Some Results on the Greatest Common Divisors of Terms of Linear Recurrences

Carlo Sanna

Group of Cryptography and Number Theory
Department of Mathematical Sciences
Politecnico di Torino
Italy

Overview of the Talk

- Introduction on G.C.D.-problems for Linear Recurrences.
- The G.C.D. of n and the nth Fibonacci number:
  - Fibers;
  - Image.
- The G.C.D. of $p-1$ and the $(p-1)$th Fibonacci number.
  - Fibers;
  - Image.

Introduction

Linear Recurrences

A sequence of integers $\boldsymbol{u} = (u_n)_{n\geq 0}$ is a **linear recurrence** of order k if there exist $a_1, \ldots, a_k \in \mathbb{Z}$, with $a_k \neq 0$, such that

$$u_n = a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k}, \tag{1}$$

for all integers $n \geq k$, and no similar relation holds for a smaller value of k.

In such a case, the polynomial

$$f_{\boldsymbol{u}}(X) = X^k - a_1 X^{k-1} - a_2 X^{k-2} - \cdots - a_k$$

is the **characteristic polynomial** of $\boldsymbol{u}$, while the terms

$$u_0, \quad u_1, \quad u_2, \quad \ldots\,, \quad u_{k-1}$$

are the **initial conditions** of $\boldsymbol{u}$.

Together, they completely determine $\boldsymbol{u}$ via (1).

Examples of Linear Recurrences

- Geometric progressions

$$q, \quad qr, \quad qr^2, \quad qr^3, \quad qr^4, \quad \dots$$

are linear recurrences of order 1 and characteristic polynomial $X - r$.

- Sequences of the form $(a^n - 1)_{n \geq 0}$, for fixed $a \in \mathbb{Z}$.

- The sequence of Fibonacci numbers $(F_n)_{n \geq 0}$

$$0, \quad 1, \quad 1, \quad 2, \quad 3, \quad 5, \quad 8, \quad 13, \quad 21, \quad \dots$$

is a linear recurrence of order 2 and char. polynomial $X^2 - X - 1$.

- Lucas sequences, which are a generalization of Fibonacci numbers (more details later).

- Every polynomial sequence $(p(n))_{n \geq 0}$, with $p(X) \in \mathbb{Z}[X]$, is a linear recurrence of order $k := \deg(p) + 1$ and char. polynomial $(X - 1)^k$.

G.C.D.s of Terms of Linear Recurrences (1/3)

Many authors have studied the G.C.D.s of terms of two linear recurrences.

A first important result is the following.

Theorem (Bugeaud, Corvaja, and Zannier 2003)

Let $a, b > 1$ *be multiplicatively independent integers and fix* $\varepsilon > 0$. *Then*

$$\gcd(a^n - 1, b^n - 1) < \exp(\varepsilon n),$$

for all sufficiently large n.

Bugeaud, Corvaja, and Zannier, An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$, *Mathematische Zeitschrift* **243** (2003), 79–84.

G.C.D.s of Terms of Linear Recurrences (2/3)

Of which many generalization/variations have been given. For instance:

Theorem (Fuchs 2003)

Let $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$ be linear recurrences whose characteristic polynomials have only positive real roots and such that $(u_n/v_n)_{n\geq 0}$ is not a linear recurrence. Then there exists an explicit constant $C \in (0,1)$ such that

$$\mathrm{gcd}(u_n, v_n) < \min(u_n, v_n)^C,$$

for all sufficiently large n.

Fuchs, An upper bound for the G.C.D. of two linear recurring sequences, *Mathematica Slovaca* **53** (2003), 21–42.

G.C.D.s of Terms of Linear Recurrences (2/3)

An extensive survey has been given by Tron.

Tron, *The greatest common divisor of linear recurrences*, Rendiconti Seminario Matematico dell'Università e del Politecnico di Torino **78**.1 (2020), 103–124.

In general, pointwise results are difficult to prove. In fact, the following conjecture is still open.

Conjecture (Ailon–Rudnick 2004)

If a and b are multiplicatively independent integers, then there exist infinitely many positive integers n such that

$$\gcd(a^n - 1, b^n - 1) = \gcd(a - 1, b - 1).$$

Ailon and Rudnick, Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$, *Acta Arithmetica* **113** (2004), 31–38.

