View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by PORTO@iris (Publications Open Repository TOrino - Politecnico di Torino)

POLITECNICO DI TORINO
Repository ISTITUZIONALE

On the greatest common divisor of n and the nth Fibonacci number

Original
On the greatest common divisor of n and the nth Fibonacci number / Leonetti, Paolo; Sanna, Carlo. - In: ROCKY MOUNTAIN JOURNAL OF MATHEMATICS. - ISSN 0035-7596. - STAMPA. - 48:4(2018), pp. 1191-1199.

Availability:
This version is available at: 11583/2722598 since: 2020-05-03T09:57:49Z

Publisher:
Rocky Mountain Mathematics Consortium

Published
DOI:10.1216/RMJ-2018-48-4-1191

Terms of use:
openAccess

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

04 August 2020

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

PAOLO LEONETTI 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. We prove that $\#(\mathcal{A} \cap [1, x]) \gg x/\log x$ for all $x \geq 2$, and that $\mathcal{A}$ has zero asymptotic density. Our proofs rely on a recent result of Cubre and Rouse [Proc. Amer. Math. Soc. **142** (2014), 3771–3785] which gives, for each positive integer n, an explicit formula for the density of primes p such that n divides the rank of appearance of p, that is, the smallest positive integer k such that p divides F_k.

1. Introduction

Let $(F_n)_{n \geq 1}$ be the sequence of Fibonacci numbers, defined as usual by $F_1 = F_2 = 1$ and $F_{n+2} = F_{n+1} + F_n$, for all positive integers n. Moreover, let g be the arithmetic function defined by $g(n) := \gcd(n, F_n)$, for each positive integer n. The first values of g are listed in OEIS A104714 [13].

The set $\mathcal{B}$ of fixed points of g, i.e., the set of positive integers n such that n divides F_n, has been studied by several authors. For instance, André-Jeannin [2] and Somer [14] investigated the arithmetic properties of the elements of $\mathcal{B}$. Furthermore, Luca and Tron [8] proved that

$$\#\mathcal{B}(x) \leq x^{1-\left(\frac{1}{2}+o(1)\right)\log\log\log x/\log\log x}, \tag{1}$$

when $x \to +\infty$, and Sanna [12] generalized their result to Lucas sequences. More generally, the study of the distribution of positive integers n dividing the nth term of a linear recurrence has been studied by Alba González, Luca, Pomerance, and Shparlinski [1], while, Corvaja and Zannier [4], and Sanna [10] considered the distribution of positive integers n such that the nth term of a linear recurrence divides the nth term of another linear recurrence. Also, it follows from a result of Sanna [11] that the set $g^{-1}(1)$, i.e., the set of positive integers n such that n and F_n are relatively prime, has a positive asymptotic density.

Define $\mathcal{A} := \{g(n) : n \geq 1\}$. Note that, in particular, $\mathcal{B} \subseteq \mathcal{A}$. The aim of this article is to study the structural properties and the distribution of the elements of $\mathcal{A}$. Note that it is not immediately clear whether or not a given positive integer belongs to $\mathcal{A}$. To this aim, we provide in §2 an effective criterion which allows us to enumerate the elements of $\mathcal{A}$, in increasing order, as:

$$1,\ 2,\ 5,\ 7,\ 10,\ 12,\ 13,\ 17,\ 24,\ 25,\ 26,\ 29,\ 34,\ 35,\ 36,\ 37,\ \ldots$$

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

Key words and phrases. Fibonacci numbers, rank of appearance, greatest common divisor, natural density.

Our first result is a lower bound for the counting function of $\mathcal{A}$.

Theorem 1.1. *$\#\mathcal{A}(x) \gg x/\log x$, for all $x \geq 2$.*

It is worth noting that it follows at once from Theorem 1.1 and (1) that $\mathcal{B}$ has zero asymptotic density relative to $\mathcal{A}$ (we omit the details):

Corollary 1.2. *$\#\mathcal{B}(x) = o(\#\mathcal{A}(x))$, as $x \to +\infty$.*

Our second result is that $\mathcal{A}$ has zero asymptotic density:

Theorem 1.3. *$\#\mathcal{A}(x) = o(x)$, as $x \to +\infty$.*

It would be nice to have an effective upper bound for $\#\mathcal{A}(x)$ or, even better, to obtain its asymptotic order of growth. We leave these as open questions for the interested readers.

