The g.c.d. of n and the n-th term of a linear recurrence
& related problems

Emanuele Tron

Université de Bordeaux

2nd Number Theory Meeting, Torino 26/10/2017

n	F_n
1	1
2	1
3	2
4	3
5	5
6	8
7	13
8	21
9	34
10	55
11	89
12	144
13	233
14	377
15	610
16	987
17	1597
18	2584
19	4181
20	6765
21	10946
22	17711
23	28657
24	46368
25	75025

n	F_n		
1	1	13	233
2	1	14	377
3	2	15	610
4	3	16	987
5	5	17	1597
6	8	18	2584
7	13	19	4181
8	21	20	6765
9	34	21	10946
10	55	22	17711
11	89	23	28657
12	144	24	46368
		25	75025

$n|F_n$? 1, 5, 12, 24, 25, 36, 48, 60, 72, 96, 108, 120, ...

n	F_n
1	1
2	1
3	2
4	3
5	5
6	8
7	13
8	21
9	34
10	55
11	89
12	144
13	233
14	377
15	610
16	987
17	1597
18	2584
19	4181
20	6765
21	10946
22	17711
23	28657
24	46368
25	75025

$n|F_n$? 1, 5, 12, 24, 25, 36, 48, 60, 72, 96, 108, 120, ...

$\gcd(n, F_n) = 1$? 1, 2, 3, 4, 7, 8, 9, 11, 13, 14, 16, 17, ...

Let $D := \{n \in \mathbb{N} : n | F_n\}$.

Let $D := \{n \in \mathbb{N} : n | F_n\}$.

Theorem (Alba González–Luca–Pomerance–Shparlinski 2010)

As $x \to \infty$,

$$\#D(x) \leq \frac{x}{\exp\left(((1 + o(1))\sqrt{\log x \log \log x}\right)}.$$

Let $D := \{n \in \mathbb{N} : n | F_n\}$.

Theorem (Alba González–Luca–Pomerance–Shparlinski 2010)

As $x \to \infty$,

$$\#D(x) \leq \frac{x}{\exp\left(((1+o(1))\sqrt{\log x \log\log x}\right)}.$$

Theorem (Luca–T. 2014)

$$\#D(x) \leq x^{1-(1/2+o(1))\log\log\log x/\log\log x}.$$

Let $D := \{n \in \mathbb{N} : n | F_n\}$.

Theorem (Alba González–Luca–Pomerance–Shparlinski 2010)

As $x \to \infty$,

$$\#D(x) \leq \frac{x}{\exp\left(((1 + o(1))\sqrt{\log x \log\log x}\right)}.$$

Theorem (Luca–T. 2014)

$$\#D(x) \leq x^{1-(1/2+o(1))\log\log\log x/\log\log x}.$$

Conjecture (Pomerance 1981, Luca–T. 2014)

$$\#D(x) = x^{1-(1+o(1))\log\log\log x/\log\log x}.$$

Set $z(n) := \min\{m \in \mathbb{N} : n | F_m\}$, $\mathcal{S}(k) := \{n \in \mathbb{N} : n/z(n) = k\}$.

Set $z(n) := \min\{m \in \mathbb{N} : n | F_m\}$, $\mathcal{S}(k) := \{n \in \mathbb{N} : n/z(n) = k\}$.

Lemma

One has $\mathcal{S}(k) = \varnothing$ if n has (almost) a square factor; otherwise if $k = \prod_i p_i$ then (almost)

$$\mathcal{S}(k) = \left\{ c(k) \prod_i p_i^{\beta_i} : \beta_i \in \mathbb{N} \right\}$$

for some integer $c(k)$.

Set $z(n) := \min\{m \in \mathbb{N} : n | F_m\}$, $\mathcal{S}(k) := \{n \in \mathbb{N} : n/z(n) = k\}$.

Lemma

One has $\mathcal{S}(k) = \varnothing$ if n has (almost) a square factor; otherwise if $k = \prod_i p_i$ then (almost)

$$\mathcal{S}(k) = \left\{ c(k) \prod_i p_i^{\beta_i} : \beta_i \in \mathbb{N} \right\}$$

for some integer $c(k)$.

