POLYNOMIAL–EXPONENTIAL EQUATIONS AND LINEAR RECURRENCES*

CLEMENS FUCHS

ABSTRACT. Let K be an algebraic number field and let (G_n) be a linear recurring sequence defined by $G_n = \lambda_1\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_t(n)\alpha_t^n$, where $\lambda_1, \alpha_1, \ldots, \alpha_t$ are non-zero elements of K and where $P_i(x) \in K[x]$ for $i = 2, \ldots, t$. Furthermore let $f(z, x) \in K[z, x]$ monic in x. In this paper we want to study the polynomial–exponential Diophantine equation $f(G_n, x) = 0$. We want to use a quantitative version of W. M. Schmidt's Subspace Theorem (due to J.-H. Evertse [8]) to calculate an upper bound for the number of solutions (n, x) under some additional assumptions.

Address: Institut für Mathematik, Technische Universität Graz, Steyrergasse 30, 8010 Graz, Austria
E-mail: clemens.fuchs@tugraz.at
2000 *Mathematics Subject Classification:* 11D45,11D61.
Keywords: polynomial-exponential equations, linear recurrences, Subspace-Theorem

1. Introduction

Let $A_1, A_2, \ldots, A_k$ and $G_0, G_1, \ldots, G_{k-1}$ be algebraic numbers over the rationals and let (G_n) be a k-th order linear recurring sequence given by

$$G_n = A_1G_{n-1} + \cdots + A_kG_{n-k} \quad \text{for} \quad n = k, k+1, \ldots. \tag{1}$$

Let $\alpha_1, \alpha_2, \ldots, \alpha_t$ be the distinct roots of the corresponding characteristic polynomial

$$X^k - A_1X^{k-1} - \cdots - A_k. \tag{2}$$

Then for $n \geq 0$

$$G_n = P_1(n)\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_t(n)\alpha_t^n, \tag{3}$$

where $P_i(n)$ is a polynomial with degree less than the multiplicity of α_i; the coefficients of $P_i(n)$ are elements of the field: $\mathbb{Q}(G_0, \ldots, G_{k-1}, A_1, \ldots, A_k, \alpha_1, \ldots, \alpha_t)$. We shall be interested in linear recurring sequences (G_n), where G_n defined as in (3) for which $P_1(n)$ is a non-zero constant, λ_1 say. Thus

$$G_n = \lambda_1\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_t(n)\alpha_t^n. \tag{4}$$

Date: February 3, 2003.
*This work was supported by the Austrian Science Foundation FWF, grant S8307-MAT.

The recurring sequence is called simple, if all characteristic roots are simple. (G_n) is called nondegenerate, if no quotient α_i/α_j for all $1 \le i < j \le t$ is equal to a root of unity and degenerate otherwise. Observe that, even if (G_n) is degenerate, there exists a positive integer d such that, (G_{r+md}) is nondegenerate or identically zero on each of the d arithmetic progressions with $0 \le r < d$. Therefore, restricting to nondegenerate recurring sequences causes no substantial loss of generality.

Let $f(z,x)$ be a polynomial with algebraic coefficients, which is monic in x. In the present paper we deal with the Diophantine equation

$$f(G_n, x) = 0, \tag{5}$$

which was earlier investigated by several authors in the special case $f(z,x) = Ex^q - z, E \in \mathbb{Z}\backslash\{0\}$, which yields the Diophantine equation

$$G_n = Ex^q, \quad E \in \mathbb{Z}\backslash\{0\}. \tag{6}$$

A survey about this equation can be found in [9]. We cite here only those papers, which are of interest for us.

Let us mention that similar types of equations, namely

$$f(x, y, \alpha^x) = 0 \quad \text{and} \quad f(x, y, \alpha^x, \beta^y) = 0,$$

where f is a polynomial with complex coefficients and α, β are non-zero complex numbers, were studied by Schmidt [22] and Ahlgren [1, 2]. They showed that these equations can have solutions with arbitrarily large values of $|x|$ only in the case when f and α, β are of a particularly simple form.

For a nondegenerate recurring sequence (G_n) of order 2 induced by a (rational) integral recurrence, it has been proved, independently, by Pethő [14] and Shorey and Stewart [24] that for the solutions $x \in \mathbb{Z}, |x| > 1$ and $q \ge 2$ of (6) $\max(|x|, q, n)$ is bounded by an effectively computable constant depending only on E and the sequence (G_n). Pethő [14] extended in fact this result to the equation $G_n = bx^q$ with $b \in S$, where S is a set of integers composed solely of a finite number of primes, provided that the coefficients of the defining difference equation of G_n are coprime integers.

Shorey and Stewart [24] proved the above finiteness result for certain recurring sequences of order > 2. Let (G_n) be an integral nondegenerate linear recurring sequence given by

$$G_n = \lambda_1 \alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_t(n)\alpha_t^n, \tag{7}$$

where λ_1 is a non-zero constant, $|\alpha_1| > |\alpha_j|$ for $j = 2, \ldots, t$, and $G_n - \lambda_1\alpha_1^n \ne 0$. Then assuming $x, q > 1$ the solutions q of (6) can be bounded by an effectively computable constant which depends on E and the coefficients and initial values of the recurrence. Kiss [11] proved that, in fact, q is less than a number which is effectively computable in terms of the greatest prime divisor of E and the coefficients and the initial values of the sequence (G_n).

Nemes and Pethő [12] studied the more general equation

$$G_n = Ex^q + T(x), \tag{8}$$

where $T(x)$ is a polynomial of degree r and of height H with integral coefficients. For fixed $E \in \mathbb{Z}$ and T they established bounds for the integral solutions n, q, x with $|x|, q > 1$. Let (G_n) be defined as in (7) and assume

$$|\alpha_1| > |\alpha_2| > |\alpha_j|, \quad \text{for} \quad j = 3, \dots, t, \tag{9}$$

with $\alpha_2 \neq \pm 1$. Nemes and Pethő showed that $q < C_1$ provided that $n > C_2$ and $r < C_3 q$, where C_1, C_2 and C_3 are suitable positive numbers which are effectively computable in terms of E, H and the coefficients and initial values of the recurrence. For second order recurrences (G_n) with $|A_2| = 1$ Nemes and Pethő [13] characterized all polynomials P for which the equation $G_n = P(x)$ has infinitely many solutions (see also [16]). Kiss [11] and Shorey and Stewart [25] dealt with equation (8) for nondegenerate linear recurring sequences (G_n) of arbitrary order, under condition (9) and the additional assumptions that d is the degree of α_1 over $\mathbb{Q}$, α_1 and α_2 are multiplicatively independent and $\alpha_2 \neq \pm 1$. Then they showed that there are only finitely many integers n, x and q with $n \geq 0, |x| > 1$ and

$$q > \max\left(\frac{d \log|\alpha_1|}{\log(|\alpha_1|/\max(1, |\alpha_2|))}, d + r\right)$$

for which

$$G_n = x^q + T(x)$$

holds.

Recently Corvaja and Zannier [4] considered linear recurrences defined by

$$G_n = a_1\alpha_1^n + a_2\alpha_2^n + \cdots + a_t\alpha_t^n,$$

where $t \geq 2, a_1, a_2, \dots, a_t$ are non-zero rational numbers, $\alpha_1 > \alpha_2 > \cdots > \alpha_t > 0$ are integers. They used Schmidt's Subspace Theorem [19], [21] to show that for every integer $q \geq 2$ the equation

$$G_n = x^q \tag{10}$$

has only finitely many solutions $(n, x) \in \mathbb{N}^2$ assuming that G_n is not identically a perfect qth power for any n in a suitable arithmetic progression. Tichy and the author [9] gave a quantitative version of the above result of Corvaja and Zannier.