Notation. Throughout, we reserve the letters p and q for prime numbers. Moreover, given a set $\mathcal{S}$ of positive integers, we define $\mathcal{S}(x) := \mathcal{S} \cap [1, x]$ for all $x \geq 1$. We employ the Landau–Bachmann "Big Oh" and "little oh" notations O and o, as well as the associated Vinogradov symbols $\ll$ and $\gg$. In particular, all the implied constants are intended to be absolute, unless it is explicitly stated otherwise.

2. Preliminaries

This section is devoted to some preliminary results needed in the later proofs. For each positive integer n, let $z(n)$ be *rank of appearance of* n in the sequence of Fibonacci numbers, that is, $z(n)$ is the smallest positive integer k such that n divides F_k. It is well known that $z(n)$ exists. All the statements in the next lemma are well known, and we will use them implicitly without further mention.

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

(i) *$F_m \mid F_n$ whenever $m \mid n$.*
(ii) *$m \mid F_n$ if and only if $z(m) \mid n$.*
(iii) *$z(m) \mid z(n)$ whenever $m \mid n$.*
(iv) *$z(p) \mid p - \left(\frac{p}{5}\right)$, where $\left(\frac{p}{5}\right)$ is a Legendre symbol.*

For each positive integer n, define $\ell(n) := \operatorname{lcm}(n, z(n))$. The next lemma shows some elementary properties of the functions g, ℓ, z, and their relationship with $\mathcal{A}$.

Lemma 2.2. *For all positive integer m, n and all prime numbers p, we have:*

(i) *$g(m) \mid g(n)$ 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 $n = g(\ell(n))$.*
(iv) *$p \mid n$ whenever $\ell(p) \mid \ell(n)$ and $n \in \mathcal{A}$.*
(v) *$\ell(p) = pz(p)$ whenever $p \neq 5$, and $\ell(5) = 5$.*
(vi) *$p \in \mathcal{A}$ if $p \neq 3$ and $\ell(q) \nmid z(p)$ for all prime numbers q.*

Proof. Facts (i) and (ii) follow easily from the definitions of g and ℓ and the properties of z. To prove (iii), note that n divides both $\ell(n)$ and $F_{\ell(n)}$ hence $n \mid g(\ell(n))$ for all positive integers n. Conversely, if $n \in \mathcal{A}$, then $n = g(m)$ for some positive integer m. In particular, $n \mid g(m)$ which is equivalent to $\ell(n) \mid m$ by (ii). Therefore $g(\ell(n)) \mid$

$g(m) = n$, thanks to (i), and in conclusion $g(\ell(n)) = n$. Fact (iv) follows at once from (ii) and (iii).

A quick computation shows that $\ell(5) = 5$, while for all prime numbers $p \neq 5$ we have $\gcd(p, z(p)) = 1$, since $z(p) \mid p \pm 1$, so that $\ell(p) = pz(p)$, and this proves (v).

Lastly, let us suppose that $p \neq 3$ is a prime number such that $\ell(q) \nmid z(p)$ for all prime numbers q. In particular, $p \neq 5$ since $\ell(5) = z(5) = 5$, by (v). Also, the claim (vi) is easily seen to hold for $p = 2$. Hence, let us suppose hereafter that $p \geq 7$. Since $z(p) \mid p \pm 1$, it easily follows that $p \mid\mid g(\ell(p))$. At this point, if $q \mid g(\ell(p))$ for some prime $q \neq p$, then $\ell(q) \mid \ell(p) = pz(p)$ thanks to (ii). But $\ell(q) \nmid z(p)$, hence $p \mid \ell(q) = \operatorname{lcm}(q, z(q))$ so that $p \mid z(q) \leq q + 1$. Similarly, $q \mid g(\ell(p)) \mid \ell(p)$ implies $q \mid z(p) \leq p + 1$. Hence $|p - q| \leq 1$, which is impossible since $p \geq 7$. Therefore $q \nmid g(\ell(p))$, with the consequence that $p = g(\ell(p))$, i.e., $p \in \mathcal{A}$ by (iii). This concludes the proof of (vi). □

It is worth noting that Lemma 2.2(iii) provides an effective criterion to establish whether a given positive integer belongs to $\mathcal{A}$ or not. This is how we evaluated the elements of $\mathcal{A}$ listed in the introduction.

It follows from a result of Lagarias [6, 7], that the set of prime numbers p such that $z(p)$ is even has a relative density of $2/3$ in the set of all prime numbers. Bruckman and Anderson [3, Conjecture 3.1] conjectured, for each positive integer m, a formula for the limit

$$\zeta(m) := \lim_{x \to +\infty} \frac{\#\{p \leq x : m \mid z(p)\}}{x / \log x}.$$

Their conjecture was proved by Cubre and Rouse [5, Theorem 2], who obtained the following result.

