x/d)},$$

where we applied the Brun–Titchmarsh inequality [22, Ch. I.4, Theorem 4.16]. □

Now we give an upper bound for the sum of reciprocals of primes in $\mathcal{P}_d$.

Lemma 2.4. *We have*

$$\sum_{p \in \mathcal{P}_d(x)} \frac{1}{p} = \delta(d) \log\log x + O\left(\frac{\log(2d)}{\varphi(d)}\right)$$

for all odd positive integers d and for all $x \geq 3$.

Proof. First, suppose that $x < \exp(Bd^{40})$, where B is the constant of Lemma 2.2. Hence, we have that

$$\delta(d) \log\log x \ll \frac{\log\log x}{d} \ll \frac{\log(2d)}{d}.$$

Moreover, by [15, Theorem 1 and Remark 1], we have that

$$\sum_{\substack{p \leq x \\ p \equiv \pm 1 \pmod{d}}} \frac{1}{p} = \frac{2\log\log x}{\varphi(d)} + O\left(\frac{\log(2d)}{\varphi(d)}\right).$$

This together with Lemma 2.1(v) yields that

$$\sum_{p \in \mathcal{P}_d(x)} \frac{1}{p} \leq \frac{1}{d} + \sum_{\substack{p \leq x \\ p \equiv \pm 1 \pmod{d}}} \frac{1}{p} \ll \frac{1}{d} + \frac{\log(2d)}{\varphi(d)}.$$

Hence, the claim follows. Now suppose that $x \geq \exp(Bd^{40})$. By partial summation, we have that

$$\sum_{p \in \mathcal{P}_d(x)} \frac{1}{p} = \frac{\#\mathcal{P}_d(x)}{x} + \int_1^x \frac{\#\mathcal{P}_d(t)}{t^2}\, \mathrm{d}t.$$

Obviously, $\#\mathcal{P}_d(x)/x \ll 1/d$ by the trivial inequality. Thus it remains to bound the integral. By Lemma 2.1(v), we have that

$$\int_1^{2d} \frac{\#\mathcal{P}_d(t)}{t^2}\, \mathrm{d}t \leq \frac{1}{d^2} \int_1^{2d-2} 5 \, \mathrm{d}t \ll \frac{1}{d},$$

after noticing that $\#\mathcal{P}_d(t) > 0$ only if $t \geq d - 1$. By Lemma 2.3, we have that

$$\int_{2d}^{\exp(Bd^{40})} \frac{\#\mathcal{P}_d(t)}{t^2}\, \mathrm{d}t \ll \int_{2d}^{\exp(Bd^{40})} \frac{\mathrm{d}t}{\varphi(d)\, t \log(t/d)} = \left[\frac{\log\log(t/d)}{\varphi(d)}\right]_{t=2d}^{\exp(Bd^{40})} \ll \frac{\log d}{\varphi(d)}.$$

By Lemma 2.2, we have that

$$\begin{aligned}
\int_{\exp(Bd^{40})}^{x} \frac{\#\mathcal{P}_d(t)}{t^2}\, \mathrm{d}t &= \int_{\exp(Bd^{40})}^{x} \frac{\delta(d)\operatorname{Li}(t)}{t^2}\, \mathrm{d}t + O\left(\int_{\exp(Bd^{40})}^{x} \frac{\mathrm{d}t}{t(\log t)^{12/11}}\right) \\
&= \delta(d)\left[\log\log t - \frac{\operatorname{Li}(t)}{t}\right]_{t=\exp(Bd^{40})}^{x} + O\left(\frac{1}{d^{40/11}}\right) \\
&= \delta(d)\left(\log\log x + O(\log d)\right) + O\left(\frac{1}{d^{40/11}}\right) \\
&= \delta(d)\log\log x + O\left(\frac{\log d}{d}\right).
\end{aligned}$$

Putting these together, the claim follows. □

The following sieve result is a special case of [5, Theorem 7.2] (cf. [14, Lemma 2.2]).