Tichy and the author [9] also showed by combining their result with the previously mentioned result of Nemes and Pethő [12] that the following is true: Let (G_n) be a linear recurring sequence defined as above, such that (for fixed $q \geq 2$) there is no $r \in \{0, \ldots, q-1\}$ with G_{mq+r} a perfect qth power for all $m \in \mathbb{N}$. Then the equation

$$G_n = x^q$$

has only finitely many integral solutions $n, x > 1, q$. The number of solutions can be bounded by an explicitly computable constant C depending only on the recurrence.

Very recently, Pethő [17] used the above result of Corvaja and Zannier to show that there are only finitely many perfect powers in a third order linear recurring sequence (G_n), if we assume that the characteristic polynomial of (G_n) is irreducible and has a dominating root.

2. Results

Our main result is the generalization of the above quantitative result to the Diophantine equation $f(G_n, x) = 0$, where (G_n) is defined by (4). This will generalize and quantify a very recent result due to Corvaja and Zannier [5] (cf. Remark 1).

Theorem 1. *Let K be an algebraic number field and let (G_n) be a nondegenerate linear recurring sequence defined by*

$$G_n = \lambda_1 \alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_t(n)\alpha_t^n,$$

where $t \geq 2, \lambda_1$ is a non-zero element of K, $P_i(x) \in K[x]$ for all $i = 2, \ldots, t$ and where $\alpha_1, \ldots, \alpha_t$ are elements of K with $1 \neq |\alpha_1| > |\alpha_j|$ for all $j = 2, \ldots, t$. Let $f(z, x) \in K[z, x]$ be monic in x and suppose that there do not exist non-zero algebraic numbers β_j and polynomials $d_j(n) \in \bar{K}[n]$ for $j = 1, \ldots, k$ such that

$$f\left(G_n, \sum_{j=1}^{k} d_j(n)\beta_j^n\right) = 0 \tag{11}$$

for all n in an arithmetic progression. Then the number of solutions $(n, x) \in \mathbb{N} \times K$ of the equation

$$f(G_n, x) = 0$$

is finite and can be bounded by an explicitly computable number C depending on f and on the coefficients and the initial values of the recurrence.

Remark 1. Corvaja and Zannier showed in [5], under the restriction that the recurrence is simple, that the assumption of $f(G_n, x) = 0$ having infinitely many solutions implies that there exist $d_j, \beta_j \in \bar{K}\backslash\{0\}, j = 1, \ldots, k$, and an arithmetic progression $\mathcal{P}$ such that

$$f\left(G_n, \sum_{j=1}^{k} d_j\beta_j^n\right) = 0, \quad \text{for } n \in \mathcal{P}.$$

Remark 2. Observe that one can effectively determine whether there do exist non-zero numbers $\beta_j \in \bar{K}$ and polynomials $d_j(n) \in \bar{K}[n]$ for $j = 1, \dots, k$ such that (11) holds for all n in an arithmetic progression or not (see [5]). The following example shows that this condition is necessary: let

$$G_n = 18^n + 2 \cdot 6^n + 2^n,$$

and $f(z,x) = x^2 - z$. The coefficients and roots have the desired properties, but

$$G_{2k} = (18^k + 2^k)^2,$$

so $f(G_{2k}, 18^k + 2^k) = 0$ for all $k \in \mathbb{N}$. Another much simpler example is obtained by taking $f(z,x) = x - z$.

Remark 3. We want to note that the above assumption (11) also means (for $k = 0$) that $f(z,0) = 0$ does not hold identically or equivalently x is not a divisor of $f(z,x)$. For example $f(z,x) = x - z \cdot x$, which yields solutions $(n,0) \in \mathbb{N}^2$ for all $n \in \mathbb{N}$, is excluded.

Remark 4. Let us mention that the condition on the dominant root α_1 is crucial. The proof of the theorem heavily depends on that assumption.

Remark 5. For simplicity we have introduced the condition that $f(z,x)$ is monic in x. There is no problem at all, if we assume that the leading coefficient of f with respect to x does not depend on z. Moreover, it is a well-known trick how to get rid of this assumption (with a corresponding modification of the theorem); namely we may replace $f(z,x)$ with the polynomial $a(z)^{d-1} f(z, x/a(z))$, where $a(z), d$ is the leading coefficient, the degree respectively of f with respect to x.

Next we want to state some conclusion concerning special cases of the above result.

Corollary 1. *Let (G_n) be a nondegenerate linear recurring sequence defined by*

$$G_n = \lambda_1 \alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_t(n)\alpha_t^n,$$

where $t \geq 2, \lambda_1$ is a non-zero rational number, $P_i(x) \in \mathbb{Q}[x]$ for all $i = 2, \dots, t$ and where $\alpha_1, \dots, \alpha_t$ are rational numbers with $1 \neq |\alpha_1| > |\alpha_j|$ for all $j = 2, \dots, t$. Let $P(x) \in \mathbb{Q}[x]$ be monic and suppose that there do not exist non-zero algebraic numbers β_j and polynomials $d_j(n) \in \bar{\mathbb{Q}}[n]$ for $j = 1, \dots, k$ such that

$$G_n = P\left(\sum_{j=1}^{k} d_j(n)\beta_j^n\right) \tag{12}$$

for all n in an arithmetic progression. Then the number of solutions $(n,x) \in \mathbb{N} \times \mathbb{Q}$ of the equation

$$G_n = P(x)$$

is finite and can be bounded by an explicitly computable number C depending on P and on the coefficients and the initial values of the recurrence.

Remark 6. The above corollary is also true, if we assume $P(x) \in \mathbb{Q}(x)$, say $P(x) = f(x)/g(x)$, where $f(x)$ is a monic polynomial.

Remark 7. Also the classical case $P(x) = x^q$, concerning the number of perfect powers in the linear recurring sequence (G_n) is included. So we get a generalization of the results stated in [9]. Observe that from [4] it follows that condition (12) is equivalent to the assumption that G_n is not equal to a perfect qth power for all n in an arithmetic progression (cf. also [29]).

Last we want to discuss some families of Diophantine equations related to the above types of equations.

Corollary 2. *Let (G_n) be an integral nondegenerate linear recurring sequence with (4), where $t \geq 2, \lambda_1$ is a non-zero element of $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_t)$, $P_i(x) \in K[x]$ for all $i = 2, \ldots, t$ and where $\alpha_1, \ldots, \alpha_t$ are algebraic integers with $1 \neq |\alpha_1| > |\alpha_j|$ for all $j = 2, \ldots, t$. Furthermore, suppose that there do not exist non-zero numbers $\beta_j \in \bar{K}$ and polynomials $d_j(n) \in \bar{K}[n]$ for $j = 1, \ldots, k$ such that*

$$G_n = \left(\sum_{j=1}^{k} d_j(n) \beta_j^n \right)^q \tag{13}$$

for all n in an arithmetic progression and for given $q \geq 2$. Then the number of solutions $(n, x, q) \in \mathbb{N}^3$ with $n, x, q > 1$ of the equation

$$G_n = x^q$$

is finite and can be bounded by an explicitly computable number C depending only on the coefficients and the initial values of the recurrence.

Remark 8. Observe that condition (13) can be verified effectively, because under the other assumptions one can calculate an upper bound for q first. Then condition (13) must only be verified for q smaller than this bound.