Theorem 2.3. *For each prime number q and each positive integer e, we have*

$$\zeta(q^e) = \frac{q^{2-e}}{q^2 - 1},$$

while for any positive integer m, we have

$$\zeta(m) = \prod_{q^e \| m} \zeta(q^e) \cdot \begin{cases} 1 & \text{if } 10 \nmid m, \\ \frac{5}{4} & \text{if } m \equiv 10 \bmod 20, \\ \frac{1}{2} & \text{if } 20 \mid m. \end{cases}$$

Note that the arithmetic function ζ is not multiplicative. However, the restriction of ζ to the odd positive integers is multiplicative. This fact will be useful later.

Let φ be the Euler's totient function. We need the following technical lemma.

Lemma 2.4. *We have*

$$\sum_{q > y} \frac{1}{\varphi(\ell(q))} \ll \frac{1}{y^{1/4}},$$

for all $y > 0$.

Proof. For $\gamma > 0$, put $\mathcal{Q}_\gamma := \{p : z(p) < p^\gamma\}$. Clearly,

$$2^{\#\mathcal{Q}_\gamma(x)} \leq \prod_{p \in \mathcal{Q}_\gamma(x)} p \mid \prod_{n \leq x^\gamma} F_n \leq 2^{\sum_{n \leq x^\gamma} n} \leq 2^{O(x^{2\gamma})},$$

from which it follows that $\mathcal{Q}_\gamma(x) \ll x^{2\gamma}$.

Fix also $\varepsilon \in \,]0, 1-2\gamma[$. For the rest of this proof, all the implied constants may depend on γ and ε. Since $\varphi(n) \gg n/\log\log n$ for all positive integers n [15, Ch. I.5, Theorem 4], while, by Lemma 2.2(v), $\ell(q) \ll q^2$ for all prime numbers q, we have

$$\sum_{q>y} \frac{1}{\varphi(\ell(q))} \ll \sum_{q>y} \frac{\log\log \ell(q)}{\ell(q)} \ll \sum_{q>y} \frac{\log\log q}{\ell(q)} \ll \sum_{q>y} \frac{q^\varepsilon}{\ell(q)}, \tag{2}$$

for all $y > 0$.

On the one hand, again by Lemma 2.2(v),

$$\sum_{\substack{q>y \\ q\notin\mathcal{Q}_\gamma}} \frac{q^\varepsilon}{\ell(q)} \ll \sum_{\substack{q>y \\ q\notin\mathcal{Q}_\gamma}} \frac{1}{q^{1-\varepsilon} z(q)} \leq \sum_{q>y} \frac{1}{q^{1+\gamma-\varepsilon}} \ll \int_y^{+\infty} \frac{\mathrm{d}t}{t^{1+\gamma-\varepsilon}} \ll \frac{1}{y^{\gamma-\varepsilon}}. \tag{3}$$

On the other hand, by partial summation,

$$\begin{aligned}\sum_{\substack{q>y \\ q\in\mathcal{Q}_\gamma}} \frac{q^\varepsilon}{\ell(q)} \leq \sum_{\substack{q>y \\ q\in\mathcal{Q}_\gamma}} \frac{1}{q^{1-\varepsilon}} &= \frac{\#\mathcal{Q}_\gamma(t)}{t^{1-\varepsilon}}\bigg|_{t=y}^{+\infty} + (1-\varepsilon)\int_y^{+\infty} \frac{\#\mathcal{Q}_\gamma(t)}{t^{2-\varepsilon}}\,\mathrm{d}t \\ &\leq \int_y^{+\infty} \frac{\#\mathcal{Q}_\gamma(t)}{t^{2-\varepsilon}}\,\mathrm{d}t \ll \int_y^{+\infty} \frac{\mathrm{d}t}{t^{2-2\gamma-\varepsilon}} \ll \frac{1}{y^{1-2\gamma-\varepsilon}}. \end{aligned}\tag{4}$$

The claim follows by putting together (2), (3), and (4), and by choosing $\gamma = 1/3$ and $\varepsilon = 1/12$. □

Lastly, for all relatively prime integers a and m, define

$$\pi(x, m, a) := \#\{p \leq x : p \equiv a \bmod m\}.$$

We need the following version of the Brun–Titchmarsh theorem [9, Theorem 2].

