Greatest common divisors of shifted primes and Fibonacci numbers

GREATEST COMMON DIVISORS OF SHIFTED PRIMES AND FIBONACCI NUMBERS

ABHISHEK JHA AND CARLO SANNA

Abstract. Let (F_n) be the sequence of Fibonacci numbers and, for each positive integer k, let $\mathcal{P}_k$ be the set of primes p such that $\gcd(p-1, F_{p-1}) = k$. We prove that the relative density $\boldsymbol{r}(\mathcal{P}_k)$ of $\mathcal{P}_k$ exists, and we give a formula for $\boldsymbol{r}(\mathcal{P}_k)$ in terms of an absolutely convergent series. Furthermore, we give an effective criterion to establish if a given k satisfies $\boldsymbol{r}(\mathcal{P}_k) > 0$, and we provide upper and lower bounds for the counting function of the set of such k's.

As an application of our results, we give a new proof of a lower bound for the counting function of the set of integers of the form $\gcd(n, F_n)$, for some positive integer n. Our proof is more elementary than the previous one given by Leonetti and Sanna, which relies on a result of Cubre and Rouse.

1. Introduction

Let (u_n) be a non-degenerate linear recurrence with integral values. Several authors studied the arithmetic relations between u_n and n. For instance, under the mild hypothesis that the characteristic polynomial of (u_n) has only simple roots, Alba González, Luca, Pomerance, and Shparlinski [1] studied the set of positive integers n such that u_n is divisible by n. The same set was also studied by André-Jeannin [2], Luca and Tron [12], Sanna [16], and Somer [20], in the special case in which (u_n) is a Lucas sequence. Furthermore, Sanna [17] studied the set of natural numbers n such that $\gcd(n, u_n) = 1$ (see [14] for a generalization, and [23] for a survey on g.c.d.'s of linear recurrences). Similar problems, with (u_n) replaced by an elliptic divisibility sequence or by the orbit of a polynomial map, were also studied [3, 5, 6, 8, 9, 19].

Let (F_n) be the linear recurrence of Fibonacci numbers, which is defined as usual by $F_1 = F_2 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all positive integers n. For every positive integer k, define the following set of natural numbers

$$\mathcal{A}_k := \{n \geq 1 : \gcd(n, F_n) = k\},$$

Recall that the natural density $\boldsymbol{d}(\mathcal{S})$ of a set of positive integers $\mathcal{S}$ is defined as the limit of the ratio $\#\big(\mathcal{S} \cap [1, x]\big)/x$ as $x \to +\infty$, whenever this limit exists. Sanna and Tron [18] proved that each $\mathcal{A}_k$ has a natural density, which can be written as an infinite series, and they provided an effective criterion to determine if such density is positive.

2010 *Mathematics Subject Classification.* Primary: 11N32, Secondary: 11A41.

Key words and phrases. Fibonacci numbers; greatest common divisor; least common multiple; primes.

We consider similar results but for the set of *shifted primes* $p-1$. (Throughout, we reserve the letter p for prime numbers.) Shifted primes already make their appearance in relation to Fibonacci numbers. For instance, it is well known that p divides F_{p-1} for every prime number $p \equiv \pm 1 \pmod 5$. For each integer $k \geq 1$, define the following set of prime numbers

$$\mathcal{P}_k := \{p : \gcd(p-1, F_{p-1}) = k\}.$$

Recall that the *relative density* $\mathbf{r}(\mathcal{P})$ of a set of prime numbers $\mathcal{P}$ is defined as the limit of the ratio $\#(\mathcal{P} \cap [1,x])/\pi(x)$ as $x \to +\infty$, whenever this limit exists, where $\pi(x)$ denotes the number of primes not exceeding x. Let $z(m)$ denote the *rank of appearance*, or *entry point*, of a positive integer m in the sequence of Fibonacci numbers, that is, the smallest positive integer n such that m divides F_n. It is well known that $z(m)$ exists. Also, let $\ell(m) = \operatorname{lcm}\big(m, z(m)\big)$.

Our first result establishes the existence of the relative density of $\mathcal{P}_k$ and provides a criterion to check if such a density is positive.

Theorem 1.1. *For each positive integer k, the relative density of $\mathcal{P}_k$ exists. Moreover, if $\gcd\big(\ell(k), F_{\ell(k)}\big) \neq k$, or if $2 \nmid \ell(k)$ and $\ell(pk) = 2\,\ell(k)$ for some prime number p with $p \nmid k$, then $\mathcal{P}_k \subseteq \{2\}$. Otherwise, we have that $\boldsymbol{r}(\mathcal{P}_k) > 0$.*

For instance, $k = 17$ is the smallest positive integer such that $\boldsymbol{d}(\mathcal{A}_k) > 0$, since $\gcd\big(\ell(k), F_{\ell(k)}\big) = k$ (see Lemma 3.3 below) but $\boldsymbol{r}(\mathcal{P}_k) = 0$, since $\ell(k) = 153$ is odd and $\ell(pk) = 2\,\ell(k)$ for $p = 2$.

Our second result gives an explicit expression for the relative density of $\mathcal{P}_k$ in terms of an absolutely convergent series.