Corollary 3. *Let (G_n) be an integral nondegenerate linear recurring sequence with (4), where $t \geq 2, \lambda_1$ is a non-zero rational element of $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_t)$, $P_i(x) \in K[x]$ for all $i = 2, \ldots, t$ and where $\alpha_1, \ldots, \alpha_t$ are algebraic integers with $1 \neq |\alpha_1| > |\alpha_2| > |\alpha_j|$ for all $j = 3, \ldots, t$ and α_1, α_2 multiplicatively independent. Let $\alpha_2 \neq \pm 1$ and let $T(x)$ be a polynomial with integer coefficients and degree r; we take $r = 0$ if $T(x)$ is the zero polynomial. Furthermore, suppose that there do not exist non-zero numbers $\beta_j \in \bar{K}$ and polynomials $d_j(n) \in \bar{K}[n]$ for $j = 1, \ldots, k$ such that*

$$G_n = \left(\sum_{j=1}^{k} d_j(n) \beta_j^n \right)^q + T\left(\sum_{j=1}^{k} d_j(n) \beta_j^n \right) \tag{14}$$

for all n in an arithmetic progression and for given $q \geq 2$. Then there are only finitely many integers n, x and q with $n \geq 0, q \geq 1$ and $|x| > 1$ for which

$$G_n = x^q + T(x)$$

holds.

3. Auxiliary Results

Our proof of Theorem 1 depends on a quantitative version of the Subspace Theorem due to J.-H. Evertse [8].

Let K be an algebraic number field. Denote its ring of integers by O_K and its collection of places by M_K. For $v \in M_K$, $x \in K$, we define the absolute value $|x|_v$ by

(i) $|x|_v = |\sigma(x)|^{1/[K:\mathbb{Q}]}$ if v corresponds to the embedding $\sigma : K \hookrightarrow \mathbb{R}$;

(ii) $|x|_v = |\sigma(x)|^{2/[K:\mathbb{Q}]} = |\bar{\sigma}(x)|^{2/[K:\mathbb{Q}]}$ if v corresponds to the pair of conjugate complex embedding $\sigma, \bar{\sigma} : K \hookrightarrow \mathbb{C}$;

(iii) $|x|_v = (N\wp)^{-\mathrm{ord}_\wp(x)/[K:\mathbb{Q}]}$ if v corresponds to the prime ideal $\wp$ of O_K.

Here $N\wp = \#(O_K/\wp)$ is the norm of $\wp$ and $\mathrm{ord}_\wp(x)$ the exponent of $\wp$ in the prime ideal decomposition of (x), with $\mathrm{ord}_\wp(0) := \infty$. In case (i) or (ii) we call v real infinite or complex infinite, respectively; in case (iii) we call v finite. These absolute values satisfy the *Product formula*

$$\prod_{v \in M_K} |x|_v = 1 \quad \text{for } x \in K^*. \tag{15}$$

The *height* of $\mathbf{x} = (x_1, \dots, x_n) \in K^n$ with $\mathbf{x} \neq \mathbf{0}$ is defined as follows: for $v \in M_K$ put

$$\begin{aligned}
|\mathbf{x}|_v &= \left(\textstyle\sum_{i=1}^n |x_i|_v^{2[K:\mathbb{Q}]}\right)^{1/(2[K:\mathbb{Q}])} && \text{if } v \text{ is real infinite,}\\
|\mathbf{x}|_v &= \left(\textstyle\sum_{i=1}^n |x_i|_v^{[K:\mathbb{Q}]}\right)^{1/[K:\mathbb{Q}]} && \text{if } v \text{ is complex infinite,}\\
|\mathbf{x}|_v &= \max(|x_1|_v, \dots, |x_n|_v) && \text{if } v \text{ is finite}
\end{aligned}$$

(note that for infinite places v, $|\cdot|_v$ is a power of the Euclidean norm). Now define

$$\mathcal{H}(\mathbf{x}) = \mathcal{H}(x_1, \dots, x_n) = \prod_v |\mathbf{x}|_v.$$

For a linear form $l(\mathbf{X}) = a_1X_1 + \cdots + a_nX_n$ with algebraic coefficients we define $\mathcal{H}(l) := \mathcal{H}(\mathbf{a})$, where $\mathbf{a} = (a_1, \dots, a_n)$ and if $\mathbf{a} \in K^n$ then we put $|l|_v = |\mathbf{a}|_v$ for $v \in M_K$. Further we define the number field $K(l) := K(a_1/a_j, \dots, a_n/a_j)$ for any j with $a_j \neq 0$; this is independent of the choice of j.

We are now ready to state Evertse's result [8]. The following notations are used:

- S is a finite set of places on K of cardinality s containing all infinite places;

- $\{l_{1v},\ldots,l_{nv}\}$, $v\in S$ are linearly independent sets of linear forms in n variables with algebraic coefficients such that

$$\mathcal{H}(l_{iv})\le H,\quad [K(l_{iv}):K]\le D\quad \text{for } v\in S,\ i=1,\ldots,n.$$

We choose for every place $v\in M_K$ a continuation of $|\cdot|_v$ to the algebraic closure of K and denote this also by $|\cdot|_v$.

Theorem 2. (Quantitative Subspace Theorem, Evertse) *Let $0<\delta<1$ and consider the inequality for $\mathbf{x}\in K^n$.*

$$\prod_{v\in S}\prod_{i=1}^{n}\frac{|l_{iv}(\mathbf{x})|_v}{|\mathbf{x}|_v}<\left(\prod_{v\in S}|\det(l_{1v},\ldots,l_{nv})|_v\right)\cdot\mathcal{H}(\mathbf{x})^{-n-\delta}. \tag{16}$$

Then the following assertions hold:
(i) There are proper linear subspaces $T_1,\ldots,T_{t_1}$ of K^n, with

$$t_1\le(2^{60n^2}\cdot\delta^{-7n})^s\log 4D\cdot\log\log 4D$$

such that every solution $\mathbf{x}\in K^n$ of (16) satisfying $\mathcal{H}(\mathbf{x})\ge H$ belongs to $T_1\cup\cdots\cup T_{t_1}$.
(ii) There are proper linear subspaces $S_1,\ldots,S_{t_2}$ of K^n, with

$$t_2\le(150n^4\cdot\delta^{-1})^{ns+1}(2+\log\log 2H)$$

such that every solution $\mathbf{x}\in K^n$ of (16) satisfying $\mathcal{H}(\mathbf{x})<H$ belongs to $S_1\cup\cdots\cup S_{t_2}$.

We also need the following theorem of W. M. Schmidt [23] concerning the zero multiplicity of a nondegenerate recurring sequence.

Theorem 3. (W. M. Schmidt) *Suppose that $(G_n)_{n\in\mathbb{Z}}$ is a nondegenerate linear recurring sequence of complex numbers, whose characteristic polynomial has k distinct roots of multiplicity $\le a$. Then the number of solutions $n\in\mathbb{Z}$ of the equation*

$$G_n=0,$$

can be bounded by

$$A(k,a)=e^{(7k^a)^{8k^a}}.$$

(This number of solutions is called the zero multiplicity of the recurrence.)

Finally, we need some results from the theory of algebraic functions fields, which can be found in the monographs of Eichler [7] and Iwasawa [10], namely the theory of Puiseux expansions.

Let K be an algebraic number field, which is generated over the field of rational numbers $\mathbb{Q}$. We assume that $f(x,y)$ is an absolutely irreducible polynomial in x and y, with coefficients in the algebraic number field K, that is f is irreducible over the algebraic closure $\bar{K}$ of K. We denote by F the field obtained by adjoining a root of $f(x,y)$ to $\bar{K}(x)$, the field of rational functions in x with coefficients in the algebraic closure of K. Then F is an algebraic function field over the algebraically closed field $\bar{K}$ of characteristic 0.