Theorem 2.5. *If a and m are relatively prime integers and $m > 0$, then*

$$\pi(x, m, a) < \frac{2x}{\varphi(m)\log(x/m)},$$

for all $x > m$.

3. PROOF OF THEOREM 1.1

First, since $1 \in \mathcal{A}$, it is enough to prove the claim only for all sufficiently large x. Let $y > 5$ be a real number to be chosen later. Define the following sets of primes:

$$\begin{aligned}\mathcal{P}_1 &:= \{p : q \nmid z(p),\ \forall q \in [3, y]\}, \\ \mathcal{P}_2 &:= \{p : \exists q > y,\ \ell(q) \mid z(p)\}, \\ \mathcal{P} &:= \mathcal{P}_1 \setminus \mathcal{P}_2.\end{aligned}$$

We have $\mathcal{P} \subseteq \mathcal{A} \cup \{3\}$. Indeed, since $3 \mid \ell(2)$ and $q \mid \ell(q)$ for each prime number q, it follows easily that if $p \in \mathcal{P}$ then $\ell(q) \nmid z(p)$ for all prime numbers q, which, by Lemma 2.2(vi), implies that $p \in \mathcal{A}$ or $p = 3$.

Now we give a lower bound for $\#\mathcal{P}_1(x)$. Let P_y be the product of all prime numbers in $[3, y]$, and let μ be the Möbius function. By using the inclusion-exclusion principle and Theorem 2.3, we get that

$$\lim_{x\to+\infty} \frac{\#\mathcal{P}_1(x)}{x/\log x} = \lim_{x\to+\infty} \sum_{m \mid P_y} \mu(m) \cdot \frac{\#\{p \leq x : m \mid z(p)\}}{x/\log x} = \sum_{m \mid P_y} \mu(m)\zeta(m)$$
$$= \prod_{3\leq q\leq y} (1 - \zeta(q)) = \prod_{3\leq q\leq y} \left(1 - \frac{q}{q^2-1}\right),$$

where we also made use of the fact that the restriction of ζ to the odd positive integers is multiplicative.

As a consequence, for all sufficiently large x depending only on y, let say $x \geq x_0(y)$, we have

$$\#\mathcal{P}_1(x) \geq \frac{1}{2} \prod_{3\leq q\leq y} \left(1 - \frac{q}{q^2-1}\right) \cdot \frac{x}{\log x} \gg \frac{1}{\log y} \cdot \frac{x}{\log x},$$

where the last inequality follows from Mertens' third theorem [15, Ch. I.1, Theorem 11].

We also need an upper bound for $\#\mathcal{P}_2(x)$. Since $z(p) \mid p \pm 1$ for all primes $p > 5$, we have

$$\#\mathcal{P}_2(x) \leq \sum_{q>y} \#\{p \leq x : \ell(q) \mid z(p)\} \leq \sum_{q>y} \pi(x, \ell(q), \pm 1), \tag{5}$$

for all $x > 0$, where, for the sake of brevity, we put

$$\pi(x, \ell(q), \pm 1) := \pi(x, \ell(q), -1) + \pi(x, \ell(q), 1).$$

On the one hand, by Theorem 2.5 and Lemma 2.4, we have

$$\sum_{y<q<x^{1/2}} \pi(x, \ell(q), \pm 1) \ll \sum_{q>y} \frac{1}{\varphi(\ell(q))} \cdot \frac{x}{\log x} \ll \frac{1}{y^{1/4}} \cdot \frac{x}{\log x}. \tag{6}$$

On the other hand, by the trivial estimate for $\pi(x, \ell(q), \pm 1)$ and Lemma 2.4, we get

$$\sum_{q>x^{1/2}} \pi(x, \ell(q), \pm 1) \ll \sum_{q>x^{1/2}} \frac{x}{\ell(q)} \leq \sum_{q>x^{1/2}} \frac{x}{\varphi(\ell(q))} \ll x^{7/8}. \tag{7}$$

Therefore, putting together (5), (6), and (7), we find that

$$\#\mathcal{P}_2(x) \ll \frac{1}{y^{1/4}} \cdot \frac{x}{\log x} + x^{7/8}.$$

In conclusion, there exist two absolute constants $c_1, c_2 > 0$ such that

$$\#\mathcal{A}(x) \gg \#\mathcal{P}(x) \geq \#\mathcal{P}_1(x) - \#\mathcal{P}_2(x) \geq \left(\frac{c_1}{\log y} - \frac{c_2}{y^{1/4}} - \frac{c_2 \log x}{x^{1/8}}\right) \cdot \frac{x}{\log x}, \tag{8}$$

for all $x \geq x_0(y)$.

