The greatest common divisor of linear recurrences

Emanuele Tron

Rendiconti Sem. Mat. Univ. Pol. Torino
Vol. 78, 1 (2020), 103 – 124

E. Tron

THE GREATEST COMMON DIVISOR OF LINEAR RECURRENCES

Abstract. We survey the existing theory on the greatest common divisor $\gcd(u_n, v_n)$ of two linear recurrence sequences $(u_n)_n$ and $(v_n)_n$, with focus on recent development in the case where one of the two sequences is polynomial.

1. The problem

A *linear recurrence sequence* (or just *linear recurrence* for short) is a sequence $(u_n)_{n\in\mathbb{N}}$ specified by giving values $u_0, \dots, u_{d-1}$ and the condition that, for $n \geq d$,

$$u_{n+1} = \sum_{i=1}^{d} a_i u_{n+1-i}$$

for fixed $a_1, \dots, a_d$ and $a_d \neq 0$; the integer d is taken to be the least one for which a linear relation of this form holds and is called the *order* of the recurrence. All our recurrences will be assumed for simplicity to have rational integer terms, although the reader should keep in mind that much of what we are going to state holds with little to no change when they are instead defined over the ring of integers of a number field. The characteristic polynomial of the recurrence is $P(X) := X^d - \sum_{i=1}^{d} a_i X^{d-i}$ and its discriminant is $\Delta_u := \Delta(P)$: accordingly, the recurrence is called *simple* if the distinct roots of P (which are also referred to as the roots of u), say $\alpha_1, \dots, \alpha_r \in \mathbb{C}^\times$, are simple, and *non-degenerate* if no ratio α_i/α_j of any two distinct roots of P is a root of unity. Any term of the sequence can be expressed as a generalized power sum

$$u_n = \sum_{i=1}^{r} Q_i(n)\alpha_i^n$$

where the Q_i are polynomials over $\mathbb{C}$ whose degree is less than the multiplicity of α_i. The basic theory of linear recurrences will be assumed throughout, and we shall not develop it here but instead point to a general reference work such as the one of Everest–van der Poorten–Shparlinski–Ward [21] for further detail.

The problem that we are interested in is as follows. Given are two linear recurrences $(u_n)_n$ and $(v_n)_n$; what can one say about the quantity

$$g_n := \gcd(u_n, v_n)?$$

This can be thought as measuring the "arithmetical proximity" of u and v, as the G.C.D. puts together, for all non-archimedean places, how much the sequences share

(termwise) at each place. We will be interested in the distribution of the values of such a sequence, for instance in the counting function

$$G(x,y) := \#\{n \le x : g_n \ge y\};$$

this is slightly more convenient than the version with reversed inequality sign since one expects g_n to be often relatively small.

The plan is as follows. In Section 2 we shall see how one can bound large values of g_n when u and v are simple, by use of Schmidt's Subspace Theorem, and then interpret those bounds as cases of Vojta's conjecture. In Section 3 we will on the other hand see that if one recurrence is fully non-simple (one root with maximal multiplicity), almost everything concerning large and small values and averages of g_n can be determined. In Section 4, we will hint at how to translate the statements when studying other objects, such as elliptic divisibility sequences and meromorphic functions. We shall adopt an expository layout, with a focus on results over proofs.

We shall suppose, in each section, that the recurrence u (or the recurrences u and v) is fixed once and for all, so that all Vinogradov symbols depend on u in addition to other parameters: hence, read O_u, o_u, $\ll_u$, C_u (or $O_{u,v}$ etc.) for O, o, $\ll$, C respectively, which is the same as saying $O_{d,a_1,\dots,a_d}$ etc. The same is understood to hold for the objects that are meant to stand in place of linear recurrences in Sections 2 and 4.

2. The case with both recurrences non-degenerate

Throughout this section, we assume that the recurrences u and v are simple, and that their roots generate together a torsion-free multiplicative group (in particular, u and v are non-degenerate). This assumption is convenient in that it simplifies the statements of the theorems in the next sub-section, and does not entail a loss of generality [13, Sect. 1].

2.1. The Subspace Theorem and S-units

We first, and mostly, examine large values of g_n. For instance, what can one say on the cases when it is as large as possible, that is equal to $\min(|u_n|,|v_n|)$? The answer is given by the classical Hadamard Quotient Theorem.

THEOREM 1 (Pourchet [60], van der Poorten [59]). *Suppose that v_n divides u_n for all n.*[*] *Then $(u_n/v_n)_n$ is a linear recurrence.*

We may also rephrase the conclusion by saying that v has to divide u in the ring of linear recurrences.

Spectacular progress on the problem came next from exploiting the Subspace Theorem of Schmidt (as generalized by Schlickewei, Evertse, ...) in an ingenious

[*] Except possibly for those n for which $v_n = 0$, but there is a finite number of them—cf. the Skolem–Mahler–Lech theorem.

way; for the theorem itself the reader may see for instance Schmidt [68], or Bilu [6] for applications. The generalization that is used most often in applications involves all places of a number field and is due to Schlickewei.

THEOREM 2. *Suppose that K is a number field and S a finite set of places containing the Archimedean ones, $n \geq 1$ an integer. For each $\nu \in S$, let $L_{\nu,1}, \ldots, L_{\nu,n}$ be linearly independent linear forms in n variables defined over K. Then, for every fixed $\varepsilon > 0$, the nonzero solutions of*

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

with $x \in O_K^n$, lie in a finite union of proper subspaces of K^n.

First, a powerful improvement to the Hadamard Quotient Theorem was proved by Corvaja–Zannier [13]. If we only assume that the divisibility occurs for infinitely many n, then the quotient might not be a linear recurrence anymore, but it is almost so. The result is also remarkable for not requiring the so-called "dominant root condition", which had plagued many applications thus far.

THEOREM 3 (Corvaja–Zannier [13, Th. 1]). *Suppose that v_n divides u_n for infinitely many n. Then there is a polynomial $P(X) \in \mathbb{C}[X]$ such that both sequences $(P(n)u_n/v_n)_n$ and $(v_n/P(n))_n$ are linear recurrences.*

In quantitative form, they also prove that if $(u_n/v_n)_n$ is not a linear recurrence, then u_n/v_n can be an integer only for $o(x)$ values of $n \leq x$. This was made precise by Sanna [63], improving on a remark in Corvaja–Zannier [13, Cor. 2].

THEOREM 4 (Sanna [63, Th. 1.5], Corvaja–Zannier [13, Sect. 4]). *If $(u_n/v_n)_n$ is not a linear recurrence, then u_n/v_n can be an integer only for*

$$x \left(\frac{\log\log x}{\log x} \right)^C$$

values of $n \leq x$, for some explicit positive integer C. This is best possible up to a power of $\log\log x$.

The G.C.D. bounds were made quantitatively explicit in a series of works whose heart were more complex applications of the Subspace Theorem. We now consider sequences of the form $a^n - 1$ for simplicity. First, if $a = c^r$ and $b = c^s$, then the $\gcd(a^n - 1, b^n - 1)$ is as large as a power of $\min(a^n - 1, b^n - 1)$ for trivial reasons; we exclude this case by saying that a and b are multiplicatively independent. Apart from this case, the greatest common divisor is always smaller than any fixed power of the smallest of the two sequences.

THEOREM 5 (Bugeaud–Corvaja–Zannier [8, Th. 1]). *Let $a, b \geq 2$ be multiplicatively independent integers. Then for $n > n(\varepsilon)$,*

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

If b is not a power of a, then $\gcd(a^n - 1, b^n - 1) \ll a^{n/2}$ for large n.

This is close to best possible. Bugeaud–Corvaja–Zannier [8, Rem. 2] observe, after Adleman–Pomerance-Rumely [1, Prop. 10], that there are infinitely many n's that achieve $\exp(n^{c/\log\log n})$ (though they do not make a conjecture for the true maximal order; for instance, could it be $\exp(n^{(1+o(1))\log\log\log n/\log\log n})$?).

The start of the proof is as follows. For a positive integer i, write

$$z_i(n) := \frac{b^{in} - 1}{a^n - 1} = \frac{c_{i,n}}{d_n}$$

where $c_{i,n}$, d_n are integers, and d_n is taken as the denominator of $z_1(n)$.