Proof: if $n \in \mathcal{S}(k)$, look at which m have $mn \in \mathcal{S}(k)$ and inspect p-adic valuations. One needs the following.

Set $z(n) := \min\{m \in \mathbb{N} : n | F_m\}$, $\mathcal{S}(k) := \{n \in \mathbb{N} : n/z(n) = k\}$.

Lemma

One has $\mathcal{S}(k) = \varnothing$ if n has (almost) a square factor; otherwise if $k = \prod_i p_i$ then (almost)

$$\mathcal{S}(k) = \left\{ c(k) \prod_i p_i^{\beta_i} : \beta_i \in \mathbb{N} \right\}$$

for some integer $c(k)$.

Proof: if $n \in \mathcal{S}(k)$, look at which m have $mn \in \mathcal{S}(k)$ and inspect p-adic valuations. One needs the following.

Lemma

$$c(k) = k \operatorname{lcm}\{z^d(k) : d \in \mathbb{N}\}.$$

Let $C := \{n \in \mathbb{N} : \gcd(n, F_n) = 1\}$, $\ell(k) := \operatorname{lcm}(k, z(k))$.

Let $C := \{n \in \mathbb{N} : \gcd(n, F_n) = 1\}$, $\ell(k) := \operatorname{lcm}(k, z(k))$.

Theorem (Sanna 2017)

The set C has a positive asymptotic density.

Let $C := \{n \in \mathbb{N} : \gcd(n, F_n) = 1\}$, $\ell(k) := \operatorname{lcm}(k, z(k))$.

Theorem (Sanna 2017)

The set C has a positive asymptotic density.

Theorem (Sanna–T. 2017)

Let $C_k := \{n \in \mathbb{N} : \gcd(n, F_n) = k\}$. Then such a set has an asymptotic density for any k and the following are equivalent:

- C_k is nonempty;
- C_k has positive asymptotic density;
- $k = \gcd(\ell(k), F_{\ell(k)})$. (More on this in the next talk...)

Let $C := \{n \in \mathbb{N} : \gcd(n, F_n) = 1\}$, $\ell(k) := \operatorname{lcm}(k, z(k))$.

Theorem (Sanna 2017)

The set C has a positive asymptotic density.

Theorem (Sanna–T. 2017)

Let $C_k := \{n \in \mathbb{N} : \gcd(n, F_n) = k\}$. Then such a set has an asymptotic density for any k and the following are equivalent:

- C_k is nonempty;
- C_k has positive asymptotic density;
- $k = \gcd(\ell(k), F_{\ell(k)})$. (More on this in the next talk...)

Moreover, the asymptotic density admits an explicit expression as an absolutely convergent series:

$$d(C_k) = \sum_{n=1}^{\infty} \frac{\mu(n)}{\ell(nk)}.$$

Where does such an expression come from?

Where does such an expression come from? Set

$$\varrho(n,d) = \mathbb{1}_{d|F_n} = \begin{cases} 1, & d|F_n, \\ 0, & d \nmid F_n. \end{cases} \implies \prod_{p|n}(1-\varrho(n,p)) = \mathbb{1}_{\gcd(n,F_n)=1}$$

Where does such an expression come from? Set

$$\varrho(n,d) = \mathbb{1}_{d|F_n} = \begin{cases} 1, & d|F_n, \\ 0, & d \nmid F_n. \end{cases} \quad \Longrightarrow \quad \prod_{p|n}(1-\varrho(n,p)) = \mathbb{1}_{\gcd(n,F_n)=1}$$

Since $\varrho(n,d)$ is multiplicative in d,

$$\begin{aligned} \#C(x) &= \sum_{n\le x}\sum_{d|n}\mu(d)\varrho(n,d) \\ &= \sum_{d\le x}\mu(d)\sum_{m\le x/d}\mu(d)\varrho(dm,d) \\ &= \sum_{d\le x}\mu(d)\left\lfloor\frac{x}{\ell(d)}\right\rfloor = x\sum_{d\le x}\frac{\mu(d)}{\ell(d)} - R(x). \end{aligned}$$