Theorem 1.2. *For each positive integer k, the relative density of $\mathcal{P}_k$ is*

$$\mathbf{r}(\mathcal{P}_k) = \sum_{d=1}^{\infty} \frac{\mu(d)}{\varphi(\ell(dk))},$$

where μ is the Möbius function, φ is the Euler totient function, and the series converges absolutely.

Leonetti and Sanna [11] proved the following upper and lower bounds for the counting function of the set $\mathcal{A} := \{\gcd(n, F_n) : n \geq 1\}$.

Theorem 1.3. *We have*

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

as $x \to +\infty$.

As an application of Theorem 1.1, we provide an alternative proof of the lower bound in (1). We remark that our proof uses quite elementary methods, while Leonetti and Sanna's proof relies on a result of Cubre and Rouse [4], which in turn is proved by Galois theory and Chebotarev's density theorem.

Let $\mathcal{K}$ be the set of positive integers k such that $\boldsymbol{r}(\mathcal{P}_k) > 0$. We have the following upper and lower bounds for the counting function of $\mathcal{K}$.

Proposition 1.4. *We have*

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

as $x \to +\infty$.

We remark that both Theorem 1.1 and Theorem 1.2 can be generalized to non-degenerate Lucas sequences, that is, integer sequences (u_n) such that $u_1 = 1$, $u_2 = a_1$, and $u_n = a_1 u_{n-1} + a_2 u_{n-2}$, for every integer $n \geq 2$, where a_1, a_2 are non-zero relatively prime integers such that the ratio of the roots of $X^2 - a_1 X - a_2$ is not a root of unity. We decided to focus on the sequence of Fibonacci numbers in order to simplify the exposition.

A generalization in another direction could be studying the sets of primes

$$\mathcal{P}_k^{(s)} := \{p : \gcd(p + s, F_{p+s}) = k\},$$

for integers $k \geq 1$ and s.

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

2. Preliminaries on primes in certain residue classes

We shall need a mild generalization (Theorem 2.2 below) of a result of Leonetti and Sanna [10] on primes in certain residue classes. First, we have to introduce some notation. For all $x \leq y$, let $[\![x, y]\!] := [x, y] \cap \mathbb{N}$. For vectors $\boldsymbol{x} = (x_1, \dots, x_d)$ and $\boldsymbol{y} = (y_1, \dots, y_d)$ in $\mathbb{N}^d$, let $\|\boldsymbol{x}\| := x_1 \cdots x_d$, $[\![\boldsymbol{x}, \boldsymbol{y}]\!] := [\![x_1, y_1]\!] \times \cdots \times [\![x_d, y_d]\!]$, $\boldsymbol{xy} := (x_1 y_1, \dots, x_d y_d)$, and $\boldsymbol{x}/\boldsymbol{y} := (x_1/y_1, \dots, x_d/y_d)$. Let $\boldsymbol{0}$, respectively $\boldsymbol{1}$, be the vector of $\mathbb{N}^d$ with all components equal to 0, respectively 1. For every $\boldsymbol{m} = (m_1, \dots, m_d) \in \mathbb{N}^d$, write $\boldsymbol{x} \equiv \boldsymbol{y} \pmod{\boldsymbol{m}}$ if and only if $x_i \equiv y_i \pmod{m_i}$ for each $i \in [\![1, d]\!]$, and write instead $\boldsymbol{x} \not\equiv \boldsymbol{y} \pmod{\boldsymbol{m}}$ if and only if $x_i \not\equiv y_i \pmod{m}$ for at least one $i \in [\![1, d]\!]$.

Lemma 2.1. *Let d be a positive integer and let $\boldsymbol{c}_1, \dots, \boldsymbol{c}_k, \boldsymbol{d} \in \mathbb{N}^d$ be vectors such that $\boldsymbol{c}_1 \cdots \boldsymbol{c}_k \equiv \boldsymbol{0} \pmod{\boldsymbol{d}}$ and $\boldsymbol{d} \equiv \boldsymbol{0} \pmod{\boldsymbol{c}_i}$ for each $i \in [\![1, k]\!]$. Then the set $\mathcal{X}$ of all $\boldsymbol{x} \in [\![\boldsymbol{1}, \boldsymbol{d}]\!]$ such that $\boldsymbol{x} \not\equiv \boldsymbol{0} \pmod{\boldsymbol{c}_i}$ for each $i \in [\![1, k]\!]$ satisfies*

$$\#\mathcal{X} \geq \|\boldsymbol{d}\| \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{\|\boldsymbol{c}_i\|}\right).$$

Proof. See [10, Lemma 2.1]. □

For all positive integers $a_0, \dots, a_k$, let $\mathcal{Q}(a_0, \dots, a_k)$ be the set of primes p such that $p \equiv 1 \pmod{a_0}$ and $p \not\equiv 1 \pmod{a_i}$ for every $i \in [\![1, k]\!]$.