The G.C.D. of n and F_n: Fibers

The Fiber $\mathcal{A}_k$

For each positive integer k, define the **fiber**

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

Recall that the **natural density** of a set of positive integers $\mathcal{S}$ is defined as

$$\mathbf{d}(\mathcal{S}) := \lim_{x \to +\infty} \frac{\#\mathcal{S}(x)}{x},$$

whenever this limit exists, and where $\mathcal{S}(x) := \mathcal{S} \cap [1, x]$ for all $x \geq 0$.

For each positive integer n let $z(n)$ denote the **rank of appearance** of n, that is, the smallest positive integer k such that n divides F_k.
(It can be proved that $z(n)$ exists.) Moreover, put $\ell(n) := \operatorname{lcm}(n, z(n))$.

The function ℓ has the property that $m \mid \gcd(n, F_n)$ if and only if $\ell(m) \mid n$.

The Density of $\mathcal{A}_k$

Theorem (S. and Tron 2018)

For each positive integer k, the natural density of $\mathcal{A}_k$ exists and we have

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

where μ is the Möbius function and the series converges absolutely.

Also, $\mathbf{d}(\mathcal{A}_k) > 0$ if and only if $\mathcal{A}_k \neq \varnothing$ if and only if $k = \gcd(\ell(k), F_{\ell(k)})$.

S. and Tron, The density of numbers *n* having a prescribed G.C.D. with the *n*th Fibonacci number, *Indagationes Mathematicae* **29** (2018), 972–980.

Let us see a sketch of the proof...

Sketch of the Proof: From $\mathcal{A}_k$ to $\mathcal{B}_k$ (1/2)

For each integer $k \geq 1$, let $\mathcal{B}_k$ be the set of positive integers n such that:

(i) k divides $\gcd(n, F_n)$;

(ii) if a prime number p divides $\gcd(n, F_n)$, then p divides k.

By a standard application of the inclusion-exclusion principle, we have

$$\#\mathcal{A}_k(x) = \sum_{d \mid k} \mu(d)\, \#\mathcal{B}_{dk}(x) \quad \text{for } x \geq 0. \tag{2}$$

At this point, it suffices to prove the following lemma.

Lemma

For each positive integer k, we have

$$\mathbf{d}(\mathcal{B}_k) = \sum_{\gcd(d,k)=1} \frac{\mu(d)}{\ell(dk)},$$

where the series converges absolutely.

Sketch of the Proof: From $\mathcal{A}_k$ to $\mathcal{B}_k$ (2/2)

Indeed, using (2) and the previous lemma, we get

$$\begin{aligned}\mathbf{d}(\mathcal{A}_k) &= \sum_{d \mid k} \mu(d)\,\mathbf{d}(\mathcal{B}_{dk}) = \sum_{d \mid k} \mu(d) \sum_{\gcd(e,dk)=1} \frac{\mu(e)}{\ell(dek)} \\ &= \sum_{d \mid k} \sum_{\gcd(e,dk)=1} \frac{\mu(de)}{\ell(dek)} = \sum_{f=1}^{\infty} \frac{\mu(f)}{\ell(fk)},\end{aligned}$$

since every squarefree positive integer f can be written in a unique way as $f = de$, where d and e are are squarefree positive integers such that $d \mid k$ and $\gcd(e, k) = 1$.

(The rearrangement of the series is justified by absolute convergence.)

Let us see how to prove the previous lemma...

Sketch of the Proof: A Counting Argument

For all positive integers n and d, define

$$\tau(n, d) = \begin{cases} 1 & \text{if } d \mid F_n, \\ 0 & \text{if } d \nmid F_n. \end{cases}$$

Clearly, $\tau(n, de) = \tau(n, d)\, \tau(n, e)$, for all relatively prime d and e.

Moreover, $n \in \mathcal{B}_k$ if and only if: (i) $\ell(k) \mid n$ and (ii) $\tau(n, p) = 0$ for all prime numbers p dividing n but not dividing k . Therefore,

$$\#\mathcal{B}_k(x) = \sum_{\substack{n \le x \\ \ell(k) \mid n}} \prod_{\substack{p \mid n \\ p \nmid k}} (1 - \tau(n, p)) = \sum_{\substack{n \le x \\ \ell(k) \mid n}} \sum_{\substack{d \mid n \\ \gcd(d,k) = 1}} \mu(d)\, \tau(n, d)$$

$$= \sum_{\substack{d \le x \\ \gcd(d,k) = 1}} \mu(d) \sum_{\substack{m \le x/d \\ \ell(k) \mid dm}} \tau(dm, d) = \sum_{\substack{d \le x \\ \gcd(d,k) = 1}} \mu(d) \left\lfloor \frac{x}{\ell(dk)} \right\rfloor,$$

where the last equality follows from the fact that $\tau(dm, d) = 1$ and that $\ell(k) \mid dm$ if and only if $\ell(dk)/d$ divides m.