Finally, we can choose y to be sufficiently large so that

$$\frac{c_1}{\log y} - \frac{c_2}{y^{1/4}} > 0.$$

Hence, from (8) it follows that $\#\mathcal{A}(x) \gg x/\log x$, for all sufficiently large x.

4. Proof of Theorem 1.3

Fix $\varepsilon > 0$ and pick a prime number q such that $1/q < \varepsilon$. Let $\mathcal{P}$ be the set of prime numbers p such that $\ell(q) \mid z(p)$. By Theorem 2.3, we know that $\mathcal{P}$ has a positive relative density in the set of primes. As a consequence, we can pick a sufficiently large $y > 0$ so that

$$\prod_{p \in \mathcal{P}(y)} \left(1 - \frac{1}{p}\right) < \varepsilon.$$

Let $\mathcal{B}$ be the set of positive integers without prime factors in $\mathcal{P}(y)$. We split $\mathcal{A}$ into two subsets: $\mathcal{A}_1 := \mathcal{A} \cap \mathcal{B}$ and $\mathcal{A}_2 := \mathcal{A} \setminus \mathcal{A}_1$. If $n \in \mathcal{A}_2$ then n has a prime factor p such that $\ell(q) \mid z(p)$. Hence, $\ell(q) \mid \ell(n)$ and, by Lemma 2.2(iv), we get that $q \mid n$, so all the elements of $\mathcal{A}_2$ are multiples of q. In conclusion,

$$\limsup_{x \to +\infty} \frac{\#\mathcal{A}(x)}{x} \leq \limsup_{x \to +\infty} \frac{\#\mathcal{A}_1(x)}{x} + \limsup_{x \to +\infty} \frac{\#\mathcal{A}_2(x)}{x} \leq \prod_{p \in \mathcal{P}(y)} \left(1 - \frac{1}{p}\right) + \frac{1}{q} < 2\varepsilon,$$

and, by the arbitrariness of ε, it follows that $\mathcal{A}$ has zero asymptotic density.

References

1. 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.
2. R. André-Jeannin, *Divisibility of generalized Fibonacci and Lucas numbers by their subscripts*, Fibonacci Quart. **29** (1991), no. 4, 364–366.
3. P. S. Bruckman and P. G. Anderson, *Conjectures on the Z-densities of the Fibonacci sequence*, Fibonacci Quart. **36** (1998), no. 3, 263–271.
4. P. Corvaja and U. Zannier, *Finiteness of integral values for the ratio of two linear recurrences*, Invent. Math. **149** (2002), no. 2, 431–451.
5. P. Cubre and J. Rouse, *Divisibility properties of the Fibonacci entry point*, Proc. Amer. Math. Soc. **142** (2014), no. 11, 3771–3785.
6. J. C. Lagarias, *The set of primes dividing the Lucas numbers has density* 2/3, Pacific J. Math. **118** (1985), no. 2, 449–461.
7. J. C. Lagarias, *Errata to: "The set of primes dividing the Lucas numbers has density* 2/3*" [Pacific J. Math.* **118** *(1985), no. 2, 449–461]*, Pacific J. Math. **162** (1994), no. 2, 393–396.
8. 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.
9. H. L. Montgomery and R. C. Vaughan, *The large sieve*, Mathematika **20** (1973), 119–134.
10. C. Sanna, *Distribution of integral values for the ratio of two linear recurrences*, https://arxiv.org/abs/1703.10047.
11. C. Sanna, *On numbers n relatively prime to the nth term of a linear recurrence*, https://arxiv.org/abs/1703.10478.
12. C. Sanna, *On numbers n dividing the nth term of a Lucas sequence*, Int. J. Number Theory **13** (2017), no. 3, 725–734.
13. N. J. A. Sloane, *The on-line encyclopedia of integer sequences*, http://oeis.org, Sequence A104714.
14. 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.
15. G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, vol. 46, Cambridge University Press, Cambridge, 1995.

Università "Luigi Bocconi", Department of Statistics, Milan, Italy
E-mail address: leonetti.paolo@gmail.com
URL: http://orcid.org/0000-0001-7819-5301

Università degli Studi di Torino, Department of Mathematics, Turin, Italy
E-mail address: carlo.sanna.dev@gmail.com
URL: http://orcid.org/0000-0002-2111-7596