Journal de Théorie des Nombres
de Bordeaux **17** (2005), 423–435

Diophantine equations with linear recurrences An overview of some recent progress

par UMBERTO ZANNIER

RÉSUMÉ. Nous discutons quelques problèmes habituels concernant l'arithmétique des suites récurrentes linéaires. Après avoir brièvement rappelé les questions et résultats anciens concernant les zéros, nous nous focalisons sur les progrès récents pour le "problème quotient" (resp. "problème de la racine d-ième"), qui, pour faire court, demande si l'intégralité des valeurs du quotient (resp. racine d-ième) de deux (resp. d'une) suites récurrentes linéaires entraine que ce quotient (resp. racine d-ième) est lui-même une suite récurrente linéaire. Nous relions également ces questions à certaines équations diophantiennes naturelles, qui par ailleurs proviennent du cas non résolu le plus simple de la conjecture de Vojta sur les points entiers des variétés algébriques.

ABSTRACT. We shall discuss some known problems concerning the arithmetic of linear recurrent sequences. After recalling briefly some longstanding questions and solutions concerning zeros, we shall focus on recent progress on the so-called "quotient problem" (resp. "d-th root problem"), which in short asks whether the integrality of the values of the quotient (resp. d-th root) of two (resp. one) linear recurrences implies that this quotient (resp. d-th root) is itself a recurrence. We shall also relate such questions with certain natural diophantine equations, which in turn come from the simplest unknown cases of Vojta's conjecture for integral points on algebraic varieties.

The *linear recurrences* have an ancient tradition in Number Theory and diophantine questions about them go back to long ago. In modern times they have been widely studied, for their own sake but also as auxiliary tools toward other diophantine problems. We shall not even attempt here to give a complete overview of these developments, but rather we shall concentrate on a few typical aspects where some recent progress has been made. We start by recalling some standard definitions and properties.

A sequence $\{f(n)\}_{n\in\mathbf{N}}$ of complex numbers is called a *linear recurrence* (or sometimes just *recurrence*) if there exist $a_0,\dots,a_{r-1}\in\mathbf{C}$, $(r\geq 1)$,

$a_0 \neq 0$, such that

$$f(n+r) = a_0 f(n) + a_1 f(n+1) \ldots + a_{r-1} f(n+r-1), \quad \text{for all } n \in \mathbf{N}.$$

The minimum integer r with this property is called the *order* of the recurrence.

Consider the *generating function* $F(X) = \sum_{n=0}^{\infty} f(n) X^n$; one verifies at once that for $n \geq 0$ the coefficient of X^{n+r} in the product $(1 - a_{r-1}X - \ldots - a_0 X^r)F(X)$ is $f(n+r) - a_{r-1} f(n+r-1) - \ldots - a_0 f(n)$, which vanishes; hence the product is a polynomial (of degree $\leq r-1$) and $F(X)$ is a rational function (vanishing at ∞). Conversely, the Laurent coefficients of the expansion (at 0) of a rational function coincide with a recurrence from a certain point onwards. The partial fraction decomposition for $F(X)$ immediately shows that there exists an expression, essentially unique,

$$f(n) = \sum_{i=1}^{s} c_i(n) \rho_i^n, \quad \forall n \in \mathbf{N}, \tag{1}$$

where the $c_i \in \mathbf{C}[X]$ are nonzero polynomials and where the $\rho_i \in \mathbf{C}^*$ are distinct. Reciprocally, the right-hand side of (1) defines a recurrence sequence. The ρ_i's are called the *roots* of the recurrence; they are roots of $X^r - a_{r-1}X^{r-1} - \ldots - a_0$. The recurrence is said to be *simple* if all the $c_i(n)$ are constant (and the right-hand side of (1) is then said *power sum*) and *nondegenerate* when no ratio of distinct roots is a root of unity. (We agree that the zero recurrence is degenerate.)

When k is a field such that in (1) $c_i(X) \in k[X]$ and $\rho_i \in k$ for $i = 1, \ldots, s$, we shall say that f *is defined over* k. Normally we shall consider only recurrences defined over the field $\overline{\mathbf{Q}}$ of algebraic numbers, but many results remain true for arbitrary complex recurrences; the corresponding proofs may be often reduced to the algebraic case by specialization (see e.g. the papers [R]).

For a power sum f defined over a number field k, (1) shows that all the values $f(n)$ are sums of a bounded number of S-units, for a suitable finite set $S \subset M_k$ (as usual we shall denote by $\mathcal{O}_{k,S}$, $\mathcal{O}_{k,S}^*$ the S-integers and S-units in k, respectively): it suffices that the c_i and ρ_j all lie in $\mathcal{O}_{k,S}^*$; this remark already shows that S-unit theory may be relevant here. In fact, a fundamental tool in this context, as well as for S-unit equations, has been the Subspace Theorem of Wolfgang M. Schmidt, especially its versions with several places by H.P. Schlickewei. These results may be roughly described as multi-dimensional versions of Roth's and Ridout's results for the diophantine approximation to algebraic numbers. We shall not give here any complete statement of the Subspace Theorem, referring e.g. to [S2] and [Z]; however in the sequel we shall see in some detail an application of it.