Sketch of the Proof: The Error Term (1/2)

As a consequence,

$$\#\mathcal{B}_k(x) = x \sum_{\substack{d \leq x \\ \gcd(d,k)=1}} \frac{\mu(d)}{\ell(dk)} - R(x),$$

where

$$R(x) := \sum_{\substack{d \leq x \\ \gcd(d,k)=1}} \mu(d) \left\{ \frac{x}{\ell(dk)} \right\}.$$

Hence, in order to have

$$\mathbf{d}(\mathcal{B}_k) = \sum_{\gcd(d,k)=1} \frac{\mu(d)}{\ell(dk)},$$

we need to prove that $R(x) = o(x)$, as $x \to +\infty$.

Sketch of the Proof: The Error Term (2/2)

Actually, it suffices to prove that the series

$$\sum_{d=1}^{\infty} \frac{\mu(d)}{\ell(dk)}$$

converges absolutely.

Indeed, in such a case we have

$$|R(x)| \leq \sum_{d \leq x} |\mu(d)| \left\{ \frac{x}{\ell(dk)} \right\} \leq x^{1/2} + \sum_{d > x^{1/2}} |\mu(d)| \left\{ \frac{x}{\ell(dk)} \right\}$$

$$\leq x^{1/2} + x \sum_{d > x^{1/2}} \frac{|\mu(d)|}{\ell(dk)} = o(x), \qquad \text{as } x \to +\infty.$$

The convergence of the series is proved using properties of ℓ and some elementary bounds of Analytic Number Theory (we omit the details).

Sketch of the Proof: Positivity (1/2)

It remains to prove that $\mathbf{d}(\mathcal{A}_k) > 0$ if and only if $\mathcal{A}_k \neq \varnothing$ if and only if $k = \gcd(\ell(k), F_{\ell(k)})$.

The last equivalence is relatively easy, while proving the first equivalence is the difficult part.

In particular, working directly with the formula

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

seems hopeless.

Sketch of the Proof: Positivity (2/2)

For any set of positive integers $\mathcal{S}$, let $\mathcal{N}(\mathcal{S}) := \big\{n \geq 1 : s \nmid n, \ \ \forall s \in \mathcal{S}\big\}$.

Lemma

Let $\mathcal{S}$ be a set of positive integers such that

$$\sum_{s \in S} \frac{1}{s} < +\infty$$

and $\mathcal{N}(\mathcal{S})$ has a natural density. Then, $\mathbf{d}(\mathcal{N}(\mathcal{S})) > 0$ if and only if $1 \notin \mathcal{S}$.

Lemma

For each positive integer k such that $\mathcal{A}_k \neq \varnothing$, we have

$$\mathcal{A}_k = \big\{\ell(k)m : m \in \mathcal{N}(\mathcal{L}_k)\big\},$$

where $\mathcal{L}_k := \big\{p : p \mid k\big\} \cup \big\{\ell(kp)/\ell(k) : p \nmid k\big\}$.

Since it can be proved that $\sum_{s \in \mathcal{L}_k} 1/s < +\infty$ and that $1 \notin \mathcal{L}_k$, we get that $\mathbf{d}(\mathcal{A}_k) > 0$ if and only if $\mathcal{A}_k \neq \varnothing$, as claimed.

Generalization to Lucas Sequences (1/2)

A **Lucas sequence** is a linear recurrence $\boldsymbol{u} = (u_n)_{n \geq 0}$ satisfying

$$u_0 = 0, \quad u_1 = 1, \quad \text{and} \quad u_n = a_1 u_{n-1} + a_2 u_{n-2} \quad \text{for all } n \geq 2,$$

where a_1 and a_2 are fixed nonzero relatively prime integers.

A Lucas sequence is **nondegenerate** if the ratio of the roots of the characteristic polynomial $f_{\boldsymbol{u}}(X) = X^2 - a_1 X - a_2$ is not a root of unity.