Theorem 2.2. *Let $a_0, \dots, a_k$ be positive integers with $a_0 \mid a_i$ for each $i \in [\![1, k]\!]$. Then the relative density of $\mathcal{Q} := \mathcal{Q}(a_0, \dots, a_k)$ exists and satisfies*

$$\boldsymbol{r}(\mathcal{Q}) \geq \frac{1}{\varphi(a_0)} \prod_{i=1}^{k} \left(1 - \frac{\varphi(a_0)}{\varphi(a_i)}\right). \tag{2}$$

Proof. We generalize the proof of [10, Theorem 1.2], which corresponds to the special case $a_0 = 1$. Let $L := \operatorname{lcm}(a_0, \dots, a_k) = p_1^{e_1} \cdots p_d^{e_d}$ where $p_1 < \cdots < p_d$ are primes and $e_1, \dots, e_d$ are positive integers. Also, let $\mathcal{S}$ be the set of integers $n \in [1, L]$ such that: $\gcd(n, L) = 1$, $n \equiv 1 \pmod{a_0}$, and $n \not\equiv 1 \pmod{a_i}$ for every $i \in [\![1, k]\!]$. By Dirichlet's theorem on primes in arithmetic progressions, we have that

$$\begin{aligned} \boldsymbol{r}(\mathcal{Q}) &= \lim_{x \to +\infty} \frac{\#(\mathcal{Q} \cap [1, x])}{\pi(x)} \\ &= \lim_{x \to +\infty} \sum_{n \in \mathcal{S}} \frac{\#\{p \le x : p \equiv n \pmod{L}\}}{\pi(x)} = \frac{\#\mathcal{S}}{\varphi(L)}. \end{aligned} \tag{3}$$

Hence, the relative density of $\mathcal{Q}$ exists. Let us give a lower bound on $\#\mathcal{S}$.

First, assume that $8 \nmid L$. Let g_j be a primitive root modulo $p_j^{e_j}$, for each $j \in [\![1, d]\!]$. Note that g_1 exists when $p_1 = 2$ since $e_1 \le 2$. Put $\boldsymbol{b} := \big(\varphi(p_1^{e_1}), \dots, \varphi(p_d^{e_d})\big)$. By the Chinese remainder theorem, each $n \in [\![1, \ell]\!]$ with $\gcd(n, L) = 1$ is uniquely determined by a vector $\boldsymbol{y}(n) = (y_1(n), \dots, y_d(n)) \in [\![\boldsymbol{1}, \boldsymbol{b}]\!]$ such that $n \equiv g_j^{y_j(n)} \pmod{p_j^{e_j}}$ for each $j \in [\![1, d]\!]$. Write $a_i = p_1^{\alpha_{i,1}} \cdots p_d^{\alpha_{i,d}}$, where $\alpha_{i,1}, \dots, \alpha_{i,d} \ge 0$ are integers, and define $\boldsymbol{a}_i := \big(\varphi(p_1^{\alpha_{i,1}}), \dots, \varphi(p_d^{\alpha_{i,d}})\big)$ for each $i \in [\![0, k]\!]$. Also, put $\boldsymbol{c}_i = \boldsymbol{a}_i / \boldsymbol{a}_0$ for every $i \in [\![0, k]\!]$, $\boldsymbol{d} := \boldsymbol{b}/\boldsymbol{a}_0$, and let $\mathcal{X}$ be defined as in Lemma 2.1. At this point, it follows easily that $n \in \mathcal{S}$ if and only if $\boldsymbol{y}(n) \equiv \boldsymbol{0} \pmod{\boldsymbol{a}_0}$ and $\boldsymbol{y}(n) \not\equiv \boldsymbol{0} \pmod{\boldsymbol{a}_i}$ for each $i \in [\![1, k]\!]$. Therefore, the map $n \mapsto \boldsymbol{y}(n)/\boldsymbol{a}_0$ is a bijection $\mathcal{S} \to \mathcal{X}$ and, consequently, $\#\mathcal{S} = \#\mathcal{X}$. Since $\|\boldsymbol{d}\| = \varphi(L)/\varphi(a_0)$, $\|\boldsymbol{c}_i\| = \varphi(a_i)/\varphi(a_0)$, $\boldsymbol{c}_1 \cdots \boldsymbol{c}_k \equiv \boldsymbol{0} \pmod{\boldsymbol{d}}$, and $\boldsymbol{d} \equiv \boldsymbol{0} \pmod{\boldsymbol{c}_i}$ for each $i \in [\![1, k]\!]$, we can apply Lemma 2.1, which gives a lower bound on $\#\mathcal{X}$, that is, on $\#\mathcal{S}$. Then (3) and the lower bound on $\#\mathcal{S}$ yield (2).

Now let us consider the case in which $8 \mid L$. This is a bit more involved since there are no primitive roots modulo 2^e, for every integer $e \ge 3$. However, the previous arguments still work by changing $\boldsymbol{a}_i$ and $\boldsymbol{b}$ with

$$\boldsymbol{a}_i := \big(2^{\max(0, \alpha_{i,1}-1) - \max(0, \alpha_{i,1}-2)}, 2^{\max(0, \alpha_{i,1}-2)}, \varphi(p^{\alpha_{i,2}}), \dots, \varphi(p^{\alpha_{i,d}})\big)$$

and

$$\boldsymbol{b} = \big(2, 2^{e_1-2}, \varphi(p_2^{e_2}), \dots, \varphi(p_d^{e_d})\big).$$

Then each $n \in [\![1, \ell]\!]$ with $\gcd(n, L) = 1$ is uniquely determined by a vector $\boldsymbol{y}(n) = (y_0(n), \dots, y_d(n)) \in [\![\boldsymbol{1}, \boldsymbol{b}]\!]$ such that $n \equiv (-1)^{y_0(n)} 5^{y_1(n)} \pmod{2^{e_1}}$ and $n \equiv g_j^{y_j(n)} \pmod{p_j^{e_j}}$ for each $j \in [\![2, d]\!]$. The rest of the proof proceeds similarly to the previous case. □

For all positive integers $a_0, a_1, \dots$, let $\mathcal{Q}(a_0, a_1, \dots) := \bigcap_{k \ge 1} \mathcal{Q}(a_0, \dots, a_k)$.