Actually, (1) shows that diophantine equations with recurrences fall in the realm of polynomial-exponential equations. Here we have a remarkable finiteness general theorem by M. Laurent, obtained around 1986, relying again on the Subspace Theorem. Its statement requires however certain definitions, and so we do not recall it here, referring instead to [S2, Thm. 7.1]. We stress that an important special case, also relevant for recurrences, had been obtained previously, independently by Evertse and van der Poorten-Schlickewei: *For a given finitely generated subgroup* $G \subset \mathbf{C}^*$, *the equation* $x_1 + \ldots + x_n = 1$ *with* $x_i \in G$ *has only finitely many solutions such that no subsum of the* x_i *vanishes.* (See [S2, Lemma 8.3].) On expressing the x_i as products of powers of a set of generators for G, we see that the linear equation is transformed in a purely exponential one, making the connection with (1) apparent.

These results apply for instance to the old problem of describing the *zeros*, i.e. the $n \in \mathbf{N}$ such that $f(n) = 0$. Simple examples like $f(n) = 1+(-1)^n$ show that their set may be infinite if f is degenerate, even if $f \neq 0$. Without special assumptions, the nondegenerate case is far from obvious in general; one can easily reduce to this case by partitioning $\mathbf{N}$ in a finite number of suitable arithmetic progressions and studying the restriction to each progression separately.

From the qualitative point of view, this problem was completely solved by Skolem, Mahler and Lech, independently, who proved that (see [vdP]): *The set of zeros of a recurrence* f *is the union of a finite set with a finite union of arithmetic progressions. If* f *is nondegenerate, it is a finite set.* (A nice application of this to cubic Thue's equations was given by Skolem; see e.g. [Z].)

Their proof consisted in suitably viewing a linear recurrence as the restriction to $\mathbf{N}$ of a p-adic analytic function. A different proof follows from the mentioned result by Evertse *et al.*, in the case of simple recurrences, and from Laurent's Theorem in the general case (see [S2, Cor. 7.2]). This approach also yieds certain sharpenings and quantitative bounds which escape from the p-adic method. Actually, the recent quantitative versions of the Subspace Theorem, obtained by Evertse, Schlickewei, Schmidt, have enabled Schmidt to solve a longstanding conjecture on the zeros, which represented the main problem in the context. Namely, *for a nondegenerate recurrence, the number of zeros is bounded only in terms of the order* (see [S], where an explicit bound is given).

We cannot pause here on the many other papers in the area, some of them containing quite striking bounds for special cases of Schmidt's Theorem; instead, we refer e.g. to [S2].

Another application of Laurent's Theorem concerns the problem of "equal values" of recurrences, i.e. describing the solutions $(r, s) \in \mathbf{N}^2$

to $f(r) = g(s)$, for given recurrences f, g. The theorem leads to an *almost* complete classification of the cases with an infinity of solutions, as shown by Schmidt and Schlickewei (see [S2, Thm. 11.2] and [S2, p. 11/6]). By *almost* we mean that f, g are supposed not to be of the form $P(n)\alpha^n$ for a polynomial P and a root of unity α. This may seem a mild restriction, but it excludes fairly natural problems, like the one of *perfect powers in a recurrence sequence.* And the so-called *quotient problem* of the integral values for $f(n)/g(n)$ falls out as well. From now on we shall concentrate precisely on these questions, which have been the object of several researches. They are certainly special ones, but they are rather typical, and also embody some of the fundamental difficulties which appear in more general instances.

The quotient problem. Given recurrences f, g, the so-called *Hadamard quotient* $f(n)/g(n)$ is not a recurrence in general. A necessary condition for being a recurrence is of course that *all* the values $f(n)/g(n), n \in \mathbf{N}$, lie in a finitely generated ring (we agree that for $g(n) = 0$ this means that $f(n) = 0$). It was Pisot who conjectured the converse implication, while it was van der Poorten [vdP2] who obtained a general proof (see also [R]), after an incomplete argument by Pourchet [Po]. (See [PeZ] for partial results with elementary means.)

The general case of this theorem is rather delicate, and the ingenious proof by Pourchet-van der Poorten relies on an intricate auxiliary construction and on certain p-adic estimates. However, even such a method leaves open the natural question of the *infinitude* of the set of $n \in \mathbf{N}$ such that $f(n)/g(n)$ lies in $\mathbf{Z}$, or more generally in a prescribed finitely generated ring $\mathcal{R}$: to assume that *all* the values (not merely an infinity of them) lie in $\mathbf{Z}$ (or $\mathcal{R}$) is crucial for those proofs.

For simple nondegenerate recurrences f, g defined over $\mathbf{Q}$, the problem is solved in [CZ1]. In this case, with the aid of the Subspace Theorem it is established that (see Thm 1 there):

Theorem A. *If f, g are simple recurrences with positive rational roots and if the ratio $f(n)/g(n) \in \mathbf{Z}$ for infinitely many $n \in \mathbf{N}$, then f/g is a recurrence.*

We stress that the conclusion is easy to check in practice, and can in fact be reduced to verifying the divisibility between certain polynomials (see for this [CZ1] or [CZ2, Lemma 2.1] or [vdP]). Also, the restriction to "positive" roots is harmless and the method of [CZ1] often works even over $\overline{\mathbf{Q}}$ and for non-simple recurrences, as noted in that paper.