Observe that for a fixed integer m we have the approximation

$$\frac{1}{a^n - 1} = a^{-n}\frac{1}{1 - a^{-n}} = a^{-n}\sum_{r=0}^{\infty} a^{-rn} = \sum_{r=1}^{m}\frac{1}{a^{rn}} + O(a^{-(m+1)n}).$$

If we multiply this by $b^{in} - 1$ we get

$$\left| z_i(n) + \sum_{s=1}^{m}\frac{1}{a^{sn}} - \sum_{r=1}^{m}\left(\frac{b^i}{a^r}\right)^n \right| = O(b^{in}a^{-(m+1)n});$$

the key idea is to see the left-hand side of this as a linear form in the variables $z_i(n)$, b^{in}/a^{rn}, a^{-sn}, for various values of i: if it were the case that $d_n \leq a^{(1-\varepsilon)n}$ infinitely often, then such forms would be small too often and contradict Theorem 2.

Corvaja–Rudnick–Zannier [12] prove a matrix generalization of this in the setting of periods of toral automorphisms. If B is a square matrix over $\mathbb{Z}$, we write $\gcd(B)$ for the greatest common divisor of the entries of B.

THEOREM 6 (Corvaja–Rudnick–Zannier [12, Th. 2]). *Suppose that $\varepsilon > 0$ is fixed and A is a square matrix of rational integers. Under some conditions on the eigenvalues of A, we have*

$$\gcd(A^n - I) < \exp(\varepsilon n)$$

for all large n.

The Bugeaud–Corvaja–Zannier bound is recovered as a special case of this, for the diagonal matrix $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$.

Fuchs [22], building on the work of Bugeaud–Corvaja–Zannier [8] and Hernández–Luca [35], further generalized the theorem as follows.

THEOREM 7 (Fuchs [22, Thms. 1 and 2]). *Suppose that u, v have only positive real roots, and that v does not divide u in the ring of linear recurrences. Then there is an explicit constant $C < 1$ such that for large n*

$$\gcd(u_n, v_n) < \min(|u_n|, |v_n|)^C.$$

If moreover all the roots of u, v are integer, u_n is of the form $ba^n + c$, and a is coprime to all the roots of v, then for sufficiently large n this can be strengthened to

$$\gcd(u_n, v_n) < \min(|u_n|, |v_n|)^\varepsilon.$$

A further generalization by Levin [43] concerns greatest common divisors of terms with distinct indices; we give a simplified version for the sake of exposition.

THEOREM 8 (Levin [43, Th. 1.11]). *Suppose that u, v are simple linear recurrences such that for each place ν of $\mathbb{Q}$ at least one of the roots α of u or v has $|\alpha|_\nu \geq 1$. If the inequality*

$$\gcd(u_n, v_m) < \exp(\varepsilon \max(m, n))$$

has infinitely many solutions (m, n), then all but finitely many of those solutions satisfy one of finitely many linear relations $(m, n) = (a_i k + b_i, c_i k + d_i)$ $(1 \leq i \leq t)$, where the linear recurrences $(u_{a_i n + b_i})_n$ and $(v_{c_i n + d_i})_n$ have a nontrivial common factor in the ring of linear recurrences for all i.

Another direction for generalizations starts from the observation that a^n is an S-unit for a finite S, so that theorems on terms of linear recurrences really are at their heart theorems concerning sums of S-units. Hence the following:

THEOREM 9 (Corvaja–Zannier [14, Th.], Hernández–Luca [35]). *Let $S \supseteq \{\infty\}$ be a finite set of rational primes and $\varepsilon > 0$ fixed. Then for all but finitely many multiplicatively independent S-units u, v we have*

$$\gcd(u - 1, v - 1) < \max(|u|, |v|)^\varepsilon.$$

Corvaja–Zannier also give further generalizations of these to $\gcd(F(u, v), G(u, v))$ [15] and versions in positive characteristic [17].

Further still, one can obtain bounds where u, v are just assumed to be "near" S-units–for instance, of the form $F(n)a^n$. This is the case in the following.

THEOREM 10 (Luca [46, Cor. 3.3]). *Let a, b be positive integers, and F_1, F_2, G_1, G_2 non-zero polynomials with integer coefficients, $\varepsilon > 0$ fixed. Then for all large m, n we have*

$$\gcd(F_1(n)a^n + G_1(n), F_2(n)b^n + G_2(n)) < \exp(\varepsilon n).$$

Grieve–Wang [31] combine the ideas of Levin and Luca to obtain a very general upper bound in the case of non-simple recurrences, by means of the moving form of the Subspace Theorem.

For more applications of the Subspace Theorem to linear recurrences we refer to Fuchs [23] and Corvaja–Zannier [18].

2.2. More over function fields

The problem of small values of $\gcd(u_n, v_n)$ is more obscure. Indeed, the following conjecture is open (and probably very difficult).

THEOREM 11 (Ailon–Rudnick [2, Conj. A]). *If a and b are multiplicatively independent integers, then there are infinitely many n for which*

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

Evidence for this was given by Silverman [75].

To avoid the obstacle, people have thus been trying to study what happens when a, b belong to other rings. The outcome can turn out to be far more satisfying.

THEOREM 12 (Ailon–Rudnick [2, Th. 1]). *If $F, G \in \mathbb{C}[x]$ are non-constant multiplicatively independent polynomials, then there is a polynomial $H \in \mathbb{C}[X]$ such that for any n*

$$\gcd(F^n - 1, G^n - 1) \text{ divides } H.$$

In particular, $\deg \gcd(F^n - 1, G^n - 1) \leq C_{F,G}$.

The idea of Ailon and Rudnick is very simple but relies crucially on a deep theorem of Ihara–Serre–Tate, which states that an irreducible curve in $\mathbb{C}^\times \times \mathbb{C}^\times$ can only contain finitely many points both of whose coordinates are roots of unity, unless it is defined by an equation of the form $X^m Y^n - \zeta = 0$ or $X^m - \zeta Y^n = 0$ with ζ a root of unity [84, Ch. 1.1]. Applying this to the curve $\{(F(t), G(t)) : t \in \mathbb{C}\}$ we find that $F(z)$ and $G(z)$ are simultaneously roots of unity for finitely many $z \in \mathbb{C}$.

Now, for any root t of $\gcd(F^n - 1, G^n - 1)$, both $F(t)$ and $G(t)$ must simultaneously be roots of unity, so there are only finitely many possible roots t for $\gcd(F^n - 1, G^n - 1)$. Moreover, since $F^n - 1 = \prod_{i=1}^{n-1}(F - \zeta_n^i)$ and the factors on the right-hand side are pairwise coprime, any $X - t$ can divide at most one of them with multiplicity at most $\deg F$, and the same for G. Hence, we may take $H(X) = \prod (X - t)^{\min(\deg F, \deg G)}$.

THEOREM 13 (Silverman [70, Th. 4]). *If $P, Q \in \mathbb{F}_q[x]$ are non-constant monic, then*

$$\deg \gcd(P^n - 1, Q^n - 1) \geq C_{P,Q} n.$$

for infinitely many n.[†]

Denis [20, Th. 1.1] gives lower bounds for the number of integers n for which $\deg \gcd(P^n - 1, Q^n - 1)$ is on the other hand bounded, and studies the analogous problem on Drinfeld modules. Cohen–Sonn generalize Silverman's theorem to the quantity $\gcd(\Phi_m(a^n), \Phi_m(b^n))$ with $(\Phi_m)_m$ the classical cyclotomic polynomials [10, Th. 2.1].

[†]Notice thus the trichotomy $\mathbb{Z}$–$\mathbb{C}[X]$–$\mathbb{F}_q[X]$ in the results, with profoundly different kinds of bounds in each case.

Corvaja–Zannier [17] give more generally estimates on the $\gcd(u-1,v-1)$ when u,v belong to a function field of positive characteristic, and derive a bound of Weil type from this.

For more applications, and an extensive development of such concepts in the area of unlikely intersections, see Zannier [84, Ch. 2]. We just mention in passing a nice application of these bounds due to Luca–Shparlinski [47], who exploit them to show that the groups $E(\mathbb{F}_{q^n})$ ($E/\mathbb{F}_q$ an ordinary elliptic curve) have a large cyclic factor; and a follow-up by Magagna [50, Th. 5] proving $\gcd(\#E_1(\mathbb{F}_{q^n}),\#E_2(\mathbb{F}_{q^n})) < \exp(\varepsilon n)$ if E,E' are ordinary and non-isogenous.