Corollary 2.3. *If $a_0, a_1, \dots$ is a sequence of positive integers such that $a_0 \mid a_i$ for each integer $i \ge 1$ and the series $\sum_{i \ge 1} 1/\varphi(a_i)$ converges, then the relative density of $\mathcal{Q} := \mathcal{Q}(a_0, a_1, \dots)$ exists. Moreover, $\boldsymbol{r}(\mathcal{Q}) = 0$ if and only if there exists an integer $i \ge 1$ such that $a_i = a_0$, or $a_i = 2a_0$ and a_0 is odd. In such a case, we have that $\mathcal{Q} \subseteq \{2\}$.*

Proof. If there exists an integer $i \geq 1$ such that $a_i = a_0$, or $a_i = 2a_0$ and a_0 is odd, then it follows easily that $\mathcal{Q} \subseteq \{2\}$ and, consequently, $\boldsymbol{r}(\mathcal{Q}) = 0$. Hence, assume that no such integer i exists. In particular, we have that $\varphi(a_0) < \varphi(a_i)$ for every integer $i \geq 1$. From Theorem 2.2 we know that, for every integer $k \geq 1$, the relative density of $\mathcal{Q}_k := \mathcal{Q}(a_0, \ldots, a_k)$ exists and

$$r := \lim_{k \to +\infty} \boldsymbol{r}(\mathcal{Q}_k) \geq \frac{1}{\varphi(a_0)} \prod_{i=1}^{\infty} \left(1 - \frac{\varphi(a_0)}{\varphi(a_i)}\right) > 0,$$

where the infinite product converges to a positive number since $\sum_{i \geq 1} 1/\varphi(a_i)$ converges and $\varphi(a_0)/\varphi(a_i) < 1$ for every integer $i \geq 1$. Furthermore, for each $\varepsilon > 0$ and for every sufficiently large positive integer $k = k(\varepsilon)$, we have that

$$\limsup_{x \to +\infty} \left| r - \frac{\#(\mathcal{Q} \cap [1, x])}{\pi(x)} \right| < \varepsilon + \limsup_{x \to +\infty} \frac{\#\big((\mathcal{Q}_k \setminus \mathcal{Q}) \cap [1, x]\big)}{\pi(x)}$$

$$\leq \varepsilon + \limsup_{x \to +\infty} \frac{\#\{p \leq x : \exists j > k \text{ s.t. } p \equiv 1 \pmod{a_j}\}}{\pi(x)} \leq \varepsilon + \sum_{j > k} \frac{1}{\varphi(a_j)} < 2\varepsilon.$$

Therefore, the relative density of $\mathcal{Q}$ exists and, in fact, $\boldsymbol{r}(\mathcal{Q}) = r > 0$. □

3. Further preliminaries

The next lemma summarizes some basic properties of the Fibonacci numbers and the arithmetic functions ℓ and z.

Lemma 3.1. *For all positive integers m, n and all prime numbers p, we have:*

(i) $F_m \mid F_n$ *whenever* $m \mid n$.

(ii) $\gcd(F_m/F_n, F_n) \mid m/n$ *whenever* $n \mid m$.

(iii) $m \mid F_n$ *if and only if* $z(m) \mid n$.

(iv) $z(p) \mid p - \left(\frac{p}{5}\right)$ *where* $\left(\frac{p}{5}\right)$ *is a Legendre symbol.*

(v) $m \mid \gcd(n, F_n)$ *if and only if* $\ell(m) \mid n$.

(vi) $\ell(\operatorname{lcm}(m, n)) = \operatorname{lcm}(\ell(m), \ell(n))$.

(vii) $\ell(p) = z(p)p$ *for* $p \neq 5$, *and* $\ell(5) = 5$.

(viii) $\ell(n) \leq 2n^2$.

Proof. Facts (i)–(iv) are well known (for (ii), see [21, Lemma 2]). Facts (v)–(vii) follow easily from (iii) and (iv) and the definition of ℓ (cf. [18, Lemma 2.1]). Finally, fact (viii) follows easily from the well-known inequality $z(n) \leq 2n$ (see, e.g., [15]). □

Now we state a result to establish if $\mathcal{A}_k \neq \varnothing$ and $\boldsymbol{d}(\mathcal{A}_k) > 0$.

Lemma 3.2. $\mathcal{A}_k \neq \varnothing$ *if and only if* $\boldsymbol{d}(\mathcal{A}_k) > 0$ *if and only if* $\gcd\big(\ell(k), F_{\ell(k)}\big) = k$, *for all integers* $k \geq 1$.