Lemma 2.5. *We have*

$$\#\{n \leq x : p \mid n \Rightarrow p \notin \mathcal{P}\} \ll x \prod_{p \in \mathcal{P}(x)} \left(1 - \frac{1}{p}\right),$$

for all $x \geq 2$ and for all sets of prime numbers $\mathcal{P}$.

3. Proof of Theorem 1.1

Suppose that $x > 0$ is sufficiently large, and put

$$k := \left\lfloor \frac{1}{\log 5} \log\left(\frac{25}{24 \log 5} \cdot \frac{\log\log x}{\log\log\log x} \right) \right\rfloor$$

and $d := 5^k$. Note that $\delta(d) = 5^{-k} \cdot 25/24$. Hence, we get that

$$\log\left(\frac{\log d}{\delta(d)}\right) = k \log 5 + \log k + \log\left(\frac{24 \log 5}{25}\right) \leq \log\log\log x.$$

Therefore, we have that $(\log d)/\delta(d) \leq \log\log x$ and

$$(\log x)^{\delta(d)} \geq d \gg \frac{\log\log x}{\log\log\log x}. \tag{3}$$

We split $\mathcal{A}$ into two subsets: $\mathcal{A}_1$ is the subset of $\mathcal{A}$ consisting of integers without prime factors in $\mathcal{P}_d$, and $\mathcal{A}_2 := \mathcal{A} \setminus \mathcal{A}_1$.

First, we give an upper bound on $\#\mathcal{A}_1(x)$. By Lemma 2.5 and Lemma 2.4, we get that

$$\#\mathcal{A}_1(x) \ll x \prod_{p \in \mathcal{P}_d(x)} \left(1 - \frac{1}{p}\right) \ll x \exp\left(- \sum_{p \in \mathcal{P}_d(x)} \frac{1}{p} \right) \ll \frac{x}{(\log x)^{\delta(d)}}, \tag{4}$$

where we also used the inequality $1 - x \leq \exp(-x)$, which holds for $x \geq 0$.

Now we give an upper bound on $\#\mathcal{A}_2(x)$. If $n \in \mathcal{A}_2$ then n has a prime factor $p \in \mathcal{P}_d$. Hence, we have that $p \mid n$ and $d \mid z(p)$. Thus, by Lemma 2.1(i), we get that $z(p) \mid z(n)$ and so $d \mid \ell(n)$. Recalling that $d = 5^k$, by Lemma 2.1(vii) we have that $\ell(d) = d$. Hence, we get that $\ell(d) \mid \ell(n)$ and, by Lemma 2.1(iv), it follows that $d \mid n$. Thus all the elements of $\mathcal{A}_2$ are multiples of d. Consequently, we have that

$$\#\mathcal{A}_2(x) \leq \frac{x}{d}. \tag{5}$$

Therefore, putting together (4) and (5), and using (3), we obtain that

$$\#\mathcal{A}(x) = \#\mathcal{A}_1(x) + \#\mathcal{A}_2(x) \ll \frac{x}{(\log x)^{\delta(d)}} + \frac{x}{d} \ll \frac{x \log\log\log x}{\log\log x},$$

as desired. The proof is complete.

4. Numerical computations

We computed the elements of $\mathcal{A} \cap [1, 10^6]$ by using a program written in C that employs Lemma 2.1(iii). Note that computing $g\big(\ell(n)\big)$ directly as $\gcd\big(\ell(n), F_{\ell(n)}\big)$ would be prohibitive, in light of the exponential grown of Fibonacci numbers. Instead, we used the fact that

$$g\big(\ell(n)\big) = \gcd\big(\ell(n), F_{\ell(n)} \bmod \ell(n)\big),$$

and we computed Fibonacci numbers modulo an integer by efficient matrix exponentiation.

References

[1] OEIS Foundation Inc. (2022), The On-Line Encyclopedia of Integer Sequences, Published electronically at https://oeis.org.

[2] J. J. Alba González, F. Luca, C. Pomerance, and I. E. Shparlinski, *On numbers n dividing the nth term of a linear recurrence*, Proc. Edinb. Math. Soc. (2) **55** (2012), no. 2, 271–289.

[3] R. André-Jeannin, *Divisibility of generalized Fibonacci and Lucas numbers by their subscripts*, Fibonacci Quart. **29** (1991), no. 4, 364–366.