2.3. The geometric approach and Vojta's conjecture

We come back to the results of Section 2 to put them in a different light. The connection between G.C.D. bounds and Vojta's conjecture that we are going to see was first noticed by Silverman [72]. We recall here the statement of the conjecture in a form that suits applications; here we take the ambient variety X as fixed and fix a choice of height functions as well.

CONJECTURE 2 (Vojta). Let X/k be a smooth projective variety over a number field k and S a finite set of places of k, K_X a canonical divisor, A an ample divisor, D a divisor with normal crossings. Then for any $\varepsilon > 0$ there is a proper Zariski closed subset Z of X and a constant C such that, for all $P \in X(k)\setminus Z$, it holds that

$$\sum_{v\in S} \lambda_{D,v}(P) + h_{K_X}(P) \le \varepsilon h_A(P) + C.$$

This conjecture is very general and encompasses many open problems in Diophantine geometry. For our needs, the point is that *G.C.D. bounds and are essentially equivalent to cases of Vojta's conjecture*. We immediately state an instance of this.

THEOREM 14 (Silverman [72, Th. 1]). *We let $|x|'_S$ be the prime-to-S part of x, i.e. the largest divisor of x that is not divisible by any prime in S. Let S be a finite set of places, $F_1,\dots,F_t \in \mathbb{Z}[X_1,\dots,X_n]$ homogeneous polynomials such that their zero set V is a smooth variety in $\mathbb{P}^n$ which does not intersect any hyperplane $\{X_i = 0\}$; let $r := n - \dim V$. Assume Vojta's conjecture for $\mathbb{P}^n$ blown up along V and fix $\varepsilon > 0$. Then there is a homogeneous $G \in \mathbb{Z}[X_1,\dots,X_n]$ and a constant $\delta > 0$ such that for any $n+1$-tuple of coprime integers $x_0,\dots,x_n \in \mathbb{Z}$ either $G(x_0,\dots,x_n) = 0$ or*

$$\gcd(F_1(x_0,\dots,x_n),\dots,F_t(x_0,\dots,x_n)) \le \max(|x_0|,\dots,|x_n|)^{\varepsilon}(|x_0\cdots x_n|'_S)^{1/(r-1+\delta\varepsilon)}.$$

If we apply for instance this with $n=2$, $F_1 = X_1 - X_0$, $F_2 = X_2 - X_0$, this theorem says that outside a one-dimensional set we have

$$\gcd(x_1 - x_0, x_2 - x_0) \le \max(|x_0|,|x_1|,|x_2|)^{\varepsilon}(|x_0x_1x_2|'_S)^{1/(1+\delta\varepsilon)}.$$

If we specialize further to $x_0 = 1$ and x_1, x_2 S-units, this becomes

$$\gcd(x_1 - 1, x_2 - 1) \le \max(|x_1|,|x_2|)^{\varepsilon}$$

and we recover Theorem 9 (up to the exceptional set, which is however not hard to determine). As for the proof of Theorem 14 itself, it involves Vojta's conjecture with $X=\mathbb{P}^n$, $A=\{X_0=0\}$, $D=-\pi^*K_X=-\pi^*\sum_{i=0}^n\{X_i=0\}$ and π the blow-up of X along $\{F_1=\cdots=F_t=0\}$.

Instead of explaining the general proof, let us just see where the analogy starts from [72, Sect. 2]. One writes for $a,b\in\mathbb{Q}$

$$\log\gcd(a,b)=\sum_p \min(\nu_p(a),\nu_p(b))\log p=\sum_{\nu\in M_{\mathbb{Q}}^0}\min(\nu(a),\nu(b));$$

for general a, b in a number field we then define

$$\log\gcd(a,b):=\sum_{\nu\in M_k}\min(\nu^+(a),\nu^+(b)).$$

To bring heights into play, we note that ν^+ is the local height function on $\mathbb{P}^1(k)$ with respect to the divisor (0). We would like a similar height-theoretic interpretation for the function $\min(\nu^+(\cdot),\nu^+(\cdot))$, but here $(0,0)$ is not a divisor on $(\mathbb{P}^1(k))^2$. To try and make things work we then blow up the plane at this point, and it turns out that the height with respect to the exceptional divisor on this blow-up is in fact the logarithmic G.C.D. In general, the G.C.D. is to be interpreted as a height function with respect to a closed subscheme, following the definitions laid out by Silverman [69]. Again, the analogy is rich and complex and we will not illustrate it, but point to the ultimate reference for this—the landmark article by Silverman [72].

This important analogy has thence been used to prove various cases of Vojta's conjecture for blow-ups by mutuating the techniques that successfully apply for G.C.D. problems, namely the Subspace Theorem. Levin [43] proves some cases on toric varieties; Wang–Yasufuki [81] on Cohen-Macaulay varieties; Yasufuki [82] on $\mathbb{P}^n$, and links it with the *abc* conjecture; Yasufuki again [83] on rational surfaces; Grieve [30] on Fano toric varieties.

3. The case with one recurrence fully non-simple

It has been realized in recent times [3] that the case where one of the sequences is instead fully degenerate, and in particular a polynomial sequence, the distribution problem for $g_n=\gcd(P(n),u_n)$ offers a more approachable toy version of the general problem. For the time being, we shall take one of the sequences to be the identity sequence and the other one to be a simple[‡] linear recurrence, and study $g_n=\gcd(n,u_n)$; the stronger results will then follow from the fact that here we have complete control over the places that divide one of the two recurrences.

Firstly, the case of u a first-order recurrence is easily settled. For instance, large and small values are immediate to estimate [3, Sect.1], and the observation that $\gcd(n,p^n)=p^{v_p(n)}$ implies the following asymptotic for the moments.

[‡]There is no loss of generality in assuming the simplicity of u [3, Sect. 1].

THEOREM 15. *As* $x \to \infty$,

$$\sum_{n\le x} (\log \gcd(n, p^n))^k = x\left(1-\frac{1}{p}\right)(\log p)^k \sum_{m=0}^{\infty} \frac{m^k}{p^m} + O\left(\left(\frac{\log x}{\log p}\right)^{k+1}\right).$$

Moreover, if $k \ge 1$,

$$\sum_{n\le x} \gcd(n, p^n)^k = x^{k(1+o_p(1))}$$

as $x \to \infty$.[§]

The expression with $u_n = a^n$ for composite a is, however, not nearly as nice. At any rate, we shall henceforth assume that the order of the recurrence u is greater than 1.

3.1. Large values of $\gcd(n, u_n)$

We first look at large values of $\gcd(n, u_n)$. Remember that u is always a simple linear recurrence of order at least 2, and that it is fixed once and for all without further mention of it in all Vinogradov symbols.

Studies on this quantity mostly involved the naïve formulation "when does n divide u_n"—in our perspective, this is asking for which n's the $\gcd(n, u_n)$ equals n, i.e. is as large as it can possibly get. The early works were partial characterizations, usually in terms of a (more or less explicit) recursive tree structure which is however unsuited to quantitative estimates. Credit for this is to be given here to Jarden [39], Hoggatt–Bergum [36], André-Jeannin [4], Somer [78], Smyth [77], and Győry–Smyth [33].

The first major work was that of Alba González–Luca–Pomerance–Shparlinski [3], where they obtained good bounds for various cases according to how nice the recurrence is.

THEOREM 16 (Alba González–Luca–Pomerance–Shparlinski [3, Th. 1.1]). *If* u *is non-degenerate, then as* $x \to \infty$

$$\#\{n \le x : n \text{ divides } u_n\} \ll \frac{x}{\log x}.$$

An ingredient of the proof is again the Subspace Theorem 2, or rather a consequence of it due to Schlickewei, to bound the number of zeros of the recurrence modulo p, hence number of solutions modulo p of an exponential equation [67].

This is essentially best possible: if we consider for instance the recurrence $u_n = 2^n - 2$, then p always divides u_p, and the composite n's for which n divides u_n are pseudoprimes and hence [58, Th. 2] much fewer than odd primes, so that in this case $\#\{n \le x : \gcd(n, u_n) = n\} = (1+o(1))x/\log x$.