Where does such an expression come from? Set

$$\varrho(n,d) = \mathbb{1}_{d|F_n} = \begin{cases} 1, & d|F_n, \\ 0, & d \nmid F_n. \end{cases} \quad \Longrightarrow \quad \prod_{p|n}(1-\varrho(n,p)) = \mathbb{1}_{\gcd(n,F_n)=1}$$

Since $\varrho(n,d)$ is multiplicative in d,

$$\begin{aligned} \#C(x) &= \sum_{n\le x}\sum_{d|n}\mu(d)\varrho(n,d) \\ &= \sum_{d\le x}\mu(d)\sum_{m\le x/d}\mu(d)\varrho(dm,d) \\ &= \sum_{d\le x}\mu(d)\left\lfloor\frac{x}{\ell(d)}\right\rfloor = x\sum_{d\le x}\frac{\mu(d)}{\ell(d)} - R(x). \end{aligned}$$

Then one goes on to prove that

$$R(x) := \sum_{d\le x}\mu(d)\left\{\frac{x}{\ell(d)}\right\} = o(x).$$

$$F_n \quad \longrightarrow \quad u_n,$$

u_n non-degenerate linear recurrence over the integers. Let $D_u := \{n \in \mathbb{N} : n | u_n\}$, $C_u := \{n \in \mathbb{N} : \gcd(n, u_n) = 1\}$.

$$F_n \quad \longrightarrow \quad u_n,$$

u_n non-degenerate linear recurrence over the integers. Let $D_u := \{n \in \mathbb{N} : n | u_n\}$, $C_u := \{n \in \mathbb{N} : \gcd(n, u_n) = 1\}$.

Theorem (Alba González–Luca–Pomerance–Shparlinski 2010)

If u is simple then

$$\#D_u(x) \ll \frac{x}{\log x}.$$

$$F_n \quad \longrightarrow \quad u_n,$$

u_n non-degenerate linear recurrence over the integers. Let $D_u := \{n \in \mathbb{N} : n | u_n\}$, $C_u := \{n \in \mathbb{N} : \gcd(n, u_n) = 1\}$.

Theorem (Alba González–Luca–Pomerance–Shparlinski 2010)

If u is simple then

$$\#D_u(x) \ll \frac{x}{\log x}.$$

Theorem (Alba González–Luca–Pomerance–Shparlinski 2010)

If u is a Lucas sequence, then

$$\exp\left(C(\log\log x)^2\right) \le \#D_u(x) \le \frac{x}{\exp\left(((1+o(1))\sqrt{\log x \log\log x}\right)}.$$

If additionally the sequence has $a_2 = \pm 1$ then $\#D_u(x) \ge x^{1/4+o(1)}$.

Theorem (Sanna 2015)

If u is a Lucas sequence, then

$$\#D_u(x) \leq x^{1-(1/2+o(1))\log\log\log x/\log\log x}.$$

Theorem (Sanna 2015)

If u is a Lucas sequence, then

$$\#D_u(x) \leq x^{1-(1/2+o(1))\log\log\log x/\log\log x}.$$

Theorem (Sanna 2017)

The set C_u has an asymptotic density, which is positive unless $(u_n/n)_{n\in\mathbb{N}}$ is a linear recurrence.

Theorem (Sanna 2015)

If u is a Lucas sequence, then

$$\#D_u(x) \leq x^{1-(1/2+o(1))\log\log\log x/\log\log x}.$$

Theorem (Sanna 2017)

The set C_u has an asymptotic density, which is positive unless $(u_n/n)_{n\in\mathbb{N}}$ is a linear recurrence.