Proof. See [18, Theorem 1.3]. □

Lemma 3.3. *Let k and n be positive integers. Suppose that $\mathcal{A}_k \neq \varnothing$. Then $n \in \mathcal{A}_k$ if and only if $\ell(k) \mid n$ and $m \nmid n$ for every*

$$m \in \{p\,\ell(k) : p \mid k\} \cup \{\ell(pk) : p \nmid k\}.$$

Proof. See [18, Lemma 3.1]. □

We need some upper bounds for series involving $\ell(n)$.

Lemma 3.4. *We have*

$$\sum_{n>y} \frac{1}{\ell(n)} < \exp\bigl(-\delta(\log y)^{1/2}(\log\log y)^{1/2}\bigr),$$

for all $\delta \in \bigl(0, 1/\sqrt{6}\bigr)$ and $y \gg_\delta 1$.

Proof. See [13, Proposition 1.4]. □

Lemma 3.5. *We have*

$$\sum_{n>y} \frac{1}{\varphi\bigl(\ell(n)\bigr)} \ll \frac{\log\log y}{\exp(\delta(\log y)^{1/2}(\log\log y)^{1/2})},$$

for all $\delta \in \bigl(0, 1/\sqrt{6}\bigr)$ and $y \gg_\delta 1$.

Proof. From Lemma 3.4 it follows that

$$S(t) := \sum_{n\geq t} \frac{1}{\ell(n)} < f(t) := \exp\bigl(-\delta(\log t)^{1/2}(\log\log t)^{1/2}\bigr),$$

for all $t \gg_\delta 1$. By partial summation, we obtain that

$$\begin{aligned}
\sum_{n\geq y} \frac{\log\log n}{\ell(n)} &= S(y)\log\log y + \int_y^{+\infty} \frac{S(t)}{t\log t}\,\mathrm{d}t \\
&< f(y)\log\log y + \int_y^{+\infty} \frac{f(t)}{t\log t}\,\mathrm{d}t \\
&\ll_\delta f(y)\log\log y - \int_y^{+\infty} f'(t)\,\mathrm{d}t \\
&\ll f(y)\log\log y.
\end{aligned}$$

Then, since $\varphi(n) \gg n/\log\log n$ (see, e.g., [22, Chapter I.5, Theorem 4]) and $\ell(n) \leq 2n^2$ (Lemma 3.1(viii)) for all positive integers n, we have that

$$\sum_{n>y} \frac{1}{\varphi\bigl(\ell(n)\bigr)} \ll \sum_{n>y} \frac{\log\log n}{\ell(n)} \ll f(y)\log\log y.$$

The claim follows. □

For every $x > 0$ and for all integers a and b, let $\pi(x; b, a)$ be the number of primes $p \leq x$ such that $p \equiv a \pmod b$, and put also

$$\Delta(x; b, a) := \pi(x; b, a) - \frac{\pi(x)}{\varphi(b)}.$$

We need the following bounds for $\Delta(x; b, a)$.

Theorem 3.6 (Siegel–Walfisz)**.** *For every $A > 0$, we have,*

$$\Delta(x; b, a) \ll \frac{x}{(\log x)^A},$$

for all $x \gg_A 1$ and for all relatively prime positive integers a, b with $b \leq (\log x)^A$.

Proof. See [7, Corollary 5.29]. □

Lemma 3.7. *Let $\varepsilon > 0$. Then we have that*

$$\Delta(x; b, a) \ll_\varepsilon \frac{x}{\varphi(b) \log x},$$

for all $x \geq 2$ and for all relatively prime positive integers a, b with $b \leq x^{1-\varepsilon}$.

Proof. From the Brun–Titchmarsh theorem [22, Theorem 9] we know that

$$\pi(x; b, a) \ll \frac{x}{\varphi(b) \log(x/b)},$$

for all $b < x$. Hence, the condition $b \leq x^{1-\varepsilon}$ and the upper bound $\pi(x) \ll x/\log x$ yield that

$$\Delta(x; b, a) \ll \pi(x; b, a) + \frac{\pi(x)}{\varphi(b)} \ll \frac{x}{\varphi(b) \log(x/b)} + \frac{x}{\varphi(b) \log x} \ll_\varepsilon \frac{x}{\varphi(b) \log x},$$

as desired. □

4. Proof of Theorem 1.1

Let k be a positive integer. If $\mathcal{P}_k = \varnothing$ then, obviously, the relative density of $\mathcal{P}_k$ exists and is equal to zero. Hence, suppose that $\mathcal{P}_k \neq \varnothing$. In particular, $\mathcal{A}_k \neq \varnothing$, since $p - 1 \in \mathcal{A}_k$ for every $p \in \mathcal{P}_k$. Therefore, by Lemma 3.2, we have that $\gcd\big(\ell(k), F_{\ell(k)}\big) = k$. Recall the definition of $\mathcal{Q}(a_0, a_1, \dots)$ given before Corollary 2.3. Define the sequence $\mathcal{M}_k = m_0, m_1, \dots$ where $m_0 < m_1 < \dots$ are all the elements of

$$\big\{\ell(k)\big\} \cup \big\{p\,\ell(k) : p \mid k\big\} \cup \big\{\ell(pk) : p \nmid k\big\}.$$