In general however, it is crucial for that method that g admits a *dominant root* (which is automatic for positive roots in $\mathbf{R}$). By this we mean that *there exists an absolute value v of $\overline{\mathbf{Q}}$ such that g has a unique root which is maximal for v.* It may well happen that such dominant-root

assumption, often crucial in the whole theory, is not satisfied. (Consider e.g. the recurrence $g(n+3)+g(n+2)+g(n+1)=g(n)$).

Coming back to Theorem A, we pause to illustrate the method of proof in the special case when $f(n)=a^n-1$, $g(n)=b^n-1$, for integers $a,b>1$. Namely, we shall give a proof of the claim:

If $(a^n-1)/(b^n-1)\in\mathbf{Z}$ *for infinitely many* $n\in\mathbf{N}$, *then* a *is a power of* b.

We remark that if one assumes $(a^n-1)/(b^n-1)\in\mathbf{Z}$ for *all* $n\in\mathbf{N}$, the conclusion (actually a special case of van der Poorten's mentioned theorem) is capable of an elementary proof (see e.g. [PeZ]); and still another proof may be obtained by means of Algebraic Number Theory, by constructing (when the conclusion is not true) prime numbers p and integers n (of the shape $(p-1)/h$) such that p divides b^n-1 but not a^n-1 (a hint is given in [BCZ]). However none of these approaches works with the much weaker assumption of the claim.

To prove the claim, put $q(n)=(a^n-1)/(b^n-1)$ and assume that $q(n)\in\mathbf{Z}$ for all n in a certain infinite set Σ of natural numbers. To start with, fix any integer $r=r_{a,b}$ such that $b^r>a$, and observe the identity

$$(b^{rn}-1)q(n)=(a^n-1)(1+b^n+\ldots+b^{(r-1)n})$$

which may be rewritten as

$$b^{rn}q(n)+\sum_{(i,j)\in A}(-1)^i a^{in}b^{jn}=q(n),\quad A=\{0,1\}\times\{0,1,\ldots,r-1\}. \tag{2}$$

We now put $\mathbf{x}=\mathbf{x}(n)=(x_0,x_{00},\ldots,x_{1,r-1})$, where $x_0=x_0(n)=b^{rn}q(n)$ and $x_{ij}=x_{ij}(n)=a^{in}b^{jn}$ for $(i,j)\in A$. Observe that for $n\in\Sigma$ the vector $\mathbf{x}(n)$ is integral. We view the left side of (2) as the value at $\mathbf{x}(n)$ of the linear form $L(\mathbf{X})=X_0+\sum_{(i,j)\in A}(-1)^iX_{ij}$. Note that, since r has been chosen to be "large", the euclidean length $||\mathbf{x}(n)||$ of $\mathbf{x}(n)$ will grow much faster than the absolute value $|L(\mathbf{x}(n))|$ (i.e. $|q(n)|$), so we may say that L takes rather "small" values at the vectors $\mathbf{x}(n)$. We want to construct other linear forms taking small values at the $\mathbf{x}(n)$. We can do this if the smallness is interpreted in the p-adic sense, for primes p dividing ab. In fact, for these primes the values $a^{in}b^{jn}$ are in general p-adically small.

More precisely, let S denote the (finite) set of absolute values of $\mathbf{Q}$ made up of the usual one, denoted ∞, together with those corresponding to the primes p dividing ab (normalized so that $|p|_p=p^{-1}$). For any element v of S we now construct a set of $2r+1$ linearly independent linear forms in the $2r+1$ variables X_0,X_{ij} $((i,j)\in A)$, as follows. We put $L_{0,\infty}=L$ and $L_{ij,\infty}=X_{ij}$ for all $(i,j)\in A$, while for $v\in S\setminus\{\infty\}$ we simply put $L_{0,v}=X_0$, $L_{ij,v}=X_{ij}$ for $(i,j)\in A$. We now show that the linear forms are "on average" small at $\mathbf{x}=\mathbf{x}(n)$, for $n\in\Sigma$, by estimating the product

$\prod_{v\in S}(|L_{0,v}(\mathbf{x})|_v \prod_{(i,j)\in A}|L_{ij,v}(\mathbf{x})|_v)$. Observe that, if $(i,j)\in A$ we have

$$\prod_{v\in S}|L_{ij,v}(\mathbf{x})|_v = \prod_{v\in S}|x_{ij}(n)|_v = \prod_{v\in S}|a^{in}b^{jn}|_v = 1;$$

in fact, S contains all the absolute values nontrivial on a or b, whence, for any integers i,j, $\prod_{v\in S}|a^ib^j|_v = \prod_{all\ v}|a^ib^j|_v = 1$, because of the product formula on $\mathbf{Q}$. Further,

$$\prod_{v\in S}|L_{0,v}(\mathbf{x})|_v = |L(\mathbf{x})|_\infty \prod_{v\in S\setminus\infty}|x_0(n)|_v = |q(n)| \prod_{v\in S\setminus\infty}|b^{rn}q(n)|_v.$$