[§] In fact the sum admits an asymptotic of the form $\left(x/p^{\psi_{p,k}(\log x/\log p)}\right)^k$, where ψ is a bounded periodic function with an explicit description as well; but we are not concerned here with such higher order terms.

THEOREM 17 (Alba González–Luca–Pomerance–Shparlinski [3, Th. 1.2]). *If the recurrence u is a non-degenerate Lucas sequence then as $x \to \infty$*

$$\#\{n \le x : n \text{ divides } u_n\} \le x \exp\left(-(1+o(1))\sqrt{\log x \log\log x}\right). \tag{1}$$

THEOREM 18 (Alba González–Luca–Pomerance–Shparlinski [3, Thms. 1.3 and 1.4]). *Suppose that u is a non-degenerate Lucas sequence with characteristic polynomial $X^2 - a_1X - a_2$.*

If $a_2 = \pm 1$ then as $x \to \infty$

$$\#\{n \le x : n \text{ divides } u_n\} \ge x^{1/4+o(1)}. \tag{2}$$

If $a_2 \ne \pm 1$ but $\Delta_u \ne \pm 1$ then, as $x \to \infty$

$$\#\{n \le x : n \text{ divides } u_n\} \ge \exp\left(C(\log\log x)^2\right).$$

In fact, to show (2) they use an explicit construction of integers of the form $2s\prod_{p\le x} p$ with s as follows: every one if its prime factors q is greater than x and such that q^2-1 is x-friable (has only prime factors smaller than x). If the factorization of integers of the form q^2-1 is statistically the same as a typical integer of their size, a lower bound $x^{1+o(1)}$ in (2) holds.

The next step was that of Luca and the author [49], who showed that the upper bound (1) can be vastly improved, and gave an explicit structure theorem for such integers. Their result was for Fibonacci numbers and was generalized by Sanna [62] to any Lucas sequence, using the appropriate formulae for the p-adic valuation of Lucas sequences [61]. From now on Lucas sequences will be understood to be non-degenerate as degenerate ones pose no problem [62, Sect. 2].

THEOREM 19 (Sanna [62, Th. 1.2], Luca–Tron [49, Th. 1]). *If the recurrence u is a Lucas sequence, then*

$$\#\{n \le x : n \text{ divides } u_n\} \le x \exp\left(-\left(\frac{1}{2}+o(1)\right)\frac{\log x \log\log\log x}{\log\log x}\right).$$

The $1/2+o(1)$ factor is just an artifact of the methods [27, Th. 3]. In fact, based on this and on analogies [58, Sect. 4] with Carmichael numbers via Korselt's criterion, Luca–Tron conjecture the following.

CONJECTURE 3 (Luca–Tron [49, Sect. 1]). If the recurrence u is a Lucas sequence, then

$$\#\{n \le x : n \text{ divides } u_n\} = x \exp\left(-(1+o(1))\frac{\log x \log\log\log x}{\log\log x}\right).$$

It should be noted that numerical evidence supporting this conjecture is relatively poor [58, Sect. 5], but there is a very precise and interesting reason why [29].

The "workhorse" here is a structure theorem for such integers n which reads as follows. We let $z_u(n)$ to be the least positive integer m for which n divides a term u_m of the sequence, whenever it is defined.

LEMMA 1 (Luca–Tron [49, Th. 2], Sanna [62, Lemma 3.3]). *For any fixed k let $\mathcal{R}_k := \{n \in \mathbb{N} : n/z_u(n) = k\}$. If n is in $\mathcal{R}_k$, then it is of the form $\gamma(k)m$, where m is a positive integer all of whose prime factors divide $6\Delta_u k$, and $\gamma(k)$ an integer depending only on k.*

In other words, if the ratio $n/z_u(n)$ is prescribed, every integer n is the product of a fixed integer times an S-integer with controlled S. This can be proved using explicit formulas for the p-adic valuation of u_n [61] and then, taking any n that belongs to $\mathcal{R}_k$, inspect for which n' the integer nn' also belongs to $\mathcal{R}_k$. This is of course no use without being able to estimate $\gamma(k)$, and the little miracle here is the existence of a very neat expression for it.

LEMMA 2 (Luca–Tron [49, Th. 2], Sanna [62, Lemma 3.3], Leonetti). *For any k, $\gamma(k)$ is the least element in $\mathcal{R}_k$ and we have*

$$\gamma(k) = k \operatorname*{lcm}_{m \geq 1} z^{\circ m}(k).$$

One can indeed see that this is well defined; once we know this expression we can notice that indeed $\gamma(k) \in \mathcal{R}_k$ almost by construction. This kind of expression might be telling for someone working in dynamical systems, but a satisfying dynamical interpretation is still lacking.

The work of Luca–Tron and Sanna does in fact prove an upper bound for the counting function when one instead asks for $\gcd(n, u_n) \geq \alpha n$ with $0 \leq \alpha \leq 1$ fixed (and thus a bound on $G(x,y)$ in the range $y \gg x$). With some more work, the methods would imply the following uniform bound.

CONJECTURE 4. If $0 \leq \alpha \leq 1$ is fixed, then

$$\#\{n \leq x : \gcd(n, u_n) \geq \alpha n\} \leq x \exp\left(-\left(\frac{1}{2} + o_\alpha(1)\right) \frac{\log x \log\log\log x}{\log\log x}\right).$$

The conjecture for the correct order of magnitude is still the same, that the $1/2 + o(1)$ on the right-hand side is actually an $1 + o(1)$. The key here is that Lemma 11, as well as its proof, adapts almost word by word when instead of $n = bz(n)$, $b \in \mathbb{N}$ a fixed integer, one asks for $n = \beta z(n)$, $\beta \in \mathbb{Q}$ a fixed rational number.

We end the section by considering the more general case when one of the recurrences is fully non-simple but of possibly higher order, i.e. the G.C.D. has the form $\gcd(F(n), u_n)$ with F a non-constant polynomial with integer coefficients. In this case, using sieve methods Alba González–Luca–Pomerance–Shparlinski prove a sligthly worse upper bound.

THEOREM 20 (Alba González–Luca–Pomerance–Shparlinski [3, Sect. 7]). *If*

the recurrence u has order $d \geq 2$ and F is as above, as $x \to \infty$ it holds that

$$\#\{n \leq x : F(n) \text{ divides } u_n\} \ll_F \frac{x \log\log x}{\log x}.$$

3.2. Small values of $\gcd(n, u_n)$

After studying when n divides u_n, next is the "dual" problem of when n is coprime to u_n. We retain the notation and hypotheses of the previous section.

The first basic theorem is due to Sanna [65] and proves, under very general assumptions, that those n have an asymptotic density.

THEOREM 21 (Sanna [65, Th. 1.1]). *If u is non-degenerate, the set of integers n such that $\gcd(n, u_n) = 1$ has an asymptotic density. Such a density is positive, unless $(u_n/n)_n$ is also a linear recurrence, in which case this set is in fact finite.*

Next came the work of Sanna and the author [66], where it was shown that not only this generalizes to any fixed value of the G.C.D., but also that another little miracle occurs: there is a very explicit expression for the asymptotic density. For notational convenience set $\ell_u(m) := \operatorname{lcm}(m, z_u(m))$.

THEOREM 22 (Sanna–Tron [66, Thms. 1.3 and 1.4]). *Let u be a non-degenerate Lucas sequence with characteristic polynomial $X^2 - a_1X - a_2$. For any $k \in \mathbb{N}$, let $\mathcal{A}_k$ be the set of integers n such that $\gcd(n, u_n) = k$. Then $\mathcal{A}_k$ has an asymptotic density which is given by the absolutely convergent series*

$$\sum_{\gcd(d,a_2)=1} \frac{\mu(d)}{\ell_u(dk)}.$$

Such a density is positive if and only if $\mathcal{A}_k$ is not empty if and only if $\gcd(k, a_2) = 1$ and $k = \gcd(\ell_u(k), u_{\ell_u(k)})$.