Then, from Lemma 3.3 and the definition of $\mathcal{Q}(\mathcal{M}_k)$, it follows that $\mathcal{P}_k = \mathcal{Q}(\mathcal{M}_k)$. Furthermore, by Lemma 3.5, we have that

$$\sum_{i \geq 0} \frac{1}{\varphi(m_i)} \ll_k \sum_p \frac{1}{\varphi\big(\ell(pk)\big)} \ll_k \sum_p \frac{1}{\varphi\big(\ell(p)\big)} < +\infty.$$

Hence, thanks to Corollary 2.3, we get that the relative density of $\mathcal{P}_k$ exists and, in particular, $\boldsymbol{r}(\mathcal{P}_k) = 0$ if and only if $\mathcal{P}_k \subseteq \{2\}$ if and only if there exists an integer $i \geq 1$ such that $m_i = m_0$, or $m_i = 2m_0$ and m_0 is odd. The first case is impossible, since the sequence $\mathcal{M}_k$ is increasing. The second case is equivalent to $2 \nmid \ell(k)$ and either $p\,\ell(k) = 2\,\ell(k)$, for some prime number p with $p \mid k$, or $\ell(pk) = 2\,\ell(k)$, for some prime number p with $p \nmid k$. In turn, since $k \mid \ell(k)$, this is equivalent to $2 \nmid \ell(k)$ and $\ell(pk) = 2\,\ell(k)$ for some prime number p with $p \nmid k$. The proof is complete.

Remark 4.1. *We remark that the convergence of the series*

$$\sum_p \frac{1}{\varphi\big(\ell(p)\big)}$$

admits a simpler proof than invoking Lemma 3.5 which we highlight below.

Proof. Note that $\ell(p) \gg p\, z(p) \gg p \log p$ due to Lemma 3.1(vii). Thus, we have that

$$\sum_p \frac{1}{\varphi\big(\ell(p)\big)} \ll \sum_p \frac{\log\log p}{p\, z(p)} \ll \sum_p \frac{\log\log p}{p \log p} < +\infty$$

since $\varphi(n) \gg n/\log\log n$ (see, e.g., [22, Chapter I.5, Theorem 4]) and $\ell(n) \le 2n^2$ (Lemma 3.1(viii)) for all positive integers n, and the convergence of last sum is standard . □

5. Proof of Theorem 1.2

For each positive integer k, let $\mathcal{R}_k$ be the set of prime numbers p such that:

(i) $k \mid \gcd(p-1, F_{p-1})$;

(ii) if $q \mid \gcd(p-1, F_{p-1})$ for some prime number q, then $q \mid k$.

The essential part of the proof of Theorem 1.2 is the following formula for the relative density of $\mathcal{R}_k$.

Lemma 5.1. *For all positive integers k, the relative density of $\mathcal{R}_k$ exists and*

$$\mathbf{r}(\mathcal{R}_k) = \sum_{(d,\,k)\,=\,1} \frac{\mu(d)}{\varphi\big(\ell(dk)\big)}, \tag{4}$$

where the series is absolutely convergent.

Proof. For every prime p and for every positive integer d, let us define

$$\varrho(p,d) := \begin{cases} 1 & \text{if } d \mid F_{p-1}, \\ 0 & \text{if } d \nmid F_{p-1}. \end{cases}$$

Note that ϱ is multiplicative in its second argument, that is,

$$\varrho(p, de) = \varrho(p,d)\, \varrho(p,e)$$

for all primes p and for all coprime positive integers d and e.

From Lemma 3.1(v), it follows easily that $p \in \mathcal{R}_k$ if and only if $p \equiv 1 \pmod{\ell(k)}$ and $\varrho(p,q) = 0$ for all prime numbers q dividing $p-1$ but not dividing k. Therefore,

$$\begin{aligned} \#\big(\mathcal{R}_k \cap [1,x]\big) &= \sum_{\substack{p \le x \\ \ell(k)\,\mid\, p-1}} \prod_{\substack{q \,\mid\, p-1 \\ q \nmid k}} \big(1 - \varrho(p,q)\big) = \sum_{\substack{p \le x \\ \ell(k)\,\mid\, p-1}} \sum_{\substack{d \,\mid\, p-1 \\ (d,\,k)\,=\,1}} \mu(d)\, \varrho(p,d) \\ &= \sum_{\substack{d \le x \\ (d,\,k)\,=\,1}} \mu(d) \sum_{\substack{p \le x \\ \operatorname{lcm}(\ell(k),\,d)\,\mid\, p-1}} \varrho(p,d), \end{aligned} \tag{5}$$

for all $x > 0$. Furthermore, by Lemma 3.1(iii), given a positive integer d that is relatively prime with k, we have that $\varrho(p,d) = 1$ and $\operatorname{lcm}(d, \ell(k)) \mid p-1$ if and only if $\operatorname{lcm}(z(d), d, \ell(k)) \mid p-1$, which in turn is equivalent to $p-1$ being divisible by