Theorem 4. (Puiseux's Theorem) *Let F be an algebraic functions field over an algebraically closed field $\bar{K}$ of characteristic* 0, *given by $f(x,y)=0$. For simplicity we suppose $f(x,y)$ to be monic in y. Let us denote by $n=[F:\bar{K}(x)]$ the degree of F over $\bar{K}(x)$. Then with every element $\xi\in K$ there are associated $r=r(\xi)\le n$ natural number $e_i=e_i(\xi)$ whose sum is*

$$e_1+\cdots+e_r=n;$$

similar numbers $e_i(\infty)$ are associated with the symbol $\xi=\infty$. These numbers have the following meaning: Setting

$$z_\xi=x-\xi,\quad z_\infty=1/x, \tag{17}$$

the irreducible equation $f(x,y)=0$ satisfied by an arbitrary function y of F over $\bar{K}$ has for solutions the $r=r(\xi)$ power series

$$y_i=\sum_{k=v_i}^{\infty}a_{ik}(\sqrt[e_i(\xi)]{z_\xi})^k,\quad a_{iv_i}\neq 0,\quad i=1,2,\dots,r(\xi). \tag{18}$$

With a primitive e_ith root of unity ζ form

$$y_{ij}=\sum_k a_{ik}\zeta^{jk}(\sqrt[e_i(\xi)]{z_\xi})^k,\quad j=0,\dots,e_i(\xi)-1; \tag{19}$$

then the left side of $f(x,y)=0$ is identical with

$$f(x,y)=\prod_{j,i}(y-y_{ij}). \tag{20}$$

The coefficients a_{ik} are elements of a finite field extension K' of K, and their images under isomorphisms of K' give permutations of the y_{ij} in (20). The power series have respective radii of convergence $\neq 0$.

Let us mention that the theory of Puiseux expansions is equivalent to the valuation theory. The numbers $e_i(\xi)$, $i=1,\dots,r(\xi)$ are called ramifications indices related to the place generated by $z_\xi=x-\xi$, respectively $z_\infty=1/x$ in the rational function field $\bar{K}(x)$.

We also want to state an explicit form of the last theorem, which enables us to derive estimates for the coefficients of the Puiseux expansions of an algebraic function and which is due to Coates (cf. [3]).

We introduce the following notation first. If α is an algebraic number, then $\deg\alpha,\delta(\alpha),h(\alpha)$ denote respectively the degree of α, the least positive rational integer such that $\delta(\alpha)\alpha$ is an algebraic integer, and the maximum of the absolute values of the conjugates of α, and we put $\sigma(\alpha)=\max\{\deg\alpha,\delta(\alpha),h(\alpha)\}$. Let $f(x,y)$ be as above and let the maximum of the absolute values of the conjugates of the coefficients of $f(x,y)$ be at most f, where $f \geq 2$, and let $f(x,y)$ have degree m and n in x and y, respectively. Put $N = \max\{n, m, 3\}$.

Theorem 5. (Explicit Puiseux's Theorem, Coates) *Let F be an algebraic functions field over an algebraically closed field $\bar{K}$ of characteristic 0, given by $f(x,y) = 0$. Let $\xi \in K$ and A_i $(1 \leq i \leq r = r(\xi))$ be the valuations of F extending the valuation of $\bar{K}(x)$ defined by $x - \xi$, and let e_i be the ramification index of A_i. We write*

$$y = \sum_{k=0}^{\infty} w_{ik}(x-\xi)^{k/e_i}$$

for the Puiseux expansion of y at A_i. Then the coefficients w_{ik} $(1 \leq i \leq r, k = 0, 1, \ldots)$ are algebraic numbers, and the number field K' obtained by adjoining ξ and these coefficients to K has degree at most $(N \deg \xi)^N$ over K. Further, K' is generated over K by ξ and w_{ik} $(1 \leq i \leq r, 0 \leq k \leq 2N^4)$. Finally, there exists a positive rational integer Δ such that $\Delta^{k+1} w_{ik}$ $(1 \leq i \leq r, k = 0, 1, \ldots)$ is an algebraic integer with

$$\max\{\Delta^{k+1}, \Delta^{k+1} h(w_{ik})\} \leq \Lambda^{k+1}, \tag{21}$$

where $\Lambda = (f\sigma(\xi))^{\mu}$, $\mu = (N^4 n \deg \xi)^{3N^4}$.

Let Q_i $(1 \leq i \leq r(\infty))$ be the valuations of F extending the valuation of $\bar{K}(x)$ defined by $1/x$. Let e_i be the ramification index of Q_i, and let

$$y = \left(\frac{1}{x}\right)^{-m} \sum_{k=0}^{\infty} w_{ik} \left(\frac{1}{x}\right)^{k/e_i}$$

be the expansion of y at Q_i. Then the coefficients are algebraic numbers, and the number field K' obtained by adjoining them to K has degree at most N^N over K. Further K' is generated over K by the w_{ik} $(1 \leq i \leq r, 0 \leq k \leq 2N^4)$. Finally, there exists a positive rational integer Δ such that $\Delta^{k+1} w_{ik}$ $(1 \leq i \leq r, k = 0, 1, \ldots)$ is an algebraic integer with

$$\max\{\Delta^{k+1}, \Delta^{k+1} h(w_{ik})\} \leq \Lambda^{k+1}, \tag{22}$$

where $\Lambda = f^{\mu}$, $\mu = (N^4 n)^{3N^4}$.

The value Λ is called the Eisenstein constant, due to Eisenstein who first proved the qualitative statement from above. Let us mention that improvements on the Eisenstein constant (at least in special cases) can be found in [20, 6].

We want to remark that the proof of the last theorem yields an algorithm for the actual determination of the coefficients of the Puiseux expansion of an algebraic function. In fact, for the proof one constructs polynomials $p_i(w)$ with coefficients in the field obtained by adjoining the first i coefficients of the Puiseux expansion in question, such that the $(i+1)$st coefficient is a root of $p_i(w)$. From this sequence of polynomials everything follows (see [3]).

4. Proof of the Main Theorem

First of all we can assume that $f(z,x)=0$ depends on z and x, otherwise the assertion of our Theorem 1 would be trivially true. We can also suppose without loss of generality that $f(z,x)$ is absolutely irreducible. Otherwise we can find a finite extension field L of K such that $f(z,x)$ splits into a product of absolutely irreducible factors in $L[z,x]$. Then we can proceed with each of those factors as below and sum up the number of solutions to get the final result. So let us denote by F the functions field obtained by adjoining a root of $f(z,x)=0$ to $\bar{K}(z)$, where $\bar{K}$ denotes the algebraic closure of K.

Moreover, we may assume that $\alpha_1,\ldots,\alpha_t$ generate together a torsion-free multiplicative group. Because otherwise, if q is the order of the torsion in the multiplicative group generated by the roots, then for each $r=0,1,\ldots,q-1$, the recurrences G_{nq+r} have roots generating a torsion-free group. Thus, we can proceed by considering each of these cases separately and sum up the resulting bounds. Observe that by the assumption that the characteristic roots are nondegenerate, the number of characteristic roots of G_{nq+r} is always ≥ 2.

We work only in the case $|\alpha_1|>1$ and consider the Puiseux expansion at $z=\infty$ of the solution $x=x(z)$ of $f(z,x)=0$. The arguments in the case $|\alpha_1|<1$ are completely analogous and use the expansion at $z=0$.