The last part vindicates a conjecture made in another setting by Silverman [73, Q. 1]. The statement is moderately far-reaching: for instance, the integers n such that $\gcd(n, 2^n - 1) = k$ have an asymptotic density given by $\sum_{n \text{ odd}} 1/\operatorname{lcm}(kn, \operatorname{ord}_{kn}(2))$. However, a way of proving *a priori* the criterion for such a sum to be zero or not, or even just showing its non-negativity, directly without going through the related arithmetical problem, is not known to exist.

The heart of the proof is also the apparently least interesting part, to show that the expression is well defined. We record it separately to emphasize it.

LEMMA 3. *The series*

$$\sum_{\gcd(d,a_2)=1} \frac{1}{\ell_u(d)}$$

converges absolutely.

If in place of $\ell_u(d) = \operatorname{lcm}(d, z_u(d))$ we just had $d\, z_u(d)$ things would be much easier: the convergence of the sum $\sum_d 1/dz_u(d)$ has been known at least since the work of Romanoff in the '30s [53].

Once we know this, the expression for the density in Theorem 22 is straightforward to derive; let us do the case $k = 1$ and $a_2 = 1$, so that z_u is defined on all integers. If we set $\rho(n,d)$ to be the indicator function of "$d|u_n$" then

$$\#\mathcal{A}_1(x) = \sum_{n\le x}\prod_{p|n}(1-\rho(n,p)) = \sum_{n\le x}\sum_{d|n}\mu(d)\rho(n,d) = \sum_{d\le x}\mu(d)\sum_{m\le x/d}\rho(dm,d);$$

now, $\rho(dm,d) = 1$ is equivalent to m being divisible by $\ell_u(d)/d$, so the latter quantity is

$$\sum_{d\le x}\mu(d)\sum_{m\le x/d}1 = \sum_{d\le x}\mu(d)\left\lfloor\frac{x}{\ell(d)}\right\rfloor = x\left(\sum_{d\le x}\frac{\mu(d)}{\ell(d)}\right) - \sum_{d\le x}\mu(d)\left\{\frac{x}{\ell(d)}\right\}.$$

All we need to do now is to use that $\sum_{d>x}\frac{\mu(d)}{\ell(d)}$ is the tail of a convergent series, and split the latter sum into large and small d (say, at a cutoff of $x^{1/2}$) to recover Theorem 22.

REMARK 1. In light of Theorem 22, the set of numbers k for which $\mathcal{A}_k$ is empty (or not) is itself of interest. Leonetti–Sanna [42] prove that there are at least $Cx/\log x$ and at most $o(x)$ integers k up to x for which $\mathcal{A}_k$ is not empty. Given that they only consider prime numbers in the lower bound, the true order of magnitude should be somewhat larger; are there, say, at least $x\log\log x/\log x$ such integers up to x?

Parallel to the previous sections, the problem with $\gcd(F(n),u_n)$ a fixed integer, where F is a polynomial with integer coefficients, has also been studied.

THEOREM 23 (Mastrostefano–Sanna [52, Th. 1.4]). *Suppose that F splits over $\mathbb{Q}$, and let k be a fixed integer. Then the set of integers n such that $\gcd(F(n),u_n) = k$ has an asymptotic density. If moreover u is non-degenerate and F does not have fixed divisors, then the set set of integers n such that $\gcd(F(n),u_n) = 1$ has zero asymptotic density if and only if it is finite.*

However, no nice expression for the density is presently known in cases other than $F(n) = n$.

3.3. Averages of $\gcd(n,u_n)$

The previous sections give quite satisfying answers to the problem of determining extreme values of $\gcd(n,u_n)$. If we inquire, however, about its average size, much less is known–let alone the distribution function $G(x,y)$ in general. We summarize here partial progress towards the solution.

If we allow for some more regular version of the G.C.D., say its logarithm $\log\gcd(n,u_n)$, the situation is already quite different.

THEOREM 24 (Sanna [64, Th. 1.1]). *Let u be a non-degenerate Lucas sequence. Then for any fixed positive integer k, as $x\to\infty$,*

$$\sum_{n\le x}(\log\gcd(n,u_n))^k = M_k x + O_k(x^{1-1/(3k+3)}).$$

Moreover, the constant M_k is given explicitly by an absolutely convergent series

$$M_k = \sum_{\gcd(d,a_2)=1}\frac{\rho_k(d)}{\ell_u(d)}$$

and ρ_k is a certain, explicitly defined, arithmetical function such that $\rho_k(m)\le(k\log m)^k$.

This implies directly a bound for the counting function.

COROLLARY 1 (Sanna [64, Cor. 1.3]).

$$G(x,y)\ll_{u,k}\frac{x}{(\log y)^k}.$$

The argument itself is not too different to what we have seen already in the previous section. Suppose for instance that $k=1$: we can write

$$\sum_{n\le x}\log\gcd(n,u_n)=\sum_{n\le x}\sum_{\ell_u(p^e)\mid n}\log p=\sum_{p^e}\log p\sum_{\substack{n\le x\\ \ell_u(p^e)\mid n}}1=\sum_{p^e}\log p\left\lfloor\frac{x}{\ell_u(p^e)}\right\rfloor$$

$$=:\sum_{\gcd(m,a_2)=1}\rho_1(m)\left\lfloor\frac{x}{\ell_u(m)}\right\rfloor=\left(\sum_{\gcd(m,a_2)=1}\frac{\rho_1(m)}{\ell_u(m)}\right)x-\sum_{\gcd(m,a_2)=1}\rho_1(m)\left\{\frac{x}{\ell_u(m)}\right\},$$

then argue as in Section 3.2; for larger k there is more combinatorial work involved, but again convergence of the relevant sum is the bulk of the proof.

Inspired by this work, Mastrostefano set out to find more on the moments themselves. Here is the upper bound that he obtained.

THEOREM 25 (Mastrostefano [51, Th. 1.3]). *Let u be a non-degenerate Lucas sequence. Then for any fixed positive integer k, as $x\to\infty$,*

$$\sum_{n\le x}\gcd(n,u_n)^k\le x^{k+1-(1+o_k(1))\sqrt{\log\log x/\log x}}.$$

The key to improving these estimates is the study of the tail of a series

$$\sum_{\substack{d>x\\ \gcd(d,a_2)=1}}\frac{1}{\ell_u(d)}:$$

Mastrostefano bounds it by $\exp\left(-(1/\sqrt{6}-\varepsilon+o_\varepsilon(1))\sqrt{\log x\log\log x}\right)$. We also get the following for the counting function.

COROLLARY 2 (Mastrostefano [51, Cor. 1.5]). *As $x\to\infty$,*

$$G(x,y)\le x^{2-(1+o(1))\sqrt{\log\log x/\log x}}/y.$$

The determination of the moments can be a subtle problem [51, Sect. 6]. However, it is not difficult to conjure up a simple heuristic: if we come back to numbers n such that $\gcd(n,u_n)=n$, there are conjecturally $x^{1-(1+o(1))\log\log\log x/\log\log x}$ of them up to x. If they were evenly spaced (which they are not, but they are at least well distributed) they would contribute at least

$$\sum_{n\le x/x^{(1+o(1))\log\log\log x/\log\log x}}\left(nx^{(1+o(1))\log\log\log x/\log\log x}\right)^k = x^{k+1-(1+o(1))\log\log\log x/\log\log x}$$

to the k-th moment. If we compound this with the *ansatz* that "most" of the mass of the moments comes from those n with large $\gcd(n,u_n)$—e.g. larger than βn, cf. Conjecture 4—we end up with the following conjecture.

CONJECTURE 5. If the recurrence u is a non-degenerate Lucas sequence, then as $x\to\infty$

$$\sum_{n\le x}\gcd(n,u_n)^k = x^{k+1-(1+o_k(1))\log\log\log x/\log\log x}.$$

As Mastrostefano kindly pointed out to me, this very argument, coupled with the input from Alba González–Luca–Pomerance–Shparlinski (cf. Theorem 18), immediately provides the following.

THEOREM 26. *If $a_2=\pm1$ then as $x\to\infty$*

$$\sum_{n\le x}\gcd(n,u_n)^k \ge x^{k+1/4+o_k(1)}.$$

It is maybe worth to point out the formal resemblance of Theorems 24 and 15 with work of Luca–Shparlinski [48, Th. 2]. They study sums of the form $\sum_{n\le x}f(u_n)^k$, where f is any arithmetic function satisfying certain stringent growth conditions, and they prove an estimate $M_{f,k}\,x+O_{f,k}(x(\log\log x)^k/\log x)$.