Now, $q(n)$ is an integer for $n\in\Sigma$, whence $|q(n)|_v\le 1$ for finite v; also, $\prod_{v\in S\setminus\infty}|b^{rn}|_v = b^{-rn}$, again by the definition of S and by the product formula. Summing up, we find

$$\prod_{v\in S}\left(|L_{0,v}(\mathbf{x}(n))|_v \prod_{(i,j)\in A}|L_{ij,v}(\mathbf{x}(n))|_v\right) \le |q(n)|b^{-rn}, \quad n\in\Sigma.$$

Recall now that $b^r > a$, so $|q(n)| < b^{(r-1)n}$ for all large $n\in\mathbf{N}$. Then both sides of the last displayed formula become $< b^{-n}$ for large $n\in\Sigma$. Also, we have $||\mathbf{x}(n)||\le (2r+1)b^{rn}a^n$, whence, for suitable numbers $c = c_{a,b}$ and $\delta = \delta_{a,b} > 0$, both independent of n, we have

$$\prod_{v\in S}\left(|L_{0,v}(\mathbf{x}(n))|_v \prod_{(i,j)\in A}|L_{ij,v}(\mathbf{x}(n))|_v\right) \le c||\mathbf{x}(n)||^{-\delta}, \quad n\in\Sigma.$$

This inequality represents precisely the fundamental assumption needed for an application of the Schmidt Subspace Theorem, in one of the versions with several places (see e.g. the version in [CZ1], due to Schlickewei). That result would in fact apply even to linear forms with algebraic coefficients (on extending in some way the absolute values to $\overline{\mathbf{Q}}$); its conclusion states that all the vectors $\mathbf{x}(n)$ in question lie in a certain finite union (independent of n) of proper linear spaces defined over $\mathbf{Q}$. In particular, recalling the definition of $\mathbf{x}(n)$, we may assume that some nontrivial equation

$$\gamma_0 b^{rn}(a^n-1) + (b^n-1)\left(\sum_{(i,j)\in A}\gamma_{ij}a^{in}b^{jn}\right) = 0 \tag{3}$$

holds for all n in a suitable infinite subset Σ' of Σ, where the coefficients γ_0,γ_{ij} are rationals not all zero. Now, this implies that a,b are multiplicatively dependent, for otherwise the functions $n\mapsto a^n$, $n\mapsto b^n$, $n\in\Sigma'$ would be algebraically independent (because Σ' is infinite), whence (3) would lead to the identity $\gamma_0V^r(U-1)+(V-1)(\sum_{(i,j)\in A}\gamma_{ij}U^iV^j) = 0$ in the variables U,V. However it is immediate to check that this yields the vanishing of all

the coefficients γ_0, γ_{ij}, a contradiction. Hence we may write $a = c^p$, $b = c^q$ for some integer $c > 1$ and some positive integers p, q and we then have just to show that q divides p. Write $p = mq + s$ for integers m, s with $0 \leq s < q$. Then $a^n = (c^{qn})^m \cdot c^{sn} \equiv c^{sn} \pmod{c^{qn} - 1}$. Therefore, since $c^{qn} - 1 = b^n - 1$ divides $a^n - 1$ for all $n \in \Sigma$, we find that $c^{qn} - 1$ divides in fact $c^{sn} - 1$ for all $n \in \Sigma$. This is however plainly impossible if $0 < s < q$, whence $s = 0$ as desired.

As remarked above such an argument works in far greater generality; however we need the mentioned "dominant root" assumption in order to construct an identity analogous to (2), i.e. a non-obvious linear form which is small at the relevant vectors. (The "obvious" forms are just the variables X_0, X_{ij}, whose values at the $\mathbf{x}(n)$ are small at suitable p-adic places.) In the general case, a small linear form may be constructed out of several dominant roots (instead of a single dominant root), but the inequality so obtained turns out to be too weak for an application of the Subspace Theorem. Nevertheless, a somewhat surprising device allows to produce many small linear forms out of a single one (one multiplies the initial linear form by many monomials in the dominant roots) and this procedure finally enables to eliminate the annoying assumption about the dominant root. The arguments appear in [CZ2] in full detail; since the construction is a bit technical we do not reproduce it here, but rather just state the main theorem of [CZ2] as:

Theorem B. *Let f, g be recurrences defined over a number field k. Suppose that S is a finite set of places of k such that $f(n)/g(n) \in \mathcal{O}_{k,S}$ for infinitely many $n \in \mathbf{N}$. Then there exist a nonzero polynomial $P(n)$ and positive integers q, r such that both $P(n)f(qn + r)/g(qn + r)$ and $g(qn + r)/P(n)$ are recurrences.*

In practice the conclusion says that, over a suitable arithmetic progression, the recurrence g divides f up to a polynomial factor. Often one can take $P = 1$: this occurs e.g. when g is simple, and hence we get a substantial extension of Theorem A. However this is not generally the case, as shown by examples like $(2^n - 2)/n$; now the quotient is integral whenever n is a prime, hence for a fairly dense set in $\mathbf{N}$. In an appendix to [CZ2] a density conclusion is shown in this direction, which in particular immediately yields a sharpening of van der Poorten's Theorem. Still in other words, these results say that a divisibility relation between infinitely many pairs of values $f(n), g(n)$ may always be explained by algebraic identities. This is rather easy to prove for polynomials f, g; we may view the above statements as analogues for polynomial-exponential functions.