Theorem (Sanna–T. 2017)

If u is a simple non-degenerate divisibility sequence, then results formally analogous to the Fibonacci case hold. For instance,

$$\frac{1}{x}\#\{n \leq x : \gcd(n, a^n - 1) = k\} \sim \sum_{\substack{d\in\mathbb{N}\\ \gcd(a,kd)=1}} \frac{\mu(d)}{\operatorname{lcm}(kd, \operatorname{ord}_a(kd))}.$$

$$n, F_n \quad \longrightarrow \quad u_n, v_n,$$

u_n, v_n non-degenerate linear recurrences over $\mathbb{Z}$. We take them to be simple (otherwise, methods of the previous case apply).
Let $D := \{n \in \mathbb{N} : u_n | v_n\}$.

$$n, F_n \quad \longrightarrow \quad u_n, v_n,$$

u_n, v_n non-degenerate linear recurrences over $\mathbb{Z}$. We take them to be simple (otherwise, methods of the previous case apply).
Let $D := \{n \in \mathbb{N} : u_n | v_n\}$. The main tool is the following.

Subspace Theorem (Schmidt 1972, Schlickewei 1977)

$K/\mathbb{Q}$ number field, S a finite set of absolute values containing the Archimedean ones. For each $v \in S$ let $L_1^\nu, \ldots, L_n^\nu$ be linearly independent linear forms in n variables with coefficients in K; let $\varepsilon > 0$. Then the solutions of

$$\prod_{\nu \in S} \prod_{i=1}^{n} |L_i^\nu(\mathbf{x})|_\nu < H(\mathbf{x})^{-\varepsilon}$$

with $\mathbf{x} \in \mathcal{O}_S^n$ lie in the union of finitely many subspaces of K^n, $H(x) = \prod_\nu \max(1, |x|_\nu)$ being the absolute Weil height of x.

Hadamard Quotient Theorem (Pourchet 1979, van der Poorten 1988)

If $D = \mathbb{N}$ then v_n/u_n is itself a linear recurrence.

Hadamard Quotient Theorem (Pourchet 1979, van der Poorten 1988)

If $D = \mathbb{N}$ then v_n/u_n is itself a linear recurrence.

Theorem (Corvaja–Zannier 1998)

If u, v are simple with positive integer roots, and if D is infinite, then the same conclusion holds. The same holds if we assume the *dominant root condition*.

Hadamard Quotient Theorem (Pourchet 1979, van der Poorten 1988)

If $D = \mathbb{N}$ then v_n/u_n is itself a linear recurrence.

Theorem (Corvaja–Zannier 1998)

If u, v are simple with positive integer roots, and if D is infinite, then the same conclusion holds. The same holds if we assume the *dominant root condition*.

Theorem (Corvaja–Zannier 2002)

If D is infinite, then there are a polynomial f and integers q, r such that $f(n)v_{qn+r}/u_{qn+r}$ and $u_{qn+r}/f(n)$ are linear recurrences. (No dominant root condition!)
If the roots generate a torsion-free multiplicative group and v_n/u_n is not a linear recurrence, then $\#D(x) = o(x)$.

Proof: Apply the Subspace Theorem to linear forms that look like

$$x_n^s \frac{v_n}{u_n} - v_n \sum_{i=0}^{s-1} \binom{s}{i} u_n^{s-1-i} y_n^i$$

(split $u_n = x_n - y_n$ and expand $x_n^s v_n / u_n = (u_n + y_n)^s v_n / u_n$); in other words, approximate v_n / u_n by truncating to an appropriate recurrence w_n. If there is no dominant root, use a trick to construct several more small linear forms out of this one.

Proof: Apply the Subspace Theorem to linear forms that look like

$$x_n^s \frac{v_n}{u_n} - v_n \sum_{i=0}^{s-1} \binom{s}{i} u_n^{s-1-i} y_n^i$$

(split $u_n = x_n - y_n$ and expand $x_n^s v_n / u_n = (u_n + y_n)^s v_n / u_n$); in other words, approximate v_n / u_n by truncating to an appropriate recurrence w_n. If there is no dominant root, use a trick to construct several more small linear forms out of this one.

Theorem (Sanna 2017)

If v_n / u_n is not a linear recurrence then

$$\#D(x) \ll x \left(\frac{\log \log x}{\log x} \right)^c$$

for some positive integer c. Assuming the Hardy–Littlewood h-tuples conjecture, this is optimal up to a power of $\log \log x$.