For each positive integer k, define the fiber

$$\mathcal{A}_{\boldsymbol{u},k} := \{n \geq 1 : \gcd(n, u_n) = k\}.$$

For each positive integer n with $\gcd(n, a_2) = 1$, let $z_{\boldsymbol{u}}(n)$ be the **rank of appearance** of n in $\boldsymbol{u}$, i.e., the smallest positive integer k such that n divides u_k. (It can be proved that $z_{\boldsymbol{u}}(n)$ exists.)
Moreover, put $\ell_{\boldsymbol{u}}(n) := \operatorname{lcm}(n, z_{\boldsymbol{u}}(n))$.

Generalization to Lucas Sequences (2/2)

The proof of the previous theorem can be easily generalize to obtain:

Theorem (S. and Tron, 2018)

For each positive integer k, the natural density of $\mathcal{A}_{\boldsymbol{u},k}$ exists and we have

$$\mathbf{d}(\mathcal{A}_{\boldsymbol{u},k}) = \sum_{\gcd(d,a_2)=1} \frac{\mu(d)}{\ell_{\boldsymbol{u}}(dk)},$$

where the series converges absolutely.

Also, $\mathcal{A}_{\boldsymbol{u},k} \neq \varnothing$ if and only if $\gcd(k, a_2) = 1$ and $k = \gcd(\ell_{\boldsymbol{u}}(k), u_{\ell_{\boldsymbol{u}}(k)})$.

Further Remarks

An analog result for elliptic divisibility sequences was proved by Kim.

Kim, The density of the terms in an elliptic divisibility sequence having a fixed G.C.D. with their indices, *Journal of Number Theory* **207** (2020), 22–41.

The existence of the density has a generalization to linear recurrences.

Theorem (Mastrostefano and S. 2019)

Let $(u_n)_{n \geq 0}$ be a nondegenerate linear recurrence and let k be a positive integer. Then the set

$$\{n \geq 1 : \gcd(u_n, n) = k\}$$

has a natural density, which is zero if and only if the set is empty.

Mastrostefano and S., On numbers n with polynomial image coprime with the nth term of a linear recurrence, *Bulletin of the Australian Mathematical Society* **99** (2019), 23–33.

The G.C.D. of n and F_n: Image

Integers of the Form $\gcd(n, F_n)$

Let $\mathcal{G}$ be the set of all integers of the form $\gcd(n, F_n)$ for some integer $n \geq 1$.

For example, $10 \in \mathcal{G}$ since $10 = \gcd(30, 832040) = \gcd(30, F_{30})$.

Equivalently, we have that $\mathcal{G} = \{k \geq 1 : \mathcal{A}_k \neq \varnothing\}$.

The first elements of $\mathcal{G}$ are

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

It is not immediately clear how to establish if $n \in \mathcal{G}$.

An effective criterion is the following.

Lemma

$n \in \mathcal{G}$ if and only if $n = \gcd(\ell(n), F_{\ell(n)})$.

How Big is $\mathcal{G}$?

Numerical experiments suggest that $\#\mathcal{G}(x) \sim x/(\log x)^c$, as $x \to +\infty$, for some constant $c \approx 0.63$, but it is difficult to say.

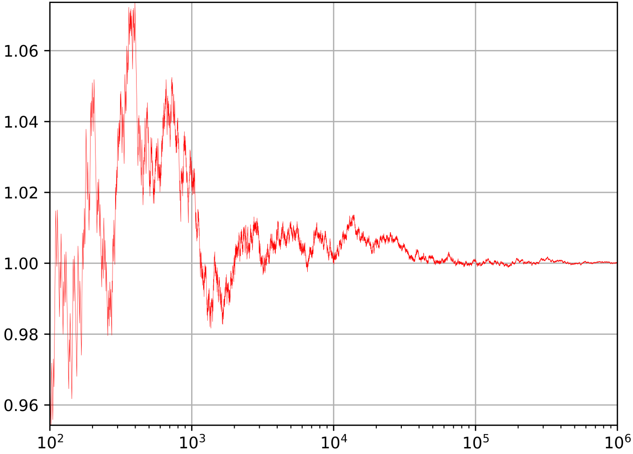

Figure: Plot of $\#\mathcal{G}(x)/(x/(\log x)^c)$ for $x \in [10^2, 10^6]$.

Upper and Lower Bounds

Theorem (Leonetti and S. 2018)

We have

$$\#\mathcal{G}(x) \gg \frac{x}{\log x}$$

for all $x \geq 2$*, while*

$$\#\mathcal{G}(x) = o(x)$$

as $x \to +\infty$*.*

Leonetti and S., On the greatest common divisor of *n* and the *n*th Fibonacci number, *Rocky Mountain Journal of Mathematics* **48** (2018), 1191–1199.