$$\operatorname{lcm}\big(\operatorname{lcm}\big(z(d), d\big), \ell(k)\big) = \operatorname{lcm}\big(\ell(d), \ell(k)\big) = \ell(dk),$$

where we used Lemma 3.1(vi) and the fact that d and k are relatively prime. Hence, we get that

$$\sum_{\substack{p \le x \\ \operatorname{lcm}(\ell(k),d) \,|\, p-1}} \varrho(p,d) = \sum_{\substack{p \le x \\ p \equiv 1 \pmod{\ell(dk)}}} 1 = \pi\big(x; \ell(dk), 1\big), \tag{6}$$

for all $x > 0$. Therefore, from (5) and (6), it follows that

$$\#\big(\mathcal{R}_k \cap [1,x]\big) = \sum_{\substack{d \le x \\ (d,k)=1}} \mu(d)\, \pi\big(x; \ell(dk), 1\big),$$

for all $x > 0$. Pick any $A > 2$. Also, set $y := x^{1/4}/\big(\sqrt{2}k\big)$ and $z := (\log x)^{A/2}/\big(\sqrt{2}k\big)$. Then we have that

$$\frac{\#\big(\mathcal{R}_k \cap [1,x]\big)}{\pi(x)} = \sum_{(d,k)=1} \frac{\mu(d)}{\varphi\big(\ell(dk)\big)} - E_1(x) + E_2(x) + E_3(x) + E_4(x)$$

for all $x > 0$, where, by Lemma 3.5, the infinite series converges absolutely, while

$$E_1(x) := \sum_{\substack{d > x \\ (d,k)=1}} \frac{\mu(d)}{\varphi\big(\ell(dk)\big)},$$

$$E_2(x) := \frac{1}{\pi(x)} \sum_{\substack{d \le z \\ (d,k)=1}} \mu(d)\, \Delta\big(x; \ell(dk), 1\big),$$

$$E_3(x) := \frac{1}{\pi(x)} \sum_{\substack{z < d \le y \\ (d,k)=1}} \mu(d)\, \Delta\big(x; \ell(dk), 1\big),$$

and

$$E_4(x) = \frac{1}{\pi(x)} \sum_{\substack{y < d \le x \\ (d,k)=1}} \mu(d)\, \Delta\big(x; \ell(dk), 1\big),$$

It remains only to prove that $E_1(x)$, $E_2(x)$, $E_3(x)$, $E_4(x)$ go to zero as $x \to +\infty$. From Lemma 3.5 it follows that

$$E_1(x) \ll \sum_{d > y} \frac{1}{\varphi\big(\ell(d)\big)} = o(1),$$

as $x \to +\infty$. Note that, thanks to Lemma 3.1(viii), if $d \le z$ then $\ell(dk) \le (\log x)^A$. Hence, from Theorem 3.6, we get that

$$E_2(x) \ll \frac{1}{\pi(x)} \cdot \frac{x}{(\log x)^A} \cdot z \ll \frac{1}{(\log x)^{A/2-1}} = o(1),$$

as $x \to +\infty$. Observe that due to Lemma 3.1(viii), if $d \le y$ then $\ell(dk) \le x^{1/2}$. Hence, applying Lemma 3.7 and Lemma 3.5, we get that

$$E_3(x) \ll \frac{1}{\pi(x)} \cdot \frac{x}{\log x} \cdot \sum_{d>z} \frac{1}{\varphi\big(\ell(dk)\big)} = o(1),$$

as $x \to +\infty$. Finally, using the trivial bound $\pi(x;b,1) \le x/b$ and Lemma 3.5, we get that

$$\begin{aligned} E_4(x) &\ll \frac{1}{\pi(x)} \sum_{d>y} \left(\frac{x}{\ell(dk)} + \frac{\pi(x)}{\varphi\big(\ell(dk)\big)} \right) \ll \frac{x}{\pi(x)} \sum_{d>y} \frac{1}{\varphi\big(\ell(dk)\big)} \\ &\ll \frac{\log x \log\log y}{\exp(\delta(\log y)^{1/2}(\log\log y)^{1/2})} = o(1), \end{aligned}$$

as $x \to +\infty$. The proof is complete. □

By the definition of $\mathcal{R}_k$ and by the inclusion-exclusion principle, it follows easily that

$$\#\big(\mathcal{P}_k \cap [1,x]\big) = \sum_{d \mid k} \mu(d)\, \#\big(\mathcal{R}_{dk}(x) \cap [1,x]\big)$$

for all $x > 0$. Therefore, by Lemma 5.1, we get that

$$\begin{aligned} \mathbf{r}(\mathcal{P}_k) &= \sum_{d \mid k} \mu(d)\, \mathbf{r}(\mathcal{R}_{dk}) = \sum_{d \mid k} \mu(d) \sum_{(e,dk)=1} \frac{\mu(e)}{\varphi\big(\ell(dek)\big)} \\ &= \sum_{d \mid k} \sum_{(e,k)=1} \frac{\mu(de)}{\varphi\big(\ell(dek)\big)} = \sum_{f=1}^{\infty} \frac{\mu(f)}{\varphi\big(\ell(fk)\big)}, \end{aligned} \tag{7}$$

since every squarefree integer f can be written uniquely as $f = de$, where d and e are squarefree integers such that $d \mid k$ and $\gcd(e,k) = 1$. The rearrangement of series in (7) is justified by the absolute convergence of the series of Lemma 5.1. The proof is complete.