4. The problem in other settings

4.1. Elliptic divisibility sequences

The most straightforward adaptation of statements from Part 3 is in the setting of elliptic divisibility sequences—which by the way is an indicator that some properties have more to do with u_n being a divisibility sequence rather than a linear recurrence. We

recall that an elliptic divisibility sequence, call it u_n still, is defined by taking a non-torsion point $P \in E(\mathbb{Q})$ of an elliptic curve $E/\mathbb{Q}$ defined by a Weierstrass equation and then the reduced x-coordinates of its orbit $x_{[n]P} = v_n/u_n^2$.

The recursive structure theorems mentioned at the start of Section 3.1 have an elliptic version by Silverman–Stange [76]; the theorems for the distribution of $\gcd(n,u_n) = n$ are due to Gottschlich [28].

THEOREM 27 (Gottschlich [28, Th. 1.1]). *As $x \to \infty$, we have*

$$\#\{n \le x : n \text{ divides } u_n\} \ll_{E,P} x \, \frac{(\log\log x)^{5/3}(\log\log\log x)^{1/3}}{(\log x)^{4/3}}.$$

When E has complex multiplication, and for any E under the Lang–Trotter conjecture, he also obtains an upper bound

$$x \, \exp\left(-(1+o_{E,P}(1)) \cdot \sqrt{\log x \log\log x/8}\right).$$

On the other hand, the analogy is even closer for the problem of $\gcd(n,u_n) = k$ constant. In this case, Kim [40] proved that a theorem *formally analogous* to Theorem 2.2 holds. Again, the delicate point is the convergence of the sum [40, App. A], while the proof itself is otherwise formally the same.

As an aside, we comment that the setting of elliptic curves gives a more transparent geometric interpretation which otherwise, in the case of linear recurrences, is to be found in the work of Cubre–Rouse [19] (after Lagarias [41]), solving a conjecture of Bruckman–Anderson [7] by means of the "torus trick" of Hasse–Ballot [5]. For a slightly different take on this, also see Silverman [72].

Finally, the Ailon–Rudnick theorem 1.2 as well is proved by Silverman for elliptic divisibility sequences over function fields (i.e. obtained from a curve $E/k(T)$) in case the j-invariant of the curve is k-rational [71, Th. 3]. Ghioca–Hsia–Tucker give a variant over any field of positive characteristic [25], Ostafe [56] for multivariate polynomials, Ghioca–Hsia–Tucker again [26] over elliptic curves, Ulmer–Urzúa [79] a result of similar flavor on unlikely intersections. Silverman [72] has a theorem analogous to Theorem 1.4 where a bound in the same form as Theorem 9 but for elliptic divisibility sequences is shown to be another consequence of Vojta's conjecture.

4.2. Nevanlinna theory

An extremely fruitful development in analogy with the greatest common divisors of recurrences is in Nevanlinna theory, where the quantities are replaced by their cousins in the setting of entire functions in the spirit of Vojta's celebrated dictionary between Nevanlinna theory and diophantine approximation [80]. Without developing the basics of Nevanlinna theory, we shall limit ourselves to mentioning the most relevant results.

The basic ideas involved in the correct analogy where introduced in the landmark work of Noguchi–Winkelmann–Yamanoi [55]. The article of Pastén–Wang [57]

is the most complete source of meromorphic counterparts to the arithmetic G.C.D. bounds, and we now introduce some of them.

For f a meromorphic function on $\mathbb{C}$ and $z \in \mathbb{C}$, we set $\nu_z^+(f) := \max(0, \mathrm{ord}_z(f))$ and $\nu_z^-(f) := -\min(0, \mathrm{ord}_z(f))$. We then define the characteristic function

$$T(f,r) := \frac{1}{2\pi}\int_0^{2\pi} \max(0, \log|f(re^{i\theta})|)d\theta + \sum_{0<|z|\le r} \nu_z^-(f)\log|r/z| + \nu_0^-(f)\log r.$$

The analogue for the G.C.D. is defined as follows: if

$$n(f,g,r) := \sum_{|z|\le r} \min(\nu_z^+(f), \nu_z^+(g)),$$

then the relevant counting function is

$$N(f,g,r) := \int_0^r \frac{n(f,g,t) - n(f,g,0)}{t}dt + n(f,g,0)\log r.$$

A sample of the many G.C.D. bounds that Pastén–Wang obtain in this setting are the following.

THEOREM 28 (Pastén–Wang [57, Th. 1.3]). *Let f, g be algebraically independent meromorphic functions and $\varepsilon > 0$. Then*

$$N(f^n - 1, g^n - 1, r) < \varepsilon \max(nT(f,r), nT(g,r))$$

for all r in a set of infinite Lebesgue measure.

THEOREM 29 (Pastén–Wang [57, Th. 1.5]). *Let f, g be multiplicatively independent entire functions without zeros, both of finite order, and $\varepsilon > 0$. Then for all large n, as $r \to \infty$ we have*

$$N(f^n - 1, g^n - 1, r) < \varepsilon \min(T(f^n, r), T(g^n, r)) + O(\log r).$$

They give many more theorems under various different hypotheses on the growth of the functions, and even general results for meromorphic functions over any complete algebraically closed field, so the reader is advised to read their introduction. For more on the general technical background, see Noguchi–Winkelmann [54].

This line of work spawned the following developments.

THEOREM 30 (Guo–Wang [32, Th. 1.1]). *Let f, g be algebraically independent meromorphic functions and $\varepsilon > 0$. Then for all large n, and for all r outside a set of finite Lebesgue measure,*

$$N(f^n - 1, g^n - 1, r) < (1/2 + \varepsilon)\max(T(f^n, r), T(g^n, r)).$$

THEOREM 31 (Levin–Wang [44, Cor. 1.6]). *Let f, g be multiplicatively independent meromorphic functions, and $\varepsilon > 0$. Then for all large n, as $r \to \infty$ (outside a set of finite Lebesgue measure), we have*

$$N(f^n - 1, g^n - 1, r) < \varepsilon \max(T(f^n, r), T(g^n, r)).$$

The Corvaja–Zannier version of the Hadamard Quotient Theorem has an analog for entire functions as well, due to Guo [34].

THEOREM 32 (Guo [34, Th. 1.2]). *Let $f_1,\dots,f_k,g_1,\dots,g_m$ be nonconstant entire functions such that $\max_i T(f_i,r) \asymp \max_j T(g_j,r)$ as $r\to\infty$. Set $F(n) := a_0 + a_1 f_1^n + \cdots + a_k f_k^n$, $G(n) := b_0 + b_1 g_1^n + \cdots + b_k g_k^n$ where the a_i and b_j are nonzero complex numbers. If $F(n)/G(n)$ is an entire function for infinitely many n, then the f_i, g_j are multiplicatively dependent (there is a product $f_1^{r_1}\cdots f_k^{r_k} g_1^{s_1}\cdots g_k^{s_k}$ which is a nonzero constant).*

For more work on G.C.D. bounds in Nevanlinna theory in the setting of holomorphic maps to semi-abelian varieties also see Liu–Yu [45]. Corvaja–Noguchi [11] prove another counterpart to the Corvaja–Zannier theorem [13].

4.3. Rational dynamical systems

Another domain of research which is rich in analogies with the problems that we have studied is that of rational dynamical systems [74], i.e. the study of the behavior of iterates of rational maps (which is itself linked to the domain of unlikely intersections [84, Ch. 3.4.7]). The links usually exploit Silverman's ideas in some way or another, and the powers of integers are replaced by n-fold iterates of polynomials.

Chen–Gassert–Stange [9] prove analogues of the structure theorems mentioned at the beginning of Section 3.1 and Gassert–Urbanski [24] study the divisibility by n of $F^{\circ n}(0)$, F a polynomial.

More interestingly, Hsia–Tucker [37] prove a "compositional" cousin to the Ailon–Rudnick theorem.