Theorem (Bugeaud–Corvaja–Zannier 2003)

Let a and b be multiplicatively independent positive integers. For any $\varepsilon > 0$ one has

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

for all large n.
If b is not a power of a then

$$\gcd(a^n - 1, b^n - 1) \ll a^{n/2}.$$

Theorem (Bugeaud–Corvaja–Zannier 2003)

Let a and b be multiplicatively independent positive integers. For any $\varepsilon > 0$ one has

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

for all large n.
If b is not a power of a then

$$\gcd(a^n - 1, b^n - 1) \ll a^{n/2}.$$

Proof: Apply the Subspace Theorem to the linear forms

$$\frac{b^{in} - 1}{a^n - 1} - \sum_{i=1}^{t} \frac{1}{a^{in}} + \sum_{j=1}^{t} \left(\frac{b^i}{a^j}\right)^n$$

obtained by truncating the expansion of $1/(a^n - 1)$.

Theorem (Fuchs 2003, Fuchs 2005)

u_n, v_n with positive integer roots, one of which coprime to all the others. Then for any $\varepsilon > 0$ one has

$$\gcd(u_n, v_n) < \exp(\varepsilon n)$$

for all large n (with effective constants).

Theorem (Fuchs 2003, Fuchs 2005)

u_n, v_n with positive integer roots, one of which coprime to all the others. Then for any $\varepsilon > 0$ one has

$$\gcd(u_n, v_n) < \exp(\varepsilon n)$$

for all large n (with effective constants).

Proof: Similar to Corvaja–Zannier, but even more technical–also needs several linear forms coming from different places.

Also some result in the mixed multiplicity case.

Theorem (Luca 2005)

f, p, g, q polynomials with integer coefficients, $\varepsilon > 0$, then

$$\gcd(f(n)a^n + p(n), g(n)b^n + q(n)) < \exp(\varepsilon n)$$

for all large n.

Also some result in the mixed multiplicity case.

Theorem (Luca 2005)

f, p, g, q polynomials with integer coefficients, $\varepsilon > 0$, then

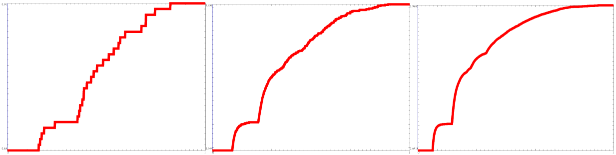
$$\gcd(f(n)a^n + p(n), g(n)b^n + q(n)) < \exp(\varepsilon n)$$

for all large n.

This kind of results comes from studying the $\gcd(u - 1, v - 1)$ for u, v S-units or near S-units (Corvaja–Zannier 2005): this has many more applications.

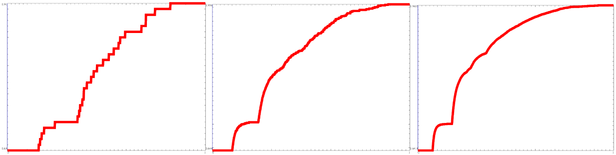
To do: we know the distribution of the n's for which $\gcd(n, F_n) \leq \alpha$ fixed and of those for which $\gcd(n, F_n) = n$.
It would be nice to extend our knowledge to $\gcd(n, F_n) \geq \beta n$, $0 < \beta < 1$ fixed (presumably not too hard); even more interesting to estimate (probably hard)

$$G_\varepsilon(x) := \#\{n \leq x : \gcd(n, F_n) \leq n^\varepsilon\}.$$



To do: we know the distribution of the n's for which $\gcd(n, F_n) \leq \alpha$ fixed and of those for which $\gcd(n, F_n) = n$.
It would be nice to extend our knowledge to $\gcd(n, F_n) \geq \beta n$, $0 < \beta < 1$ fixed (presumably not too hard); even more interesting to estimate (probably hard)

$$G_\varepsilon(x) := \#\{n \leq x : \gcd(n, F_n) \leq n^\varepsilon\}.$$



Thanks for your attention!

emanuele.tron@u-bordeaux.fr