In the sequel $C_1,C_2,\ldots$ will denote positive numbers depending only on $f(z,x)$ and on λ_1 and on the P_i,α_i.

According to Theorem 3 the number of solutions of (5) of the form $(n,0)$, $n\in\mathbb{N}$ can be estimated by

$$C_2=A(t,a)=e^{(7t^a)^{8t^a}},$$

where $a=\max\{\deg P_i\,|\,i=2,\ldots,t\}$. Observe that this follows from the fact that (G_n) is nondegenerate. Consequently, we can restrict ourselves to solutions of the form $(n,x)\in\mathbb{N}\times K$ with $x\neq 0$. These solutions are denoted by $(n,x_n)\in\mathbb{N}\times K$ with $n\in\Sigma$, where Σ is a set of positive integers.

Now by Puiseux's Theorem 4 we can conclude that

$$f(z,x)=\prod_{j,i}(x-x_{ij}),$$

where

$$x_{ij}=\sum_{k=v_i}^{\infty}a_{ik}\zeta^{jk}\left(\frac{1}{z}\right)^{\frac{k}{e_i}},$$

for $j=0,\ldots,e_i-1$, $i=1,2,\ldots,r$ and where $e_1,\ldots,e_r$ are the ramification indices of the valuations extending $1/z$ to the function field F. Furthermore by the Explicit Puiseux's Theorem 5 we get that all coefficients lie in a fixed finite extension field K' of K and we have

$$h(a_{ik}\zeta^{jk}) \leq \Lambda^{k-v_i+1},$$

for $j=0,\dots,e_i-1$, $i=1,2,\dots,r$ and where Λ denotes the Eisenstein constant. Therefore for each solution (n,x_n) of (5) we get

$$x_n = \sum_{k=w}^{\infty} \beta_k G_n^{-\frac{k}{e}}, \tag{23}$$

for some w, e and β_k with

$$|\beta_k| \leq \Lambda^{k-w+1}$$

for all $k=1,2,\dots$, which lie in a fixed finite extension of K. In what follows we will only consider those n, lying in a subsequence $\mathcal{R}\subseteq\Sigma$, for which the same expansion occurs. The final number is just the sum of all numbers obtained by all those expansions.

Let us remark that for $n>C_3$ (which will be specified later) the above series converges absolutely; this is because

$$\begin{aligned}
|G_n| &= |\lambda_1\alpha_1^n+\ldots+P_t(n)\alpha_t^n| = |\lambda_1||\alpha_1|^n\left|1+\sum_{j=2}^{t}\frac{P_j(n)}{\lambda_1}\left(\frac{\alpha_j}{\alpha_1}\right)^n\right| \geq \\
&\geq |\lambda_1||\alpha_1|^n\left|1-\underbrace{\sum_{j=2}^{t}\left|\frac{P_j(n)}{\lambda_1}\right|\left|\frac{\alpha_j}{\alpha_1}\right|^n}_{\leq 1/2 \text{ for } n>C_3}\right| \geq \frac{|\lambda_1|}{2}|\alpha_1|^n \longrightarrow \infty,
\end{aligned}$$

because $|\alpha_1|>1$. Thus

$$\begin{aligned}
\sum_{k=w}^{\infty}|\beta_k||G_n|^{-k/e} &\leq \sum_{k=w}^{\infty}\Lambda^{k-w+1}\left(\frac{|\lambda_1|}{2}|\alpha_1|^n\right)^{-k/e} = \\
&= \Lambda^{-w+1}\sum_{k=w}^{\infty}\Bigg(\underbrace{\Lambda\left(\frac{|\lambda_1|}{2}|\alpha_1|^n\right)^{-1/e}}_{\leq 1/2 \text{ for } n>C_3}\Bigg)^k < \infty,
\end{aligned}$$

converges, if $n>C_3$ is satisfied.

Since $|\alpha_1|>|\alpha_i|$ for $i=2,\dots,t$, we have binomial expansions

$$\begin{aligned}
G_n^{-\frac{k}{e}} &= \lambda_1^{-\frac{k}{e}}\alpha_1^{-\frac{kn}{e}}\left(1+\sum_{i=2}^{t}\frac{P_i(n)}{\lambda_1}\left(\frac{\alpha_i}{\alpha_1}\right)^n\right)^{-\frac{k}{e}} = \\
&= \lambda_1^{-\frac{k}{e}}\alpha_1^{-\frac{kn}{e}}\sum_{r=0}^{\infty}\binom{-\frac{k}{e}}{r}\left(\sum_{i=2}^{t}\frac{P_i(n)}{\lambda_1}\left(\frac{\alpha_i}{\alpha_1}\right)^n\right)^r,
\end{aligned}$$

for some choice of the eth roots of λ_1 and α_1, which we may assume to be fixed for all $n \in \mathcal{R}$. Because of the fact that

$$\left|\sum_{i=2}^{t} \frac{P_i(n)}{\lambda_1}\left(\frac{\alpha_i}{\alpha_1}\right)^n\right| \le \frac{g}{|\lambda_1|} n^a c^n < 1,$$

where $c := \max\{|\alpha_j/\alpha_1| \mid j = 2, \dots, t\}$ and g is t times the maximum of the absolute values of the coefficients of the $P_i, i = 2, \dots, t$, if $n > C_3$, the expansion converges again absolutely for large n.

Next we are going to approximate x_n by a finite sum extracted from the Puiseux expansion (23). We define

$$H_n := \sum_{k=w}^{H} \beta_k \lambda_1^{-\frac{k}{e}} \alpha_1^{-\frac{kn}{e}} \sum_{r=0}^{H} \binom{-\frac{k}{e}}{r} \left(\sum_{i=2}^{t} \frac{P_i(n)}{\lambda_1}\left(\frac{\alpha_i}{\alpha_1}\right)^n\right)^r,$$

where $H \ge 1$ is an integer to be chosen later. We may write

$$H_n = \sum_{j=1}^{h} \tau_j(n)\gamma_j^n, \quad n \in \mathcal{R},$$

where the $\tau_j(n) \in \bar{K}[n]$ and the γ_j are distinct and lie in the multiplicative group generated by $\alpha_1^{1/e}$ and $\alpha_2, \dots, \alpha_t$. Clearly H_n is nondegenerate, in fact the roots γ_j again generate a torsion-free group. Moreover, we have

$$h \le C_4(H) := \binom{t+H}{H}(H + 1 - w), \tag{24}$$

where $C_4(H)$ means that the constant depends also on H.

We enlarge K at once and assume that it contains all the $\alpha_i^{1/e}$ and all the coefficients β_j in the Puiseux series. In particular, we may assume that K contains all the coefficients of τ_j and the γ_j.