Key Tool in the Proofs of Upper and Lower Bounds (1/2)

Recall that the **relative density** of a set of prime numbers $\mathcal{P}$ is defined as

$$\mathbf{r}(\mathcal{P}) := \lim_{x \to +\infty} \frac{\#\mathcal{P}(x)}{x/\log x},$$

whenever this limit exists.

For each positive integer m, let

$$\mathcal{Z}_m := \{p \in \mathbb{P} : m \mid z(p)\},$$

where $\mathbb{P}$ is the set of prime numbers.

Key Tool in the Proofs of Upper and Lower Bounds (2/2)

The key tool in the proofs of the bounds for $\#\mathcal{G}(x)$ is the following result.

Theorem (Cubre and Rouse 2014)

For each integer $m \geq 1$, the relative density of $\mathcal{Z}_m$ exists and

$$\mathbf{r}(\mathcal{Z}_m) = \frac{r(m)}{m} \prod_{q^e \| m} \left(1 - \frac{1}{q^2}\right)^{-1},$$

where q^e runs over the prime powers in the factorization of m, while

$$r(m) := \begin{cases} 1 & \text{if } 10 \nmid m, \\ 5/4 & \text{if } m \equiv 10 \bmod 20, \\ 1/2 & \text{if } 20 \mid m. \end{cases}$$

Cubre and Rouse, Divisibility properties of the Fibonacci entry point, *Proceedings of the American Mathematical Society* **142** (2014), 3771–3785.

Sketch of the Proof of the Upper Bound (1/2)

Let us sketch the proof of the upper bound $\#\mathcal{G}(x) = o(x)$.

We have the following lemma.

Lemma

If $n \in \mathcal{G}$ and $\ell(q) \mid \ell(n)$ for some prime q, then q divides n.

Fix $\varepsilon > 0$ and pick a prime q such that $1/q < \varepsilon/2$. Moreover, put

$$\mathcal{Q} := \mathcal{Z}_{\ell(q)} = \{p : \ell(q) \mid z(p)\}.$$

By Cubre and Rouse's result, we have that $\mathcal{Q}$ has a positive relative density in the set of all primes. As a consequence, we can pick a sufficiently large $y > 0$ so that

$$\prod_{p \in \mathcal{Q}(y)} \left(1 - \frac{1}{p}\right) < \frac{\varepsilon}{2}.$$

Sketch of the Proof of the Upper Bound (2/2)

Now we split $\mathcal{G}$ into two subsets:

$$\begin{aligned} \mathcal{G}_1 &:= \{n \in \mathcal{G} : n \text{ has no prime factors in } \mathcal{Q}(y)\} \\ \mathcal{G}_2 &:= \mathcal{G} \setminus \mathcal{G}_1. \end{aligned}$$

If $n \in \mathcal{G}_2$, then n has a prime factor $p \in \mathcal{Q}(y)$, so that $\ell(q) \mid z(p)$. Hence, $\ell(q) \mid \ell(n)$ and, by the previous lemma, $q \mid n$. Thus all the elements of $\mathcal{G}_2$ are multiples of q.

In conclusion,

$$\begin{aligned} \limsup_{x \to +\infty} \frac{\#\mathcal{G}(x)}{x} &\leq \limsup_{x \to +\infty} \frac{\#\mathcal{G}_1(x)}{x} + \limsup_{x \to +\infty} \frac{\#\mathcal{G}_2(x)}{x} \\ &\leq \prod_{p \in \mathcal{Q}(y)} \left(1 - \frac{1}{p}\right) + \frac{1}{q} < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon, \end{aligned}$$

and, by the arbitraryness of ε, it follows that $\#\mathcal{G}(x) = o(x)$. □

An Improved Upper Bound

Recently, the upper bound has been improved as it follows.

Theorem (Jha and S. 2022)

We have

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

for all sufficiently large x.

Jha and S., On the greatest common divisor of n and the nth Fibonacci number, II, *Canadian Mathematical Bulletin* (in press).

In fact, the result has been proved more generally for nondegenerate Lucas sequences.

Divisibility of the Rank of Appearance

The improved upper bound was made possible by replacing the result of Cubre and Rouse with the following more precise asymptotic formula.