[4] P. Cubre and J. Rouse, *Divisibility properties of the Fibonacci entry point*, Proc. Amer. Math. Soc. **142** (2014), no. 11, 3771–3785.

[5] H. Halberstam and H.-E. Richert, *Sieve methods*, London Mathematical Society Monographs, No. 4, Academic Press [Harcourt Brace Jovanovich, Publishers], London-New York, 1974.

[6] A. Jha, *On terms in a dynamical divisibility sequence having a fixed G.C.D. with their index*, https://arxiv.org/abs/2105.06190.

[7] A. Jha and A. Nath, *The distribution of G.C.D.s of shifted primes and Lucas sequences*, https://arxiv.org/abs/2207.00825.
[8] A. Jha and C. Sanna, *Greatest common divisors of shifted primes and Fibonacci numbers*, https://arxiv.org/abs/2204.05161.
[9] S. Kim, *The density of the terms in an elliptic divisibility sequence having a fixed G.C.D. with their indices*, J. Number Theory **207** (2020), 22–41, With an appendix by M. Ram Murty.
[10] P. Leonetti and C. Sanna, *On the greatest common divisor of n and the nth Fibonacci number*, Rocky Mountain J. Math. **48** (2018), no. 4, 1191–1199.
[11] F. Luca and E. Tron, *The distribution of self-Fibonacci divisors*, Advances in the theory of numbers, Fields Inst. Commun., vol. 77, Fields Inst. Res. Math. Sci., Toronto, ON, 2015, pp. 149–158.
[12] D. Mastrostefano, *An upper bound for the moments of a gcd related to Lucas sequences*, Rocky Mountain J. Math. **49** (2019), no. 3, 887–902.
[13] D. Mastrostefano and C. Sanna, *On numbers n with polynomial image coprime with the nth term of a linear recurrence*, Bull. Aust. Math. Soc. **99** (2019), no. 1, 23–33.
[14] P. Pollack, *Numbers which are orders only of cyclic groups*, Proc. Amer. Math. Soc. **150** (2022), no. 2, 515–524.
[15] C. Pomerance, *On the distribution of amicable numbers*, J. Reine Angew. Math. **293(294)** (1977), 217–222.
[16] C. Sanna, *On the divisibility of the rank of appearance of a Lucas sequence*, Int. J. Number Theory, online ready, https://doi.org/10.1142/S1793042122501093.
[17] C. Sanna, *On numbers n dividing the nth term of a Lucas sequence*, Int. J. Number Theory **13** (2017), no. 3, 725–734.
[18] C. Sanna, *The moments of the logarithm of a G.C.D. related to Lucas sequences*, J. Number Theory **191** (2018), 305–315.
[19] C. Sanna, *On numbers n relatively prime to the nth term of a linear recurrence*, Bull. Malays. Math. Sci. Soc. **42** (2019), no. 2, 827–833.
[20] C. Sanna and E. Tron, *The density of numbers n having a prescribed G.C.D. with the nth Fibonacci number*, Indag. Math. (N.S.) **29** (2018), no. 3, 972–980.
[21] L. Somer, *Divisibility of terms in Lucas sequences by their subscripts*, Applications of Fibonacci numbers, Vol. 5 (St. Andrews, 1992), Kluwer Acad. Publ., Dordrecht, 1993, pp. 515–525.
[22] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, third ed., Graduate Studies in Mathematics, vol. 163, American Mathematical Society, Providence, RI, 2015, Translated from the 2008 French edition by Patrick D. F. Ion.
[23] E. Tron, *The greatest common divisor of linear recurrences*, Rend. Semin. Mat. Univ. Politec. Torino **78** (2020), no. 1, 103–124.

Indraprastha Institute of Information Technology,
Okhla Industrial Estate, Phase-3, New Delhi, India
Email address: abhishek20553@iiitd.ac.in

Department of Mathematical Sciences, Politecnico di Torino
Corso Duca degli Abruzzi 24, 10129 Torino, Italy
Email address: carlo.sanna.dev@gmail.com