Actually, the method of [CZ1] (or [CZ2]) yields, more precisely, a non-trivial bound for the cancellation in the quotient $f(n)/g(n)$, i.e. for the

g.c.d.$(f(n), g(n))$. In some cases, like $(a^n - 1)/(b^n - 1)$, it is possible with more effort to get a nearly best-possible conclusion in this direction: in [BCZ] the following is proved:

Theorem C. *If $a, b \in \mathbf{Z}$ are multiplicatively independent, then for all $\epsilon > 0$ we have the estimate $(a^n - 1, b^n - 1) \ll_\epsilon \exp(\epsilon n)$.*

Note that the relevant g.c.d. may often be quite large; in fact, the lower bound $(a^n - 1, b^n - 1) > \exp(\exp(c \log n / \log\log n))$ (some $c > 0$) is valid for infinitely many integers n (see Prop. 10 in Adleman, Pomerance, Rumely, *Annals of Math.* **117** (1983), 173-206).

The methods of [BCZ] combined with the Lang-Liardet results about points on the intersection of curves in $\mathbf{G}_m^2$ with finitely generated groups actually lead to a similar, more general, conclusion, when a^n, b^n are replaced by arbitrary S-units $u, v \in \mathbf{Z}$ (see [CZ3, Remark 1] and [Z, Thm. IV.3]). In turn, this yields in particular a proof of a (sharp form of a) conjecture by Györy-Sarkozy-Stewart; in [CZ3] we prove that:

Theorem D. *For integers $a > b > c > 0$, the greatest prime factor of $(ab + 1)(ac + 1)$ tends to infinity with a.*

The original conjecture predicted the same conclusion for $(ab + 1)$ $(ac + 1)(bc + 1)$. The result may be seen as a uniform version of the well-known theorem (due to Pólya) that the greatest prime factor of the values at integers of a quadratic polynomial with distinct rational roots tends to infinity. The link with the previous context is provided by the observation that, if $u := ab + 1$ and $v := ac + 1$ have all their prime factors in a prescribed finite set S, then u, v are S-units such that g.c.d.$(u - 1, v - 1) \geq a$ is "large".

Further applications of the methods, e.g. to study the length of the continued fraction for quotients $f(n)/g(n)$ of power-sums over $\mathbf{Q}$, have been given in [CZ4]. For instance we have:

Theorem E. *If a, b are multiplicatively independent positive integers, then the length of the euclidean algorithm for $(a^n - 1) : (b^n - 1)$ tends to infinity as n tends to infinity.*

Note that Theorems C and E express in different terms the complexity of the relevant rational fractions. Theorem E appears as Corollary 3 in [CZ4], obtained therein as an application of a general statement for arbitrary pairs of power sums with rational coefficients and roots. (See also [Z, I,IV]; the case $a^n : b^n$ was a result by Pourchet, after a question by Mendès-France; see [CZ4].)

The d-th root problem. This concerns perfect d-th powers in a recurrence sequence. In addition to the mentioned "Hadamard quotient conjecture" (solved by van der Poorten), Pisot formulated a "d-root conjecture": *If all the values $f(n)$ of a recurrence are d-th powers in a given number field k, then f is identically a d-th power of a recurrence.* After some partial results by several authors, a complete proof was given in [Z2] by means of congruence considerations; one applies the Lang-Weil bound for points on varieties over finite fields, but first one has to reduce exponential congruences to polynomial ones.

In analogy with the case of the Pisot Quotient-conjecture, the arguments in [Z2] do not help in establishing the more fundamental question of the *finiteness* of the solutions of $f(n) = y^d$, $n \in \mathbf{Z}$, $y \in k$, for a given integer $d \geq 2$ and a general recurrence f satisfying appropriate necessary assumptions. In special cases (e.g. for binary recurrences or when f has a dominant root and d is large enough with respect to f) this has been worked out by several authors, like Pethö, Shorey, Stewart, Tijdeman (see e.g. [ShSt] and [ShT]); they used Baker's method, obtaining, whenever the arguments applied, effective conclusions.[1] However, when f has three or more roots, such considerations seem not to extend to the case of general d (e.g. to the case $d = 2$).