Next we estimate the approximation error we make, when we approximate x_n through H_n. We have

$$|x_n - H_n| = \left|x_n - \sum_{k=w}^{H} \beta_k \lambda_1^{-\frac{k}{e}} \alpha_1^{-\frac{kn}{e}} \sum_{r=0}^{H} \binom{-\frac{k}{e}}{r} \left(\sum_{i=2}^{t} \frac{P_i(n)}{\lambda_1}\left(\frac{\alpha_i}{\alpha_1}\right)^n\right)^r\right| \le$$

$$\le \left|\sum_{k=w}^{H} \beta_k \lambda_1^{-\frac{k}{e}} \alpha_1^{-\frac{kn}{e}} \sum_{r=H+1}^{\infty} \binom{-\frac{k}{e}}{r} \left(\sum_{i=2}^{t} \frac{P_i(n)}{\lambda_1}\left(\frac{\alpha_i}{\alpha_1}\right)^n\right)^r\right| +$$

$$+\left|\sum_{k=H+1}^{\infty} \beta_k \underbrace{\lambda_1^{-\frac{k}{e}} \alpha_1^{-\frac{kn}{e}} \sum_{r=0}^{\infty} \binom{-\frac{k}{e}}{r} \left(\sum_{i=2}^{t} \frac{P_i(n)}{\lambda_1}\left(\frac{\alpha_i}{\alpha_1}\right)^n\right)^r}_{=G_n^{-k/e}}\right| \le$$

$$\begin{aligned}
&\leq \sum_{k=w}^{H} \Lambda^{k-w+1}|\lambda_1|^{-\frac{k}{e}}|\alpha_1|^{-\frac{wn}{e}}2(H+1)^{H+1}\left|\sum_{i=2}^{t}\frac{P_i(n)}{\lambda_1}\left(\frac{\alpha_i}{\alpha_1}\right)^n\right|^{H+1}+\\
&\qquad\qquad + \sum_{k=H+1}^{\infty}\Lambda^{k-w+1}\left(\frac{|\lambda_1|}{2}|\alpha_1|^n\right)^{-k/e}\leq\\
&\leq \sum_{k=w}^{H} \Lambda^{k-w+1}|\lambda_1|^{-\frac{k}{e}}|\alpha_1|^{-\frac{wn}{e}}2(H+1)^{H+1}\left(\frac{g}{|\lambda_1|}n^a c^n\right)^{H+1}+\\
&\qquad\qquad +\Lambda^{-w+1}\frac{\left(\Lambda\left(\frac{|\lambda_1|}{2}|\alpha_1|^n\right)^{-1/e}\right)^{H+1}}{1-\underbrace{\Lambda\left(\frac{|\lambda_1|}{2}|\alpha_1|^n\right)^{-1/e}}_{\leq 1/2 \text{ for } n>C_3}}\leq\\
&\leq 2\Lambda^{H-w+1}\tilde{\lambda}(H+1)^{H+1}g^{H+1}n^{a(H+1)}|\alpha_1|^{-\frac{wn}{e}}\tilde{c}^{n(H+1)},
\end{aligned}$$

where

$$\tilde{\lambda} := \max\left\{1, |\lambda_1|^{-\frac{w}{e}-H-1}, |\lambda_1|^{-\frac{H}{e}-H-1}, |\lambda_1|^{-\frac{H+1}{e}}\right\}$$

and $\tilde{c} := \max\{c, |\alpha_1|^{-1/e}\}$. Observe that we have $\tilde{c} < 1$. Moreover, observe that we have used

$$\begin{aligned}
&\left|\sum_{r=H+1}^{\infty}\binom{-\frac{k}{e}}{r}z^r\right|\leq\\
&\quad\leq \sum_{r=H+1}^{\infty}\frac{|k|}{er}\left(1+\frac{|k|}{e}\right)\left(1+\frac{|k|}{2e}\right)\cdots\left(1+\frac{|k|}{(r-1)e}\right)|z|^r\leq\\
&\quad\leq \sum_{r=H+1}^{\infty}\left(1+\frac{|k|}{e}\right)^r|z|^r\leq\sum_{r=H+1}^{\infty}(H+1)^r|z|^r\leq\frac{(H+1)^{H+1}|z|^{H+1}}{1-(H+1)|z|}\leq\\
&\quad\leq 2(H+1)^{H+1}|z|^{H+1},
\end{aligned}$$

if $H > -w$ (which implies $|k| \leq H$) and if

$$|z| \leq \frac{g}{|\lambda_1|}n^a c^n \leq \frac{1}{2(H+1)} \leq \frac{1}{2},$$

which is possible if

$$\begin{aligned}
&n > C_3 :=\\
&\quad = \max\left\{2\frac{\log\frac{2(H+1)g}{|\lambda_1|}}{\log\frac{1}{c}} + 2\max\left\{\frac{a}{\log\frac{1}{c}}\log\frac{a}{\log\frac{1}{c}}, 15\right\},\right.\\
&\qquad\qquad\qquad\qquad \left.\frac{e\log 2\Lambda - \log\frac{|\lambda_1|}{2}}{\log|\alpha_1|}\right\},
\end{aligned}$$

to estimate the tail of the above series. Observe that we have used a Lemma of Pethő and de Weger (cf. [18],[27, Appendix]) to obtain the first part of the above lower bound.

For later purposes we need an estimate of $|x_n|$. For n larger than the constant C_3 we obtain in the same fashion as above

$$|x_n| = \left| \sum_{k=w}^{\infty} \beta_k G_n^{-\frac{k}{e}} \right| \le 2\Lambda^{-w+1} \tilde{g}^{\frac{|w|}{e}} |\alpha_1|^{\frac{n|w|}{e}}, \tag{25}$$

where $\tilde{g} := \max\{1, |\lambda_1|, g\}$.

We choose H so that

$$\tilde{c}^{H+1} |\alpha_1|^{-\frac{wn}{e} + \frac{|w|n}{e}} < 1. \tag{26}$$

To get this, we must have

$$H > \max\left\{1, \frac{2|w| \log|\alpha_1|}{e \log \frac{1}{\tilde{c}}} - 1, -w\right\}.$$

Observe that from now on H is fixed and therefore also $h, \tau_i(n), \gamma_i, i = 1, \ldots, h$ are fixed. Also, we choose a finite set S so that it contains all infinite absolute values of K. Moreover we require that all the α_j, λ_1 and all coefficients of the $P_j(n)$, all the nonzero coefficients of $f(z,x)$ are S-units, which means that the $|\cdot|_v$ of those values $= 1$ for each $v \notin S$. In particular, with this choice all γ_j are S-units. Also, the G_n are S-integers, that is $|G_n|_v \le 1$ for each $v \notin S$, and $f(z,x)$ is monic in x; therefore, the x_n too are S-integers, in view of the equations $f(G_n, x_n) = 0$. We denote by s the cardinality of S. Clearly, it is possible to choose $s \ge h$.

Let us introduce a notation: for $a \in K$ we write

$$\overline{h}_s(a) = \max\{|a|_v \mid v \in S\},$$

for the S-height of a. Observe that we have

$$\overline{h}_s(a) \le \prod_{v \in M_K} \max\{1, |a|_v\} \le \mathcal{H}(1, a).$$

For a polynomial p with coefficients in K, $\overline{h}_s(p)$ denotes the maximum of the S-heights of the coefficients. In the same fashion, we define $\overline{h}_s(p_1, \ldots, p_h)$.