THEOREM 33 (Hsia–Tucker [37, Th. 4]). *Let $F,G\in\mathbb{C}[X]$ be compositionally independent polynomials, of degree greater than 1, and $C\in\mathbb{C}[X]$ another polynomial satisfying some extra conditions. Then there is a polynomial $H\in\mathbb{C}[X]$ such that, for all m,n,*

$$\gcd(F^{\circ m}-C, G^{\circ n}-C) \text{ divides } H.$$

A compositional analogue of the Bugeaud–Corvaja–Zannier bound is known as well; here, however, the substantial recourse to Silverman's method requires Vojta's conjecture in a form not yet proved in such generality. Assuming thus Vojta's conjecture, the theorem reads as follows.

THEOREM 34 (Huang [38, Th. A]). *Let $F,G\in\mathbb{Z}[X]$ be polynomials of the same degree $d=\deg F=\deg G\geq 2$, and $a,b,\alpha,\beta\in\mathbb{Z}$ integers. Under some genericity assumption, there is a constant $C>0$ such that for all n*

$$\gcd(F^{\circ n}(a)-\alpha, G^{\circ n}(b)-\beta) \leq C\exp(\varepsilon d^n).$$

In fact he proves more general versions for rational maps and also gives more in-depth characterizations in case the genericity assumption is not satisfied.

Acknowledgements

I am thankful to Yuri Bilu, Francesco Campagna, Pietro Corvaja, Luca Ghidelli, Paolo Leonetti, Daniele Mastrostefano, Carlo Sanna, Joe Silverman, Umberto Zannier, and the anonymous referee, for useful discussion and comments before and during the preparation of this work. I also thank the organizers of the *2nd Number Theory Meeting*, where my lecture constituted the early core of this survey.

References

[1] ADLEMAN L.M., POMERANCE C., AND RUMELY S., *On Distinguishing Prime Numbers from Composite Numbers*, Annals of Math. **117** 1 (1983), 173–206.

[2] AILON N. AND RUDNICK Z., *Torsion points on curves and common divisors of a^k-1 and b^k-1*, Acta Arith. **113** (2004), 31–38.

[3] ALBA GONZÁLEZ J.J., LUCA F., POMERANCE C., AND SHPARLINSKI I.E., *On numbers n dividing the nth term of a linear recurrence*, Proc. Edinb. Math. Soc. **55** 2 (2012), 271–289.

[4] ANDRÉ-JEANNIN R., *Divisibility of generalized Fibonacci and Lucas numbers by their subscripts*, Fibonacci Q. **29** 4 (1991), 364–366.

[5] BALLOT C., *Density of Prime Divisors of Linear Recurrences*, Mem. Am. Math. Soc. **551**, AMS, Providence 2005.

[6] BILU YU., *The Many Faces of the Subspace Theorem (after Adamczewski, Bugeaud, Corvaja, Zannier...)*, Séminaire Bourbaki n° 967, Astérisque **317** (2008), 1–38.

[7] BRUCKMAN P.S. AND ANDERSON P.G., *Conjectures on the Z-densities of the Fibonacci sequence*, Fibonacci Q. **36** 3 (1998), 263–271.

[8] BUGEAUD Y., CORVAJA P., AND ZANNIER U., *An upper bound for the G.C.D. of a^n-1 and b^n-1*, Math. Z. **243** (2003), 79–84.

[9] CHEN A.S., GASSERT T.A., AND STANGE K.E., *Index divisibility in dynamical sequences and cyclic orbits modulo p*, New York J. Math. **23** (2017), 1045–1063.

[10] COHEN J. AND SONN J., *A cyclotomic generalization of the sequence* $\gcd(a^n-1,b^n-1)$, J. Théor. Nombres Bordx. **27** 1 (2015), 53–65.

[11] CORVAJA P. AND NOGUCHI J., *A new unicity theorem and Erdős problem for polarized semi-abelian varieties*, Math. Ann. **353** 2 (2012), 439–464.

[12] CORVAJA P., RUDNICK Z., AND ZANNIER U., *A Lower Bound for Periods of Matrices*, Commun. Math. Phys. **252** (2004), 535–541.

[13] CORVAJA P. AND ZANNIER U., *Finiteness of integral values for the ratio of two linear recurrences*, Invent. Math. **149** 2 (2002), 431–451.

[14] CORVAJA P. AND ZANNIER U., *On the greatest prime factor of* $(ab+1)(ac+1)$, Proc. Am. Math. Soc. **131** 6 (2003), 1705–1709 .

[15] CORVAJA P. AND ZANNIER U., *A Lower Bound for the Height of a Rational Function at S-unit Points*, Monatsh. Math. **144** 3 (2005), 203–224.

[16] CORVAJA P. AND ZANNIER U., *Some cases of Vojtas Conjecture on integral points over function fields*, J. Algebr. Geom. **17** (2008), 295–333. Addendum: Asian J. Math. **14** (2010), 581–584.

[17] CORVAJA P. AND ZANNIER U., *Greatest common divisors of $u-1$, $v-1$ in positive characteristic and rational points on curves over finite fields*, JEMS **15** 5 (2013), 1927–1942.

[18] CORVAJA P. AND ZANNIER U., *Applications of Diophantine Approximation to Integral Points and Transcendence*, Camb. Tracts Math. **212**, Cambridge University Press, Cambridge 2018.

[19] CUBRE P. AND ROUSE J., *Divisibility properties of the Fibonacci entry point*, Proc. Am. Math. Soc. **142** 3 (2014), 3771–3785.

[20] DENIS L., *Facteurs communs et torsion en caractéristique non nulle* , J. Théor. Nombres Bordx. **23** 2 (2011), 347–352.

[21] EVEREST G., VAN DER POORTEN A., SHPARLINSKI I., AND WARD T., *Recurrence Sequences*, Math. Surv. Monogr. **104**, AMS, Providence 2003.

[22] FUCHS C., *An upper bound for the G.C.D. of two linear recurring sequences*, Math. Slovaca **53** 1 (2003), 21–42.

[23] FUCHS C., *Diophantine problems with linear recurrences via the Subspace Theorem*, Integers **5** 3 (2005), A08.

[24] GASSERT T.A. AND URBANSKI M.T., *Index divisibility in the orbit of 0 for integral polynomials*, `arXiv:1709.08751 [math.NT]` (2017).

[25] GHIOCA D., HSIA L.-C., AND TUCKER T.J., *On a variant of the AilonRudnick theorem in finite characteristic*, New York J. Math. **23** (2017), 213–225.

[26] GHIOCA D., HSIA L.-C., AND TUCKER T.J., *A variant of a theorem by AilonRudnick for elliptic curves*, Pac. J. Math. **295** 1 (2018), 1–15.

[27] GORDON D.M. AND POMERANCE C., *The distribution of Lucas and elliptic pseudoprimes*, Math. Comput. **57** (1991), 825–838.

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

[29] GRANVILLE A. AND POMERANCE C., *Two contradictory conjectures concerning Carmichael numbers*, Math. Comput. **71** (2001), 883–908.

[30] GRIEVE N., *Generalized GCD for toric Fano varieties*, `arXiv:1904.13188 [math.AG]` (2019).

[31] GRIEVE N. AND WANG J.T.-Y., *Greatest common divisors with moving targets and linear recurrence sequences*, `arXiv:1902.09109 [math.NT]` (2019).

[32] GUO J. AND WANG J.T.-Y., *Asymptotic gcd and divisible sequences for entire functions*, Trans. Am. Math. Soc. **37** 9 (2019), 6241–6256.

[33] GYŐRY K. AND SMYTH C., *The divisibility of $a^n - b^n$ by powers of n*, Integers **10** (2010), A27/319–334.

[34] GUO J., *The Quotient Problem for Entire Functions*, Can. Math. Bull. **62** 3 (2019), 479–489.

[35] HERNÁNDEZ S. AND LUCA F., *On the largest prime factor of $(ab+1)(ac+1)(bc+1)$*, Bol. Soc. Mat. Mex., III. Ser. **9** 2 (2003), 235–244 .

[36] HOGGATT V.E. JR. AND BERGUM G.E., *Divisibility and Congruence Relations*, Fibonacci Q. **12** 2 (1974), 189–195.

[37] HSIA L.C. AND TUCKER T.J., *Greatest common divisors of iterates of polynomials*, Algebra Number Theory **11** 6 (2017), 1437–1459.