For unrestricted (but fixed) d, the first finiteness results valid for any number of roots have been obtained in [CZ1], in the general case of simple recurrences defined over $\mathbf{Q}$. That paper actually considers arbitrary algebraic equations $F(y, f(n)) = 0$, where F is a polynomial and where f is a simple recurrence over $\mathbf{Q}$. It is also observed that the same arguments often apply to simple recurrences over $\overline{\mathbf{Q}}$ with the sole assumption of a dominant root. A result in this direction appears as Theorem 2 in [CZ5]. Here we shall mention, more generally, the problem of classifying the perfect d-th powers which may be written as sums of a bounded number of S-units; we shall work under the crucial assumption that some term in the sum is *dominant.*

We shall use the language of the algebraic group $\mathbf{G}_m^n$ and its algebraic subgroups or translates. Recall that $\mathbf{G}_m^n$ is just the affine variety $(\mathbf{A}^1 \setminus \{0\})^n$ equipped with the coordinatewise multiplicative group law; if $X_1, \ldots, X_n$ are coordinates on $\mathbf{G}_m^n$, then every algebraic subgroup (resp. translate) is defined by some finite set of equations of the shape $X_1^{a_1} \cdots X_n^{a_n} = 1$ (resp. $X_1^{a_1} \cdots X_n^{a_n} = c \neq 0$), for integers a_i.

For an algebraic point $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbf{G}_m^n(\overline{\mathbf{Q}}) = (\overline{\mathbf{Q}}^*)^n$ we shall denote by $H(\mathbf{x})$ the Weil height of the projective point $(x_1 : \ldots : x_n)$. Also,

[1] On the contrary the present arguments do not lead to effective conclusions; it is however rather easy to estimate the number of solutions, using suitable versions of the Subspace Theorem.

we let k be a number field, $S \subset M_k$ be a finite set containing all the infinite places and we pick a $\nu \in S$. We have:

Theorem F. *Let $d \in \mathbf{N}$, $\delta > 0$. Let Σ be a set of points $\mathbf{x} = (x_1, \ldots, x_n) \in (\mathcal{O}_S^*)^n$ such that:*

(i) $|x_1|_\nu \geq (\max_{j \geq 2} |x_j|_\nu) H(\mathbf{x})^\delta$.

(ii) There exists $y = y_{\mathbf{x}} \in k$ with $x_1 + \ldots + x_n = y^d$.

Then Σ is contained in a finite union of algebraic translates $\mathbf{u}H \subset \mathbf{G}_m^n$, $\mathbf{u} \in (\mathcal{O}_S^*)^n$, $H \subset \mathbf{G}_m^n$ an algebraic subgroup, such that, for a $P = P_{\mathbf{u}H} \in k[X_1^{\pm 1}, \ldots, X_n^{\pm 1}]$ and a $c = c_{\mathbf{u}H} \in k$, we have $X_1 + \ldots + X_n = cX_1 P(X_1, \ldots, X_n)^d$, as functions in $k[\mathbf{u}H]$.

Condition (i) on the "dominant term" is probably not needed, but it seems a very difficult problem to remove it. Note that the conclusion is rather restrictive on the relevant translates $\mathbf{u}H$, and admits a partial converse. (In fact, since the values of x_1 modulo d-th powers in k have finitely many possibilities, the identity implies that all the sums $x_1 + \ldots + x_n$ are, for $x_i \in \mathcal{O}_S^*$ and $(x_1, \ldots, x_n) \in \mathbf{u}H$, d-th powers in a fixed finite extension of k.)

A complete proof of this theorem is given in [Z] (see Theorem IV.5). One starts by approximating ν-adically the d-th root of $x_1 + \ldots + x_n$ by means of the binomial theorem (it is here that the dominant term is needed). Then the Subspace Theorem is applied, more or less as in the above example for the quotient problem.

The points $(y, x_1, \ldots, x_n)$ satisfying (ii) are S-integral points (see e.g. [Z] for definitions) for the hypersurface in $\mathbf{G}_a \times \mathbf{G}_m^n$ defined by $Y^d = X_1 + \ldots + X_n$. We recall that the description of the S-integral points on subvarieties of $\mathbf{G}_m^n$ is nowadays well-known, thanks to another theorem of M. Laurent (see [Z, Ch. II]): *their Zariski closure is a finite union of algebraic translates.* However, the addition of a "$\mathbf{G}_a$-piece" makes the situation considerably more difficult and largely unknown at present. Theorem F and analogous ones that can be obtained by similar ideas represent a first step in the direction of a complete description. An ideal conclusion could be as follows: *Let V be an irreducible subvariety of $\mathbf{G}_a \times \mathbf{G}_m^n$ with a Zariski-dense set of S-integral points, such that the projection $\pi : V \to \mathbf{G}_m^n$ is finite. Then $\pi(V)$ is an algebraic translate $\mathbf{u}H$ and there exist an isogeny $\sigma : H \to H$ and a morphism $\tau : H \to V$ such that $\mathbf{u}\sigma = \pi \circ \tau$.* The difficult point in this conjecture is the existence of σ, τ; in Theorem F this corresponds to the algebraic identity holding on $\mathbf{u}H$, appearing in the conclusion. For $\dim V = 1$ the conjecture is true; it follows e.g. from Siegel's Theorem on integral points on curves (see [Z, Ex. III.10] and [Z, IV]).

A simple application of Theorem F yields the following corollary for perfect power values of recurrences. (See [Z] for a detailed proof and also [CZ1,

Thm. 2] and [CZ5, Thm. 2] for algebraic equations, involving recurrences, more general than $y^d = f(n)$.)