We shall apply Theorem 2, so let us define, for every $v \in S$, $h+1$ independent linear forms in $\mathbf{X} := (X_0, \ldots, X_h)$ as follows: put

$$L_{0,\infty}(\mathbf{X}) = X_0 + X_1 + \cdots + X_h$$

and for $v \in S, 0 \le i \le h, (i,v) \ne (0,\infty)$ put

$$L_{i,v}(\mathbf{X}) = X_i.$$

Here ∞ denotes the infinite absolute value, which coincides with the complex absolute value in the embedding of K in $\mathbb{C}$. We have

$$\mathcal{H}(L_{i,v}) \leq \sqrt{h+1}$$

for $v \in S, i = 0, \ldots, h$. Furthermore $K(L_{i,v}) = K$ and therefore

$$[K(L_{i,v}) : K] = 1 \quad \forall v \in S, i = 0, \ldots, h.$$

Moreover, we have

$$\det(L_{0,v}, \ldots, L_{h,v}) = \begin{vmatrix} 1 & 0 & 0 & \ldots & 0 \\ 1 & 1 & 0 & \ldots & 0 \\ 1 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & 0 & 0 & \ldots & 1 \end{vmatrix} = 1,$$

which yields

$$|\det(L_{0,v}, \ldots, L_{h,v})|_v = 1 \quad \forall\, v \in S.$$

For $n \in \mathcal{P}$ define the vectors $\mathbf{x}_n = (-x_n, \tau_1(n)\gamma_1^n, \ldots, \tau_h(n)\gamma_h^n) \in K^{h+1}$ and consider the double product

$$\prod_{v \in S} \prod_{i=0}^{h} \frac{|L_{i,v}(\mathbf{x}_n)|_v}{|\mathbf{x}_n|_v}.$$

By putting

$$\sigma = -x_n + \tau_1(n)\gamma_1^n + \ldots + \tau_h(n)\gamma_h^n = L_{0,\infty}(\mathbf{x}_n),$$

we can rewrite the double product as

$$|\sigma|_\infty \cdot \left(\prod_{v \in S \setminus \{\infty\}} |x_n|_v \right) \left(\prod_{v \in S} \prod_{i=1}^{h} |\tau_i(n)\gamma_i^n|_v \right) \left(\prod_{v \in S} |\mathbf{x}_n|_v \right)^{-(h+1)}.$$

Observe that x_n is an S-integer and that, due to our choice of S, the γ_i^n are S-units for $i \geq 1$. In particular, this implies

(27)

$$\left(\prod_{v \in S} \prod_{i=1}^{h} |\tau_i(n)\gamma_i^n|_v \right) = \prod_{v \in S} \prod_{i=1}^{h} |\tau_i(n)|_v \leq (aH+1)^{hs} \overline{h}_s^{hs}(\tau_1, \ldots, \tau_h) n^{aHhs}$$

and

$$\left(\prod_{v \in S \setminus \{\infty\}} |x_n|_v \right) = \prod_{v \notin S} |x_n|_v \cdot |x_n|_\infty \leq |x_n|, \tag{28}$$

where we have used the product formula (15) and (25). We want to remark that the $\tau_i(n)$ have degree at most aH. Therefore we get using the bound for the approximation error, (27) and (28)

$$\prod_{v\in S}\prod_{i=0}^{h}\frac{|L_{i,v}(\mathbf{x}_n)|_v}{|\mathbf{x}_n|_v}\le C_5 n^{C_6} C_7^n \tilde{c}^{n(H+1)}\left(\prod_{v\in S}|\mathbf{x}_n|_v\right)^{-(h+1)},$$

where

$$\begin{aligned}
C_5 &:= 4\Lambda^{H-2w+2}(aH+1)^{hs}\left((H+1)g\right)^{H+1}\tilde{\lambda}\tilde{g}^{\frac{|w|}{e}}\overline{h}_s^{hs}(\tau_1,\dots,\tau_h),\\
C_6 &:= a(H+Hhs+1),\\
C_7 &:= |\alpha_1|^{-\frac{w}{e}+\frac{|w|}{e}},
\end{aligned}$$

respectively.

Last we need an upper bound for $\mathcal{H}(\mathbf{x}_n)$. We have

$$\mathcal{H}(\mathbf{x}_n)\le\prod_{v\in S}|\mathbf{x}_n|_v\le\sqrt{h+1}\prod_{v\in S}\max\{|x_n|_v,|\tau_1(n)\gamma_1^n|_v,\dots,|\tau_h(n)\gamma_h^n|_v\},$$

where we have used again our choice of S and the fact that the two norms on K^{h+1} are equivalent. We need an estimate for $|x_n|_v$ and we derive it from the equation $f(G_n,x_n)=0$. Observe that we trivially have an estimate

$$|G_n|_v\le t\overline{h}_s(\lambda_1,P_2,\dots,P_t)n^a\overline{h}_s(\alpha_1,\dots,\alpha_t)^n.$$

On the other hand, we can estimate the absolute value of the roots of an equation in terms of the absolute value of the coefficients. We finally obtain

$$|x_n|_v\le N^2\overline{h}_s(f)t^N\overline{h}_s(\lambda_1,P_2,\dots,P_t)^N n^{aN}\overline{h}_s(\alpha_1,\dots,\alpha_t)^{nN},$$

where N denotes the total degree of $f(z,x)$. Moreover we have

$$|\tau_i(n)\gamma_i^n|_v\le(aH+1)\overline{h}_s(\tau_1,\dots,\tau_h)n^{aH+1}\overline{h}_s(\gamma_1,\dots,\gamma_h)^n,$$

for all $i=1,\dots,h$. Consequently we get

$$\mathcal{H}(\mathbf{x}_n)\le C_8 n^{C_9}C_{10}^n, \tag{29}$$

where s denotes the cardinality of S. Let us point out that the constants

$$\begin{aligned}
C_8 &:= \sqrt{h+1}\max\{N^2\overline{h}_s(f)t^N\overline{h}_s(\lambda_1,P_2,\dots,P_t)^N,\\
&\qquad\qquad (aH+1)\overline{h}_s(\tau_1,\dots,\tau_h)\}^s,\\
C_9 &:= \max\{aN,aH+1\}s,\\
C_{10} &:= \max\{\overline{h}_s(\alpha_1,\dots,\alpha_t)^N,\overline{h}_s(\gamma_1,\dots,\gamma_h)\}^s
\end{aligned}$$

do not depend on n.

We now choose $0<\delta<1$ so that

$$\tilde{c}^{H+1}C_7C_{10}^{\delta}<1. \tag{30}$$

This will be possible for small δ in view of (26), namely for

$$\delta<\frac{\log\left(\tilde{c}^{H+1}C_7\right)^{-1}}{\log C_{10}}.$$

In view of the bound for the double product we derived and (29), the verification of (16) of the Quantitative Subspace Theorem 2 will follow from

$$C_5 n^{C_6} \left(\tilde{c}^{H+1} C_7\right)^n < \left(C_8 n^{C_9} C_{10}^n\right)^{-\delta},$$

which is the same as

$$n^{C_6+\delta C_9} \left(\tilde{c}^{H+1} C_7 C_{10}^{\delta}\right)^n < \left(C_5 C_8^{\delta}\right)^{-1}.$$

However, this latter inequality follows from (30) for

$$n \geq C_{11} := 2\frac{\log\left(C_5 C_8^{\delta}\right) + (C_6+\delta C_9)\left(\log\left(C_6+\delta C_9\right) + \log\left(\tilde{c}^{H+1} C_7 C_{10}^{\delta}\right)\right)}{\log\left(\tilde{c}^{H+1} C_7 C_{10}^{\delta}\right)^{-1}},$$

(for $a = 0$ the formula is true with $\log(0) = 0$) which follows again by a Lemma of Pethő and de Weger (cf. [18],[27, Appendix]).

Therefore, by the Quantitative Subspace Theorem 2, there exist finitely many non-zero linear forms $\Lambda_1(\mathbf{X}), \ldots, \Lambda_g(\mathbf{X})$ with coefficients in $\bar{K}$ and with

$$g \leq C_{12} := (2^{60(h+1)^2} \cdot \delta^{-7(h+1)})^s (3 + \log\log 2\sqrt{h+1}),$$

such that each vector $\mathbf{x}_n$ is a zero of some Λ_j.