[38] HUANG K., *Generalized Greatest Common Divisors for the Orbits under Rational Functions*, `arXiv:1702.03881 [math.NT]` (2017).

[39] JARDEN D., *Divisibility of terms by subscripts in Fibonaccis sequence and associate sequence*, Riveon Lematematika **13** (1959), 51–56.

[40] KIM S., *The density of the terms in an elliptic divisibility sequence having a fixed G.C.D. with their indices*, J. Number Theory, to appear. Appendix by M. R. Murty.

[41] LAGARIAS J.C., *The set of primes dividing the Lucas numbers has density 2/3*, Pac. J. Math. **118** 2 (1985), 449–461. Errata: Pac. J. Math. **162** 2 (1994), 393–396.

[42] LEONETTI P. AND SANNA C., *On the greatest common divisor of n and the nth Fibonacci number*, Rocky Mt. J. Math. **48** 4 (2018), 1191–1199.

[43] LEVIN A., *Greatest common divisors and Vojta's conjecture for blowups of algebraic tori*, Invent. Math. **215** 2 (2019), 493–533.

[44] LEVIN A. AND WANG J.T.-Y., *Greatest common divisors of analytic functions and Nevanlinna theory on algebraic tori*, J. Reine Angew. Math., to appear.

[45] LIU X. AND YU G., *Upper Bounds of GCD Counting Function for Holomorphic Maps*, J. Geom. Anal. **29** 2 (2019), 1032–1042.

[46] LUCA F., *On the Greatest Common Divisor of $u-1$ and $v-1$ with u and v Near S-units*, Monatsh. Math. **146** 3 (2005), 239–256.

[47] LUCA F. AND SHPARLINSKI I.E., *On the exponent of the group of points on elliptic curves in extension fields*, Int. Math. Res. Not. **23** (2005), 1391–1409.

[48] LUCA F. AND SHPARLINSKI I.E., *Arithmetic functions with linear recurrence sequences*, J. Number Theory **125** (2007), 459–472.

[49] LUCA F. AND TRON E., *The Distribution of Self-Fibonacci Divisors*, in *Advances in the Theory of Numbers*, Fields Inst. Commun. **77**, 149–158, Springer, New York 2015.

[50] MAGAGNA C., *A lower bound for the r-order of a matrix modulo N*, Monatsh. Math. **153** 1 (2008), 59–81.

[51] MASTROSTEFANO D., *An upper bound for the moments of a GCD related to Lucas sequences*, Rocky Mt. J. Math. **49** 3 (2019), 887–902.

[52] MASTROSTEFANO D. AND SANNA C., *On numbers n with polynomial image coprime with the nth term of a linear recurrence*, Bull. Aust. Math. Soc. **99** 1 (2019), 23–33.

[53] MURTY M.R., ROSEN M., AND SILVERMAN J.H., *Variations on a theme of Romanoff*, Int. J. Math. **7** 3 (1996), 373–391.

[54] NOGUCHI J. AND WINKELMANN J., *Nevanlinna Theory in Several Complex Variables and Diophantine Approximation*, Grundlehren Math. Wiss. **350**, Springer, Berlin 2014.

[55] NOGUCHI J., WINKELMANN J., AND YAMANOI K., *The second main theorem for holomorphic curves into semi-Abelian varieties*, Acta Math. **188** 1 (2002), 129–161.

[56] OSTAFE A., *On some extensions of the AilonRudnick theorem*, Monatsh. Math. **181** 2 (2016), 451–471.

[57] PASTEN H. AND WANG J.T.-Y., *GCD Bounds for Analytic Functions*, Int. Math. Res. Not. **2017** 1 (2017), 47–95.

[58] POMERANCE C., *On the Distribution of Pseudoprimes*, Math. Comput. **37** 156 (1981), 587–593.

[59] VAN DER POORTEN A.J., *Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles*, C. R. Acad. Sci. Paris Sér. I **306** (1988), 97–102.

[60] POURCHET Y., *Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles*, C. R. Acad. Sci. Paris Sér. I **288** (1979), A 1055–1057.

[61] SANNA C., *The p-adic valuation of Lucas sequences*, Fibonacci Q. **54** 2 (2016), 118–124.

[62] SANNA C., *On numbers n dividing the nth term of a Lucas sequence*, Int. J. Number Theory **13** 3 (2017), 725–734.

[63] SANNA C., *Distribution of integral values for the ratio of two linear recurrences*, J. Number Theory **180** (2017), 195–207.

[64] SANNA C., *The moments of the logarithm of a G.C.D. related to Lucas sequences*, J. Number Theory **191** (2018), 305–315.

[65] SANNA C., *On Numbers n Relatively Prime to the nth Term of a Linear Recurrence*, Bull. Malays. Math. Sci. Soc. **42** 2 (2019), 827–833.

[66] SANNA C. AND TRON E., *The density of numbers n having a prescribed G.C.D. with the nth Fibonacci number*, Indag. Math. **29** (2018), 972–980.

[67] SCHLICKEWEI H.P. AND SCHMIDT W.M., *The Number of Solutions of Polynomial-Exponential Equations*, Compos. Math. **120** 2 (2000), 193–225.

[68] SCHMIDT W.M., *Diophantine Approximation*, Lect. Notes Math. **785**, Springer, Berlin 1980.

[69] SILVERMAN J.H., *Arithmetic distance functions and height functions in Diophantine geometry*, Math. Ann. **279** (1987), 193–216.

[70] SILVERMAN J.H., *Common divisors of $a^n - 1$ and $b^n - 1$ over function fields*, New York J. Math. **10** (2004), 37–43.

[71] SILVERMAN J.H., *Common divisors of elliptic divisibility sequences over function fields*, Manuscr. Math. **114** 4 (2004), 431–446.

[72] SILVERMAN J.H., *Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups*, Monatsh. Math. **145** 4 (2005), 333–350.

[73] SILVERMAN J.H., *Divisibility sequences and powers of algebraic integers*, Doc. Math. extra vol. (2007), 711–727.

[74] SILVERMAN J.H., *The Arithmetic of Dynamical Systems*, Grad. Texts Math. **241**, Springer–Verlag, New York 2007.

[75] SILVERMAN J.H., *The Greatest Common Divisor of $a^n - 1$ and $b^n - 1$ and the Ailon–Rudnick Conjecture*, Contemp. Math. **517**, 339–347, AMS, Providence 2010.

[76] SILVERMAN J.H. AND STANGE K.E., *Terms in elliptic divisibility sequences divisible by their indices*, Acta Arith. **146** 4 (2011), 355–378.

[77] SMYTH C., *The terms in Lucas sequences divisible by their indices*, J. Integer Seq. **13** (2010), 10.2.4.

[78] SOMER L., *Divisibility of terms in Lucas sequences by their subscripts*, Applications of Fibonacci Numbers **5**, 515–525, Kluwer Academic Publishers, Dordrecht 1992.

[79] ULMER D. AND URZÚA G., *Transversality of sections on elliptic surfaces with applications to elliptic divisibility sequences and geography of surfaces*, `arXiv:1908.02208 [math.AG]` (2019).

[80] VOJTA P., *Diophantine approximation and Nevanlinna theory*, in *Arithmetic Geometry*, Lect. Notes Math. **2009**, Springer, Berlin 2011.

[81] WANG J.T.-Y. AND YASUFUKI Y., *Greatest common divisors of integral points of numerically equivalent divisors*, `arXiv:1907.09324 [math.NT]` (2019).

[82] YASUFUKI Y., *Vojtas conjecture on blowups of $\mathbb{P}^n$, greatest common divisors, and the abc conjecture*, Monatsh. Math. **163** 2 (2011), 237–247.

[83] YASUFUKI Y., *Integral points and Vojta's conjecture on rational surfaces*, Trans. Am. Math. Soc. **364** (2012), 767–784.

[84] ZANNIER U., *Some Problems of Unlikely Intersections in Arithmetic and Geometry*, Ann. Math. Stud. **181**, Princeton University Press, Princeton 2012.

AMS Subject Classification: 11B37, 11J87

Emanuele TRON
Institut de Mathématiques de Bordeaux
351 cours de la Libération, 33405 Talence, FRANCE
e-mail: `emanuele.tron@math.u-bordeaux.fr`

Lavoro pervenuto in redazione il 02.10.2019.