Theorem G. *Let $f(n)$ be a simple recurrence defined over a number field k, with roots $\rho_1, \ldots, \rho_s \in k^*$. Suppose that for a place $\nu \in M_k$ we have $|\rho_1|_\nu > \max_{i=2}^s |\rho_i|_\nu$ and that there exist infinitely many $n \in \mathbf{N}$ such that $f(n)$ is a d-th power in k. Then there exist positive integers q, r and a recurrence $g(n)$ (defined over k) such that $g(n)^d = f(qn+r)$ for all $n \in \mathbf{N}$.*

Like many of the previous statements, this theorem too (which admits an obvious converse) says that an infinity of "special" values (now, the perfect d-th powers) may be often explained by an algebraic identity. We also note that in concrete cases the existence of such an identity may be easily checked, using the structure theorems on the ring of recurrences (see [vdP], [S2], [Z]). For instance, consider the perfect squares in the sequence $3^n + 2^n + 1$; in view of the algebraic independence of the functions $n \mapsto 2^n$, $n \mapsto 3^n$, their finiteness follows from Theorem G and the fact that $3^r X_1^q + 2^r X_2^q + 1$ is not a square in $\mathbf{Q}[X_1^{\pm 1}, X_2^{\pm 1}]$, no matter the positive integers q, r.

I owe to Attila Pethö the remark that, by combining results like Theorem G with the above alluded conclusions on d-th powers in recurrences for large d (e.g. those in [ShSt]), one may obtain a description of the d-th power values for *variable* d. For instance: *If $f(qn+r)$ is never identically a d-th power recurrence for $d \geq 2$, where f is as in Theorem G, then the equation $f(n) = y^d$ has only a finite number of solutions $(d, n, y) \in (\mathbf{N} \setminus \{0, 1\}) \times \mathbf{N} \times k$.* This conclusion follows immediately by applying [ShSt] if d is larger than a certain d_f depending on f and Theorem G for $d \leq d_f$.

Results like Theorem G have yielded in particular a solution to problems by M. Yasumoto concerning *Universal Hilbert Sets* of exponential shape; we recall that a Universal Hilbert Subset (UHS) of $\mathbf{Z}$ is an infinite set $\mathcal{H}$ of integers such that, for any polynomial $P(X, Y) \in \mathbf{Q}[X, Y]$ irreducible in $\mathbf{Q}[X, Y]$, the polynomial $P(h, Y)$ is irreducible in $\mathbf{Q}[Y]$ for all but finitely many elements $h \in \mathcal{H}$ (the finite exceptional set depending on P). M. Yasumoto conjectured in 1987 (*J. Number Theory*, **26**) that sets like $\{2^n + n : n \in \mathbf{N}\}$ or $\{2^n + 3^n : n \in \mathbf{N}\}$ are UHS. Partial results were obtained in [DZ], where it was proved that e.g. $\{2^n + n : n \in \mathbf{N}\}$ and $\{2^n + 5^n : n \in \mathbf{N}\}$ are UHS. Yasumoto's questions were completely answered affirmatively in [CZ1], where a characterization was proved on the UHS of the shape $\{f(n) : n \in \mathbf{N}\}$, for a simple recurrence f defined over $\mathbf{Q}$ (see Thm. 4 therein). As a corollary it was proved that:

Theorem H. *For multiplicatively independent positive integers $a_1, \dots, a_s$ ($s \geq 2$) and nonzero integers $c_1, \dots, c_s$, the set $\{c_1 a_1^n + \dots + c_s a_s^n : n \in \mathbf{N}\}$ is a Universal Hilbert Set.*

We conclude with a few remarks on some special diophantine equation. As we have noted, Theorem G above (or even Thm. H) proves in particular that equations like $y^2 = 1+2^n+3^n$ have only finitely many solutions $(n, y) \in \mathbf{N} \times k$. An application of Theorem F with respect to two distinct places ν sometimes yields a finiteness conclusion by adding a further variable; e.g., we have: *The equation $y^2 = 1 + 2^m + 6^n$ has only finitely many solutions $(m, n, y) \in \mathbf{N}^2 \times k$.* (See the paper [CZ6] for rather more general equations in three variables. Recently the special equation $y^2 = 1 + 2^m + 2^n$ has been completely solved by L. Szalay.)

In this example it is crucial that $2, 6$ are not coprime (so Thm. F may be applied with $\nu = \infty$ or $\nu = 2$, according as m/n lies "near" or not to 0 or ∞). In fact, it seems not known whether an equation like $y^2 = 1 + 2^m + 3^n$ may have an infinity of solutions $(m, n, y) \in \mathbf{N}^2 \times k$.[2] We now illustrate how such equations happen to be less artificial than they perhaps appear (though they are certainly special ones). Actually, they represent a typical instance of the problem of the S-integral points on a variety $\mathbf{P}_2 \setminus D$, where D is a divisor which is the sum of two lines and a conic in general position. To see the link, say that the lines and conic are given by $X_0 = 0$, $X_1 = 0$ and $X_2^2 = X_0^2 + X_0 X_1$, and that $S = \{\infty, 2, 3\}$. Then the S-integral points $(x_0 : x_1 : x_2)$ are those such that both $u = x_1/x_0$ and $v = (x_2/x_0)^2 - 1 - (x_1/x_0)$ are S-units. That is, they correspond to S-units u, v such that $1 + u + v$ is a perfect square. On the other hand, u, v have the shape $\pm 2^a 3^b$, and the connection with the above equations becomes clear. In particular, by known results one may show that an infinite set of solutions $(m, n, y) \in \mathbf{N}^3$ to $y^2 = 1 + 2^m + 3^n$ would produce a Zariski-dense set of S-integral points for $\mathbf{P}_2 \setminus D$.