6. Proof of the lower bound in (1) and Proposition 1.4

We need the following lemma.

Lemma 6.1. *Let k be a positive integer such that $10 \mid k$ and $\mathbf{r}(\mathcal{P}_k) > 0$, and let $p \in \mathcal{P}_k$. Then we have that $kp \in \mathcal{K}$.*

Proof. Since $p \in \mathcal{P}_k$, we have that $\gcd(p-1, F_{p-1}) = k$. Furthermore, since $5 \mid k$, we have that $p \equiv 1 \pmod 5$, and so $z(p) \mid p-1$ and $p \mid F_{p(p-1)}$ due to Lemma 3.1(iv) and (iii). In particular, $\gcd(p, F_{p(p-1)}) = p$. For the sake of brevity, put $g := \gcd(p-1, F_{p(p-1)})$. We shall proved that $g = k$. First, in light of Lemma 3.1(i), we have that $k \mid g$. Suppose that q is a prime factor of g/k. Then $q \ne p$ and $q \mid F_{p(p-1)}/F_{p-1}$. Furthermore, by Lemma 3.1(iii), we have that $z(q) \mid p(p-1)$. If $p \mid z(q)$ then, by Lemma 3.1(iv), $p \mid q-1$, which is impossible since $q \le p-1$. Thus $p \nmid z(q)$ and so $z(q) \mid p-1$. In particular, by

Lemma 3.1(iii), we get that $q \mid F_{p-1}$. Hence, Lemma 3.1(ii), yields that $q = p$, which is impossible. Therefore, we have that $g = k$. Consequently, we get that

$$\gcd\big(p(p-1), F_{p(p-1)}\big) = \gcd(p-1, F_{p(p-1)})\ \gcd(p, F_{p(p-1)}) = kp.$$

Thus $\mathcal{A}_{kp} \neq \varnothing$ and, by Lemma 3.2, we have that $\gcd\big(\ell(kp), F_{\ell(kp)}\big) = kp$. Also, since $2 \mid k$, we have that $2 \mid \ell(kp)$. Hence, from Theorem 1.1 it follows that $kp \in \mathcal{K}$, as desired. □

Let us prove the lower bound of Proposition 1.4. Note that $\ell(10) = 30$ and $\gcd(\ell(10), F_{\ell(10)}) = 10$ so that, by Theorem 1.1, we have that $\mathbf{r}(\mathcal{P}_{10}) > 0$. Hence, applying Lemma 6.1 with $k = 10$, we get that

$$\#\big(\mathcal{K} \cap [1, x]\big) \gg \#\big\{kp : p \in \mathcal{P}_k \cap [1, x/k]\big\} \gg \frac{x}{\log x}, \tag{8}$$

which proves the lower bound.

If $k \in \mathcal{K}$ then, by Theorem 1.1, we have that $\gcd\big(\ell(k), F_{\ell(k)}\big) = k$. Hence, from [11, Lemma 2.2(iii)], it follows that k belongs to $\mathcal{A}$. Therefore $\mathcal{K} \subseteq \mathcal{A}$. Consequently, on the one hand, by (8), we get that

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

for all $x \geq 2$, which is the lower bound of (1). On the other hand, by Theorem 1.3, we get that

$$\#\big(\mathcal{K} \cap [1, x]\big) \leq \#\big(\mathcal{A} \cap [1, x]\big) = o(x),$$

as $x \to +\infty$, which is the upper bound of Proposition 1.4. The proofs are complete.

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] A. S. Chen, T. A. Gassert, and K. E. Stange, *Index divisibility in dynamical sequences and cyclic orbits modulo p*, New York J. Math. **23** (2017), 1045–1063.

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

[5] T. A. Gassert and M. T. Urbanski, *Index divisibility in the orbit of 0 for integral polynomials*, Integers **20** (2020), Paper No. A16, 15.

[6] A. Gottschlich, *On positive integers n dividing the nth term of an elliptic divisibility sequence*, New York J. Math. **18** (2012), 409–420.

[7] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004.

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

[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, *A note on primes in certain residue classes*, Int. J. Number Theory **14** (2018), no. 8, 2219–2223.

[11] 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.
[12] 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.
[13] 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.
[14] 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.
[15] H. J. A. Sallé, *A maximum value for the rank of apparition of integers in recursive sequences*, Fibonacci Quart. **13** (1975), 159–161.
[16] C. Sanna, *On numbers n dividing the nth term of a Lucas sequence*, Int. J. Number Theory **13** (2017), no. 3, 725–734.
[17] 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.
[18] 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.
[19] J. H. Silverman and K. E. Stange, *Terms in elliptic divisibility sequences divisible by their indices*, Acta Arith. **146** (2011), no. 4, 355–378.
[20] 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.
[21] C. L. Stewart, *On divisors of Fermat, Fibonacci, Lucas, and Lehmer numbers*, Proc. London Math. Soc. (3) **35** (1977), no. 3, 425–447.
[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