Theorem (S. 2022)

Let $\boldsymbol{u} = (u_n)_{n \geq 0}$ be a Lucas sequence satisfying some mild hypotheses [here omitted]. Then there exists a constant $B_{\boldsymbol{u}} > 0$ such that, for all odd integers $m \geq 1$ and for all $x \geq \exp(B_u m^{40})$, we have that

$$\#\{p \leq x : m \mid z_{\boldsymbol{u}}(p)\} = \delta_{\boldsymbol{u}}(m) \, \frac{x}{\log x} + O\left(\frac{x}{(\log x)^{12/11}}\right),$$

where $\delta_{\boldsymbol{u}}(m) > 0$ is given explicitly [here omitted].

S., On the divisibility of the rank of appearance of a Lucas sequence, *International Journal of Number Theory* **18** (2022), 2145–2156.

Gaps of the Bounds

In light of the previous results we have that

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

for all sufficiently large x.

Therefore, there is a large gap between the proved upper and lower bounds.

Open Problems

What is the true order of $\#\mathcal{G}(x)$?

Is it $\#\mathcal{G}(x) \sim x/(\log x)^c$ for some $c > 0$?

The G.C.D. of $p - 1$ and F_{p-1}: Fibers

Shifted Primes and Fibonacci Numbers

One can consider similar results but for the set of shifted primes $p - 1$.

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

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

Relative Density of $\mathcal{P}_k$

Theorem (Jha and S. 2022)

For each positive integer k, the relative density of $\mathcal{P}_k$ exists and we have

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

where φ is the Euler function and the series converges absolutely.

Moreover, if $\gcd(\ell(k), F_{\ell(k)}) \neq k$, or if $2 \nmid \ell(n)$ and $\ell(pk) = 2\,\ell(k)$ for some prime p with $p \nmid k$, then $\mathcal{P}_k \subseteq \{2\}$. Otherwise, we have that $\mathbf{r}(\mathcal{P}_k) > 0$.

Jha and S., Greatest common divisors of shifted primes and Fibonacci numbers, *Research in Number Theory* **8** (2022), Paper No. 65.

Some Remarks on the Proof

The proof of the formula for the relative density proceeds similarly to the proof of the formula for $\mathbf{d}(\mathcal{A}_k)$, but it requires results on prime numbers in arithmetic progressions (Siegel–Walfisz and Brun–Titchmarsh theorems).

The proof of the claim on $\mathbf{r}(\mathcal{P}_k) > 0$ requires the following theorem.

Theorem (Leonetti and S. 2018)

Let $m_1, \ldots, m_k$ be positive integers and let

$$\mathcal{Q} := \left\{ p \in \mathbb{P} : p \not\equiv 1 \pmod{m_i} \text{ for } i = 1, 2, \ldots, k \right\}.$$

Then $\mathcal{Q}$ has a relative density and

$$\mathbf{r}(\mathcal{Q}) \geq \prod_{i=1}^{k} \left(1 - \frac{1}{\varphi(m_i)} \right).$$

Leonetti and S., A note on primes in certain residue classes, *International Journal of Number Theory* **14** (2018), 2219–2223.

The G.C.D. of $p - 1$ and F_{p-1}: Image

Integers of the Form $\gcd(p-1, F_{p-1})$

Let $\mathcal{K}$ be the set of all integers of the form $\gcd(p-1, F_{p-1})$ for some prime number $p > 2$.

Equivalently, we have that $\mathcal{K} = \{k \geq 1 : \mathbf{r}(\mathcal{P}_k) > 0\}$.

Since $\mathcal{K} \subseteq \mathcal{G}$, from the upper bound on $\#\mathcal{G}(x)$ it follows that

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

for all sufficiently large x.

We also have the following lower bound.

Theorem (Jha and S. 2022)

We have that

$$\#\mathcal{K}(x) \gg \frac{x}{\log x},$$

for all sufficiently large x.

Further Remarks and Some Open Problems

The last theorem is proved by elementary methods only, especially not involving Cubre and Rouse's theorem or generalization thereof, which are based on Chebotarev density theorem. Therefore, since $\mathcal{K} \subseteq \mathcal{G}$, the last theorem yields an alternative proof of the lower bound for $\mathcal{G}$.

Open Problem

What is the true order of $\#\mathcal{K}(x)$?

Open Problem

What about $\gcd(p \pm 1, F_{p \pm 1})$ for the other three choices of signs?

Open Problem

Extend the previous results to Lucas sequences.

Thanks and References

Thanks for your Attention!