Now, a broad conjecture by Lang and Vojta (see [HS, p. 486]) predicts in particular that removing from $\mathbf{P}_2$ a divisor D with normal crossings and of degree (at least) four leaves a variety whose set of S-integral points is not Zariski dense. This is known when D is the sum of four lines in general position; the next simplest case, presently unknown, occurs just when D has the above mentioned shape. Thus the above equations arise in one of the simplest unknown cases of the Lang-Vojta conjecture. This again illustrates a relation of some of the problems in question with central themes from Diophantine Geometry, providing further motivations for the subject.

---

[2] This is excluded by a conjecture of Lang and Vojta, as we show in a moment. From Thm. F one can deduce that for any possible infinite sequence of solutions the ratio $m/n \to \log 3/\log 2$.

References

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

[CZ1] P. CORVAJA, U. ZANNIER, *Diophantine equations with power sums and Universal Hilbert Sets.* Indag. Mathem., N.S. **9** (3) (1998), 317–332.

[CZ2] P. CORVAJA, U. ZANNIER, *Finiteness of integral values for the ratio of two linear recurrences.* Invent. Math. **149** (2002), 431–451.

[CZ3] P. CORVAJA, U. ZANNIER, *On the greatest prime factor of $(ab+1)(ac+1)$.* Proc. Amer. Math. Soc. **131** (2003), 1705–1709.

[CZ4] P. CORVAJA, U. ZANNIER, *On the length of the continued fraction for values of quotients of power sums.* Preprint 2003, to appear on Journal de Théorie des nombres de Bordeaux.

[CZ5] P. CORVAJA, U. ZANNIER, *Some New Applications of the Subspace Theorem*, Compositio Math. **131** (2002), 319–340.

[CZ6] P. CORVAJA, U. ZANNIER, On the diophantine equation $f(a^m, y) = b^n$. Acta Arith. **94**.1 (2000), 25–40.

[DZ] P. DÈBES, U. ZANNIER, *Universal Hilbert Subsets.* Math. Proc. Camb. Phil. Soc. **124** (1998), 127–134.

[HS] M. HINDRY, J.H. SILVERMAN, *Diophantine Geometry.* Springer-Verlag, 2000.

[PeZ] A. PERELLI, U. ZANNIER, *Arithmetic properties of certain recurrent sequences.* J. Austral. Math. Soc. (A) **37** (1984), 4–16.

[vdP] A.J. VAN DER POORTEN, *Some facts that should be better known, especially about rational functions.* In Number Theory and Applications, (Banff, AB 1988), 497–528, Kluwer Acad. Publ., Dordrecht, 1989.

[vdP2] A.J. VAN DER POORTEN, *Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles.* C. R. Acad. Sci. Paris **306** (1988), 97–102.

[Po] Y. POURCHET, *Solution du problème arithmétique du quotient de Hadamard de deux fractions rationnelles.* C. R. Acad. Sci. Paris **288**, Série *A* (1979), 1055–1057.

[R] R. RUMELY, *Note on van der Poorten's proof of the Hadamard quotient theorem I, II.* In: Séminaire de Théorie des nombres de Paris 1986-87, 349–409, Progress in Math. **75**, Birkhäuser, Boston, 1988.

[S] W.M. SCHMIDT, *The zero multiplicity of linear recurrence sequences.* Acta Math. **182** (1999), 243–282.

[S2] W.M. SCHMIDT, *Linear Recurrence Sequences and Polynomial-Exponential Equations.* In Diophantine Approximation, F. Amoroso, U. Zannier Eds., Proc. of the C.I.M.E. Conference, Cetraro (Italy), 2000, Springer-Verlag LNM **1819**, 2003.

[ShSt] T.N. SHOREY, C.L. STEWART, *Pure Powers in Recurrence Sequences and Some Related Diophantine Equations.* Journal of Number Theory **27** (1987), 324–352.

[ShT] T.N. SHOREY, R. TIJDEMAN, *Exponential Diophantine Equations.* Camb. Univ. Press, 1986.

[Z] U. ZANNIER, *Some applications of Diophantine Approximation to Diophantine Equations.* Editrice Forum, Udine, Dicembre 2003.

[Z2] U. ZANNIER, *A proof of Pisot d^{th} root conjecture.* Annals of Math. **151** (2000), 375–383.

Umberto ZANNIER
Scuola Normale Superiore
Piazza dei Cavalieri, 7
56126 Pisa, ITALY
E-mail : u.zannier@sns.it