Suppose first Λ_j does not depend on X_0. Then, if $\Lambda_j(\mathbf{x}_n) = 0$, we have a nontrivial relation

$$\sum_{i=1}^{h} u_i \tau_i(n) \gamma_i^n = 0, \quad u_i \in \bar{K}, i = 1, \ldots, h.$$

By Theorem 3 this can hold for at most a finite number of n. More precisely, we can conclude that the number of those solutions can be bounded by a constant

$$C_{13} := A(h, aH) = e^{(7h^{aH})^{8h^{aH}}},$$

since the γ_i are nondegenerate.

Suppose that Λ_j depends on X_0 and that $\Lambda_j(\mathbf{x}_n) = 0$. Then we have

$$x_n = \sum_{i=1}^{h} v_i \tau_i(n) \gamma_i^n, \quad v_i \in \bar{K}, i = 1, \ldots, h. \tag{31}$$

Substituting this into $f(z, x) = 0$ we get

$$f\left(G_n, \sum_{i=1}^{h} v_i \tau_i(n) \gamma_i^n\right) = 0. \tag{32}$$

Equation (32) cannot hold identically because of the assumption of the Theorem. Moreover, the series staying on the left hand side of (32) is a nondegenerate linear recurring sequence. Hence,

$$|\{n | n \text{ satisfies } (32)\}| < C_{14} := A(C_{15}, C_{16}),$$

where

$$C_{15} := \binom{t+N}{N} \cdot \binom{h+N}{N} \quad \text{and} \quad C_{16} := a(H+1)N$$

also in this case, because the left hand side of (32) defines a nondegenerate linear recurring sequence and the conclusion follows again by Theorem 3. Observe that from the assumption that the $\alpha_1, \ldots, \alpha_t$ generate a torsion-free group, we conclude the nondegeneracy.

Then the number of solutions of (5) can be bounded by

$$C_2 + \sum_{i=1}^{r} \sum_{j=0}^{e_i - 1} \left[C_{12}(C_{13} + C_{14}) + \max\{C_3, C_{11}\} \right],$$

where the constants in the sum clearly can depend on i, j. This completes the proof. □

5. Proof of the Corollaries

Proof of Corollary 2.

This follows readily from Theorem 1 in form of Corollary 1 and a result, mentioned in the introduction, which is due to Shorey and Stewart [25, Theorem 3]. Let us remark that by Eisenstein's criterion for absolutely irreducibility the polynomials $f(z,x) = x^q - z$ are absolutely irreducible for all q. Moreover, observe that $G_n - \lambda_1 \alpha_1^n \neq 0$, because of our assumption $t \geq 2$. □

Proof of Corollary 3.

Let d be the degree of α_1 over $\mathbb{Q}$. Using a result of Shorey and Stewart [25, Corollary 1], also mentioned in the introduction, we can conclude that the number of solutions n, x and q with $n \geq 0, |x| > 1$, and

$$q > \max\left(\frac{d \log|\alpha_1|}{\log(|\alpha_1| / \max(1, |\alpha_2|))}, d + r \right)$$

of the equation

$$G_n = x^q + T(x)$$

is finite. It remains to show that the number of solutions n, x and q with $n \geq 0, |x| > 1$ and

$$1 \leq q \leq \max\left(\frac{d \log|\alpha_1|}{\log(|\alpha_1| / \max(1, |\alpha_2|))}, d + r \right)$$

is also finite. But this follows now from our Theorem 1. Observe that only for the solutions with small q, an upper bound for the number of solutions can be given. □

References

[1] S. Ahlgren, Polynomial-exponential equations in two variables, *J. Number Theory* **62** (1997), no. 2, 428-438.

[2] S. Ahlgren, Equations $F(x, y, \alpha^x) = 0$, Topics in number theory (University Park, PA, 1997), 85-100, *Math. Appl.* **467**, Kluwer Acad. Publ., Dordrecht, 1999.

[3] J. Coates, Construction of rational functions on a curve, *Proc. Camb. Phil. Soc.* **68** (1970), 105-123.

[4] P. Corvaja and U. Zannier, Diophantine equations with power sums and universal Hilbert sets, *Indag. Math., New Ser.* **9 (3)** (1998), 317-332.

[5] P. Corvaja and U. Zannier, Some new applications of the Subspace Theorem, *Compos. Math.* **131** (2002), no. 3, 319-340.

[6] B. M. Dwork and A. van der Poorten, The Eisenstein constant, *Duke Math. J.* **65** (1992) no. 1, 23-43, Corrections: *Duke Math. J.* **76** (1994), no. 2, 669-672.

[7] M. Eichler, *Introduction to the theory of algebraic numbers and functions*, Academic Press, New York and London, 1966.

[8] J.-H. Evertse, An improvement of the quantitative subspace theorem, *Compos. Math.* **101 (3)** (1996), 225-311.

[9] C. Fuchs and R. F. Tichy, Perfect powers in linear recurring sequences, *Acta Arith.*, to appear.

[10] K. Iwasawa, *Algebraic Functions*, Translations of Mathematical Monographs Vol. 118, American Mathematical Society, Providence, Rhode Island, 1993.

[11] P. Kiss, Differences of the terms of linear recurrences, *Studia Sci. Math. Hung.* **20** (1985), 285-293.

[12] I. Nemes and A. Pethő, Polynomial values in linear recurrences, *Publ. Math.* **31** (1984), 229-233.

[13] I. Nemes and A. Pethő, Polynomial values in linear recurrences II, *J. Number Theory* **24** (1986), 47-53.

[14] A. Pethő, Perfect powers in second order linear recurrences, *J. Number Theory* **15** (1982), 5-13.

[15] A. Pethő, Perfect powers in second order recurrences, Topics in classical number theory, Vol.I,II, Proceedings of the Conference in Budapest 1981, Colloq. Soc. János Bolyai 34, North-Holland, Amsterdam, 1217-1227.

[16] A. Pethő, On the solutions of the equation $G_n = P(x)$, *Fibonacci Numbers and Their Applications*, D. Reidel Publ. Comp. 1986, 193-201.

[17] A. Pethő, Diophantine properties of linear recursive sequences II, *Acta Math. Acad. Paed. Nyiregyháziensis* **17** (2001), 81-96.

[18] A. Pethő and B. M. M. de Weger, Product of Prime Powers in Binary Recurrence Sequences I., *Math. Comp.* **47** (1986), 713-727.

[19] W. M. Schmidt, "Diophantine Approximation", Springer Verlag, LNM **785**, 1980.

[20] W. M. Schmidt, Eisenstein's theorem on powers series expansions of algebraic functions, *Acta. Arith.* **56** (1990), no. 2, 161-179.

[21] W. M. Schmidt, "Diophantine Approximations and Diophantine Equations", Springer Verlag, LNM **1467**, 1991.

[22] W. M. Schmidt, Equations $\alpha^x = R(x, y)$, *J. Number Theory* **47** (1994), 348-358.

[23] W. M. Schmidt, The zero multiplicity of linear recurrence sequences, *Acta Math.* **182** (1999), 243-282.

[24] T. N. Shorey and C. L. Stewart, On the Diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrence sequences, *Math. Scand.* **52** (1983), 24-36.

[25] T. N. Shorey and C. L. Stewart, Pure Powers in Recurrence Sequences and Some Related Diophantine Equations, *J. Number Theory* **27** (1987), 324-352.

[26] T. N. Shorey and R. Tijdeman, "Exponential Diophantine Equations", Cambridge University Press, Cambridge, 1986.

[27] N. P. SMART, "The Algorithmic Resolution of Diophantine Equations", Cambridge University Press, Cambridge, 1998.

[28] H. STICHTENOTH, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, Heidelberg, 1993.

[29] U. ZANNIER, A proof of Pisot's dth root conjecture, *Ann. of Math. (2)* **151**, no. 1 (2000), 375-383.